2011

Results of the Assessment of the Implementation of the Safer Social Networking Principles for the EU:

Individual Reports of Testing of 14 Social Networking Sites

By request of the European Commission under the Safer Internet Programme

European Commission
Information Society and Media

VERÓNICA DONOSO
UNIVERSITY OF ANTWERP, BELGIUM

May, 2011

THIS IS A REPORT MADE BY REQUEST OF THE EUROPEAN COMMISSION

UNDER THE SAFER INTERNET PROGRAMME

OPINIONS EXPRESSED IN THE REPORT ARE THOSE OF AUTHORS AND DO NOT NECESSARILY

REFLECT THE VIEWS OF THE EC.

May 2011

Please cite as follows:

Donoso, V. (2011). Results of the Assessment of the Implementation of the Safer Social Networking Principles for the EU. Individual Reports of Testing of 14 Social Networking Sites. European Commission, Safer Internet Programme, Luxembourg.

TABLE OF CONTENTS

OVERVIEW OF SIGNATORIES AND TESTERS

This part consists of the reports submitted by the national researchers on each signatory Social Networking Site. Below is a summary of the participating Social Networks, the date of submission of their self-declarations (SD), the version tested, and the name and affiliation of the expert tester. For further information on the methodology and testing details please refer to the first part of this report and the annexes.

Signatories	Date of accession to the Principles	Date of submission of the self-Updated self-declarations	version	Tested by	Affiliation
Arto	10 February 2009	15 April 2009	Danish	Ditte Maria Bergstrøm	IT University of Copenhagen
Bebo	10 February 2009	17 April 2009	English	Simon Grehan	NCTE
Facebook	10 February 2009	16 December 2010	French English	Cédric Fluckiger Simon Grehan	University of Lille NCTE
Giovani	10 February 2009	02 July 2010	Italian	Giovanna Mascheroni	University of Torino and OssCom Catholic University of Milano
Hyves	10 February 2009	15 November 2010	Dutch	Michel Walrave	MIOS, University of Antwerp
IRC-Galleria	10 February 2009	05 November 2010	Finnish	Niina Uusitalo	Tampereen yliopisto
MySpace	10 February 2009	14 November 2010	English Spanish	Simon Grehan Charo Sádaba	NCTE School of Communication, Univ. of Navarra
Nasza-klasa	10 February 2009	31 May 2010	Polish	Aldona Zdrodowska	Warsaw School of Social Sciences and Humanities
Netlog	10 February 2009	03 July 2010	Dutch German	Michel Walrave Monika Taddicken	MIOS, University of Antwerp University of Hamburg
One	10 February 2009	17 June 2009	Lithuanian	Rita Žukauskienė	Mykolas Romeris University
Rate	9 June 2009	9 June 2009	Estonian	Andra Siibak	Institute of Journalism and Communication , University of Tartu
SchuelerVZ	10 February 2009	26 May 2010	German	Monika Taddicken	University of Hamburg
Tuenti	12 June 2009	21 May 2010	Spanish	Charo Sádaba	School of Communication, University of Navarra
ZAP	10 February 2009	17 April 2009	Luxembourgish	André Melzer	Université du Luxembourg

ARTO

Ditte Maria Bergstrøm, Academic Assistant, IT University of Copenhagen, Denmark
Verónica Donoso, Appointed Research Coordinator by the EC

Introduction

This paper will report the results of the evaluation of the Social Networking Site (SNS) ARTO. ARTO is a Danish site that has existed since 1998 and has about 90.000 profiles[1]. The evaluation was done by testing the site from a user perspective. This SNS is for users from the age of 10. It provides the members the option of creating profiles, sending messages to each other, posting comments on others users profiles, using applications, posting pictures, writing a diary, participating in clubs, etc. The test was performed during the period from the 20th – 29th of December 2010.

Summary of main findings

It is not possible for Arto users (including minors) to make their profile private; hence everybody, including non-registered users, can see practically all the information posted by them all the time. This is because also non-registered users can use Arto internal search engine to search for members of the SNS. However, profiles of minors cannot be found through external ones such as Google.

The Terms of Use state that the minimum age requirement is 12, while the "about ARTO"[2] section states that the SNS is for kids aged 10 years old and above. In any case, it was possible for a 9-year old to sign up on the site.

Although the provider has taken measures to reduce the risk of exposure to inappropriate content, it is still possible for minors to find some inappropriate content via forums (e.g. tips on sexual positions). Advertising displayed was age-appropriate, though.

The information about safety is limited and it is only targeted towards parents and not the young users. The information that is targeted towards parents is clearly worded and easy to find.

There are two reporting mechanisms available on the SNS. Both are easy to find and use. Once conduct/contact abuse is reported on this SNS, ARTO provides fast feedback both regarding the situation with advice on how to block the offending person and the SNS takes care of the situation by deleting the messages/photos and deleting the profile of the offender. However the reactions to reports are inconsistent and inefficient: On the one hand, only one of the two "perpetrators" made up for this test was "punished" by having his/her account closed. On the other hand, it was possible for the "banned" minor to sign up again on the site without any difficulties and even without having to change any personal details or e-mail address.

It is very easy to block a person. Although when a person is blocked they can still see the content (e.g. pictures, wall, guestbook etc.) of the person who blocked them.

A user cannot delete their profile. They are able to deactivate it, although all information is being stored. When re-logging into the site, the account reactivates.

[1] http://fdim.dk/statistik, Oct. 2010, [The Union of Danish Interactive Media]

[2] http://www.arto.com/section/support/?fc=0&tab=5

Analysis of Results by Principle

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner

Main findings in relation to the self-declaration

As stated in its self declaration, Arto provides clear and age-appropriate "Terms of Use", easy for teenagers to understand. It also provides a "Safety" section with information such as general support and safety tools available on the site, and a "Guidelines" section that provides information on the "main rules governing the site". It is not clear from the self-declaration if the information in the Safety and the Guidelines sections is specifically targeted at children and young people.
The self-declaration does not state if Arto provides educational materials for children. Besides, it does not explicitly mention what the consequences of breaking Arto`s rules are.

Arto provides parents and teachers with targeted, easy-to understand information regarding what Arto is, how it works, how it protects its younger users, and safety tools available on the site. This section also gives useful tips so that parents can better protect their children online and provides them with external links where parents may find external support.

Main findings in relation to the website

Confirming what is stated in the self-declaration, the "Guidelines" section provides age-appropriate and easy-to-understand information on what constitutes inappropriate behaviour and the consequences of breaching Arto`s Terms of Use[3]. They are easy to find and clearly worded for a minor. A different version of the Terms of Use[4] was found (only via Google, though). This document states, for instance, that the minimum age for use is 12, while the "about ARTO"[5] section states that the SNS is for kids aged 10 years old and above. Indeed, as the test shows it is possible to sign up as a 10 year old without any difficulties. The Terms of Use define what constitutes inappropriate behaviour on the site and the consequences thereof (e.g. "any signs of paedophile content will be reported to the police immediately"). This document also states that the user automatically accepts Terms of Use by signing up to ARTO. However, during the testing it was not possible to find these Terms of Use on the website (only via Google as previously stated). This indicates that many users may be unaware of the Terms they are agreeing to while signing up to Arto.

Regarding the safety information available, the user has to scroll to the bottom of the page to find this information. Safety information primarily focuses on what ARTO does to make the website safe, e.g. Arto replies to reports within 24 hours; it employs word filters to track inappropriate words, etc. This information is presented in 10 clear bullet points. However, confirming the analysis of the self-declaration, there are no safety guidelines targeted at children and young people, only educational material targeted at parents. Although, the safety information for parents is easy to find and is clearly worded, it is not concrete. Rather, it provides general guidelines such as "Talk to your child about good behaviour online". Toward the bottom of the page there are some safety tips for parents to talk about with their kids. The tips are clearly worded and presented with bullet points, making them easy to locate and to read. These tips include for example "Don't answer unpleasant messages. Report the user and delete the message". Confirming the analysis of the self-declaration, there are links to educational materials, but all of this information is oriented solely toward parents as they are included in the "Safety Tips for Parents" section. The material is easy to understand, clearly worded and

[3] http://www.arto.com/section/cms/page.aspx?id=8

[4] http://www.arto.com/section/cms/page.aspx?id=74

[5] http://www.arto.com/section/support/?fc=0&tab=5

available in Danish. However, the information provided on specific risks (e.g. hate speech, pornography, grooming, etc.) related to using ARTO is deficient. There is only one sentence in plain text stating: “Some people might bully or submit offensive content”.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience

Main findings in relation to the self-declaration

According to the self-declaration the minimum registration age to subscribe to Arto is 12 years old. In order to identify and delete underage users from Arto, they have implemented a mechanism that allows them to identify repeated offenders and, eventually, block access to their site from their IP address.

Arto provides several mechanisms to ensure the limited exposure of children to inappropriate content or contact, for instance, a few parts of the site (e.g. the forum) are age-restricted, users can only see profile pictures of users around their own age category and advertising is tailored according to the user’s age, gender and location. However, the self- declaration does not clearly specify what inappropriate content is.

Arto does not refer to the ways in which this service provider promotes the uptake of parental controls in its self-declaration.

Main findings in relation to the website

During the testing it was easy to sign up at the SNS stating an age below the minimum (10) and there are no precautions made to ensure users cannot use a fake birthday. The sign up process asks every user of Arto (independent of their age) for very little information, requiring only e-mail, date of birth and sex as mandatory. The user is asked to provide an e-mail address, but there is no e-mail verification and it is possible to register with a fake and even non-existing e-mail account.

During the initial testing it was not possible to sign up as a 9-year-old, since the user has to mark a year of birth and the youngest year of birth possible, was 2000[6], therefore the tester signed up as being 10-years-old. Since 2011, however, it was possible to mark the date of birth such as June 2001 and, thus, create a profile of a 9-year-old without even having to fake being older.

According to the self-declaration ARTO has mechanisms through which the SNS ensures limited exposure to potentially inappropriate content, e.g. age determines which categories of content users can access in the forum section. However, in the course of testing it was possible for a 10-year-old to see content such as for example how to use different sex-positions[7] through one of the forums available on the site. Besides, profiles of adults were displayed to minors.

In relation to advertising the testing revealed that when signing in as a minor no inappropriate advertising is displayed on the site. However, the ads displayed are not ”age-specific”, either, as stated in the self-declaration. For instance, e-commerce ads were displayed from online hotel reservations, clothes, travels (Copenhagen-Aahus), Air France, phone companies and rental appartments, plus banner ads for butter and a gym. When signing in as an adult the same ads were displayed plus a banner for online games.

The testing also confirmed that Arto does not encourage the uptake of parental controls. There are no tools that allow parents to manage their children’s use of the service or to monitor their child’s activities on the SNS.

[6] https://skitch.com/ditte/r8qye/9-years-old

[7] https://skitch.com/ditte/r8qb3/arto-klubber

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

As stated in the self-declaration, Arto provides several mechanisms to assist children and young people in managing their experience on their service, including the possibility to set up an age bracket so that only people within that age bracket can contact the user, block other users or delete messages on their profiles.

According to the self-declaration, profiles of minors are not set to private by default, however Arto ensures that only very little and basic information (name, age and area of residence) is displayed in the users `profiles and the user may change their settings at any time.

Arto claims it supports the safety education of parents by providing them with targeted safety information and links to relevant external institutions.

Main findings in relation to the website

The test revealed that minors are allowed to add adults to their contact list without any restrictions, warnings or safety guidance. An adult can also contact a minor without any problems and the profiles are not private by default. Although the profiles at ARTO (of both minors and adults) are not searchable via search engines such as Google, they are easy to find through the internal SNS search.

Contrarily to what is stated in the self-declaration, the default settings of minors at ARTO allow both registered and non-registered users of this SNS to view much more than only "basic information" of minor users including their real name (first and last), age, gender, political views, education, nationality, likes and dislikes, hobbies, place of residence, place of school, pictures, lists of contacts, relationship status, applications and guestbook, online status as well as when the user was online for the last time. Users can set their profile to "private". However, setting one`s profile to private does not prevent other registered users from viewing this detailed personal information. Besides, any registered user can still be contacted by any other registered user regardless of whether their profile is set to private or public. A non-registered user can view all the things mentioned above, but cannot contact a registered user through their profile. By default, Arto users can be posted comments/content and be contacted by "everybody", i.e. all Arto users, except by the ones who have been "blocked". Still users can change these default settings and select if they want to be contacted by 1) everybody 2) age bracket (by default 12-99 years old) plus my friends or 3) only my friends. Arto users can easily reject friendship – in every friendship request, there is a button for accept or decline.

There is no option for moderation of content or comments before they are published on the profile. However, it is very easy to block an offending user by clicking on "block this person" in every message and on every profile. The blocked user is still able to view all the content of the profile, but cannot contact the user who blocked them. It is easy to delete postings and pictures on the users' own profile, but a user cannot delete own postings on other users profiles if they wish to do so later on.

It is not possible to delete a profile – only deactivate it and ARTO keeps all of the information. In "settings" there is a well prominently placed button that makes it is easy to deactivate the account. However, if the user logs into the account again, the account automatically re-activates and the user is not informed of this.

Arto does not provide information/tips for parents on the benefits of using parental control tools (e.g. filtering software, etc.).

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service

Main findings in relation to the self-declaration

According to its self-declaration, Arto provides a number of mechanisms for users to report inappropriate content, contact or behaviour. Reporting can be done via the "Reporting button" or via the support tool, both accessible everywhere on the site. Arto has a tool that can also request more information on the incident, if needed; or simply inform the user that the matter has been dealt with. Arto deals with reports from users depending on their urgency, being inappropriate sexual behaviour and sexual predators the most urgent one.

The self-declaration does not specify if the reporting mechanisms are easy to understand for children or if they are age-appropriate.

Main findings in relation to the website

As part of this study, a (fake) minor user reported that she had been bullied on this SNS. A realistic bullying situation was set up between the (fictitious) owners of profiles that were created for this assessment. The scenario consisted of one minor being bullied by two other minor users who posted a nasty comment on the public guest book of the "victim" and who uploaded a hurtful picture. As the "victim" could not cope with the nasty comment put on her profile and the embarrassing pictures, she contacted the provider on December, 25th, 2010. Arto provides two prominent reporting mechanisms, namely by contacting Support directly or by clicking on the report button. For this test the reporting button was chosen. The "report" button takes the user to the report section, where the user has to confirm three times that s/he wants to report the other user. Hereafter the user can choose between 10 predefined categories (e.g."inappropriate contact between old and young user" and"sexual harassment"). Reporting abuse was easy and the "victim" was provided with all of the information needed to make an effective report. Within 1½ hours the "victim" was contacted by the Support of ARTO who stated that the profile of the offender had been deleted. They also recommended the "victim" to use the "Filter" button in "settings", but this button was not active at the time of the test and so was neither the "un-friend" button. As informed by the Support, the profile of one of the two "bullies" (created for this test) was effectively closed immediately. However, the "bully" did not receive any warning or explanations of why this had happened. Nevertheless, the bully could sign up again on Arto even with the same e-mail address he had previously provided. Strangely, nothing happened to the second "bully".

In sum, the instructions on how to use the report mechanism are easy to understand and clearly worded for a minor, reporting is quite easy and straightforward; however the reactions of the service provider are inconsistent and inefficient: On the one hand, only one of the "perpetrators" was "punished" by having his/her account closed. On the other hand, it was possible for the "banned" minor to sign up again on the site without any difficulties and without even having to change any personal details.

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

According to its self-declaration, in case of being informed of illegal actions on the site, Arto immediately closes the profile in question but only after having verified the validity of the report. If able to gather enough information on the incident, Arto will also compile a report (including a summary of the incident plus any information entered by the user involved, e.g. e-mail, name, IP address, pictures, logs of the user's correspondence on the site, etc.). All this information is then sent to the NITEC (the Danish Center for National IT investigation).

Arto claims that it counts with a review tool that allows them to review large amounts of pictures at the same time and instantly remove the content that does not follow Arto`s guidelines. Arto may share relevant information on a user with the police and the NITEC (Danish Center for National IT investigation), but only in relevant cases that are accompanied by a court order.

Because of ethical reasons, Principle 5 was not tested in the website.

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

Main findings in relation to the self-declaration

According to its self-declaration, users of Arto are provided with a range of privacy setting options and with supporting information to help them make informed decisions about the information they post online. Indeed, according to Arto self-declaration users are "in complete control of what information they wish to share through their profile, profile picture or gallery, and may customize the layout if their profile to include-or not include-their profile information and other widgets holding their personal information".

The self-declaration does not specify if users are provided with any supporting information to help them make informed decisions about the information they post online. Arto does not include information on if users' information (provided during their registration) is automatically uploaded onto their profiles, either.

Main findings in relation to the website

The testing found that even though very little information is asked for in the process of signing up, the information entered during and after registration is automatically inserted into the profiles of minors and is displayed in the news stream at the front page at the profile. If the user wishes to conceal certain information such as their relationship status, then the widget in question must be removed.

Privacy settings are easy to find and use by minors and are accessible at all times. However, these settings are not granular; hence the user does not have the option to display only certain type of information to specific people. Either the user displays the information to everybody or must delete it. As stated earlier on, it is very easy to block a person from contacting the user – writing privately and posting comments/pictures – but it is not possible to block them from viewing the content of a profile.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

Main findings in relation to the self-declaration

According to the self-declaration, Arto assesses their service to identify potential risks to children and young people through diverse mechanisms including monitoring the site for inappropriate and illegal content and conduct, employing chat robots, approving uploaded content, manually checking all media, pictures and videos uploaded to the site, etc. Arto also counts with a Filter that searches for harmful or unwanted terms. Via this filter Arto can quickly review messages sent from the user and can determine if the messages were really meant to hurt other users in an efficient way. Arto can also generate chat logs in case suspicious communication between two users may have to be reviewed.

Principle 7 was not tested in the website.

Summary of Results and Conclusions

Arto has implemented Principles 1 and 4 rather satisfactorily and Principles 2, 3 and 6 unsatisfactorily on its website. The testing on the website revealed several problematic areas, for instance:

- Profiles of minors are not set to private by default, nor is it possible to make your profile private as either the user displays the information to everybody or must delete it.
- According to the self-declaration ARTO, age determines which categories of content users can access in the forum section. However, in the course of testing it was possible for a 10-year-old to see content such as for example how to use different sex-positions through one of the forums available on the site.

- The test revealed that minors are allowed to add adults to their contact list without any restrictions, warnings or safety guidance. This is because in Arto any registered user can be contacted by any other registered user.

- The testing also confirmed that Arto does not encourage the uptake of parental controls. There are no tools that allow parents to manage their children's use of the service or monitor their child's activities on the SNS.

- It is not possible to delete your profile, but only to de-activate it.

Assessment of all the Principles in the Self-declaration

Principle	*Very satisfactory*	*Rather Satisfactory*	*Unsatisfactory*
1			x
2		x	
3		x	
4		x	
5	x		
6			x
7	x		

Implementation of the Self-declaration on the SNS

Principle	*Very satisfactory*	*Rather satisfactory*	*Unsatisfactory*
1		x	
2			x
3			x
4		x	
6			x

BEBO

Simon Grehan, NCTE, Ireland
Verónica Donoso, Appointed Research Coordinator by the EC

Introduction

Bebo is an online community where members can find and communicate with others as well as browse and share user-generated content. Users interact with friends' profiles, send messages to other users, join groups, become fans of bands, use third party applications and games, and upload and share photos and videos. Users must be 13 or older to use Bebo. Users can add their AOL Instant Messenger (AIM), Skype and Windows Live Messenger user names to their Bebo profile.
Bebo was founded in 2005, it operates globally and many different languages but is most popular in Ireland, the United Kingdom and New Zealand. AOL acquired the site from its founders in 2008 and they subsequently sold it to Criterion Capital Partners in 2010. Figures from marketing firm comScore show the monthly users in February 2010 were 3.8 million.

The following is a report of findings of the analysis of the self-declaration provided by Bebo and the testing of its website. The test was conducted in December, 2010 – January, 2011.

Summary of main findings

The self-declaration provided by Bebo is in-line with the Safer Social Networking Principles and the implementation of its self-declaration in Bebo website is quite satisfactory.

Bebo provides safety information for parents, teachers and young users. Most of the information is developed by third-party organisations and either hosted on or linked to from the Bebo website. The general safety information is easy-to-find and easy-to-understand. The footer containing links to Safety, Privacy and Terms of Service is available on all pages within the site.

Users are required to provide basic information about themselves during registration. Profiles of minors are set to private by default. Once registered there are optional fields for them to enter more personal information including details of the user's home address, relationship status, and mobile phone number. Users are able to access and alter their privacy settings at any time. Some context sensitive advice is given in to help minors make appropriate decisions about sharing their personal information.

Bebo has implemented several measures on its website to avoid that minors are confronted with inappropriate content. However, it appears that the advertisements displayed are not always selected based on the profile of the user. For instance, one of the advertisements displayed was for a dating site that requires users to be at least 18 years old to join.

Bebo provides mechanisms for reporting inappropriate content, contact or behaviour on users' profiles and beside photo and video modules on the site. However, as the testing shows, even though the reporting mechanism is user-friendly it proved to be quite ineffective. Indeed, even though the "victim of bullying" did receive an acknowledgement that her report had been received, no further actions were taken by the provider and, thus, the "bullying" pictures and messages created for this test remained on the site and the bully did not get any warnings.

Analysis of Results by Principle

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner

Main findings in relation to the self-declaration

According to its self-declaration Bebo provides clear guidance for children and young people on how to navigate their website safely. Safety pages include animations and relevant information on various relevant safety-related topics including bullying, privacy, etc.

Bebo states that they provide information about Terms of service, (un)acceptable conduct and the consequences thereof in a prominent, accessible and age-appropriate way. This information is specially targeted at children, parents and teachers.

Although the self-declaration indicates that Bebo offers targeted educational materials and tips for parents (e.g. Know it All for Parents and ConnectSafely), it is not explicitly mentioned if Bebo provides parents with technical any controls (e.g. parental filters) to support a safer and responsible safer internet use by children.

Main findings in relation to the website

Confirming the analysis of the self-declaration, Bebo provides targeted safety information for parents, teachers and young users. The general safety information is easy-to-find and easy-to-understand. The safety information is linked to directly from the footer of the homepage. The footer containing links to Safety, Privacy, and Terms of Service is available on all pages within the site. There are step-by-step ‘how to’ instructions in the Help section of the site detailing how to configure all aspects of the Bebo site including how to configure user profile settings to facilitate a safer experience on the site. The site also provides graphic and audio animations with Bebo-specific advice and general internet safety awareness raising videos that have been developed by third-party online child protection initiatives.

The code of conduct for young users is not explicitly stated but rather contained in the animated instructional pieces on the Safety page. The content for teachers has been developed by third-party organizations and hosted in the Bebo Safety section. The parenting information is linked to from the Bebo Safety section and hosted on the local internet safety awareness site.

The Terms of Service (TOS) are linked to from the footer of all pages. It is a long document (4400 words). Although efforts have been made to use plain language, it is still a quasi-legal text with technical terminology throughout. The TOS explicitly defines the types of content that if upload could result in the user's account being terminated.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience

Main findings in relation to the self-declaration

As specified in their self-declaration, the minimum age registration requirement in order to subscribe to Bebo is 13. The measures taken by the provider in order to identify and delete under-age users include textual searches to identify under age users, asking for birth dates during registration and employing cookies. Upon discovery that a user is younger than 13, Bebo deletes their account.

Bebo refers to diverse human and automated mechanisms through which the service provider ensures limited exposure to potentially inappropriate content and contact for children, for instance, by providing a Report Abuse button, by ensuring that age-restricted content is not viewable by children of certain ages, by scanning all hosted images for potential pornography; etc. As stated in the self-declaration, inappropriate URLS are blocked from the site. Bebo also claims that professionally produced content follows applicable laws and regulations to "ensure that content is age-appropriate" so that, for instance, moderate sexual or violent content should be provided with guidelines and strong sexual or violent content should be "age-restricted" (i.e. not viewable by users below a certain age).

The self-declaration does not provide information on the ways in which this service provider promotes the uptake of parental controls to allow parents to manage their children's use of the service.

Main findings in relation to the website

As stated in the self-declaration, Bebo relies on self declaration of age by the user in the registration process as the key mechanism for ensuring that only children over 13 can become members of their website. When trying to register as a 9 year-old permission was denied and a cookie was placed on the machine preventing re-registering as older from that machine until the cookie was removed. Bebo does not have any parental control mechanisms.

Confirming the analysis of the self-declaration, when logged in as a minor in Bebo no strong sexual or violent content was displayed. In the case of commercial content, most of the content-displayed is age-appropriate. Banner and right-column advertisements were displayed on minors` homepage. When visiting other pages on the site a third advertising space on the left-column was used. These advertisements changed every time the page was refreshed; usually these adverts were for mobile phone companies and internet service providers. However, Google Ads, advertisements for online games and advertisements for adult dating sites also displayed on occasions. It appears that the advertisements displayed are not selected based on the profile of the user. One of the advertisements displayed was for a dating site that requires users to be at least 18 years old to join.

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

In its self-declaration Bebo refers to a wide range of tools and technologies employed by the service provider to assist children and young people in managing their safe experience on the service. These include: all profiles are private by default. "Setting up a profile to private means that only 'friends' may view the profile or contact the user"; it is not possible to search for under 16 users via search engines; it is possible to block other users and reject friend's requests; users are able to pre-moderate/review comments before they appear on their profile; users can restrict age range of people able to contact them, etc.

Supporting information about these tools is available to users, teachers and parents from all pages.

Main findings in relation to the website

Bebo have taken measures that can help minimise the risk of unwanted or inappropriate contact between children and young people and adults. As stated in the self-declaration, Profiles of under 16 year olds were not found by searching for them in search engines. Adults registered on the site can only find young users if they know their email address or profile URL, even then the young user must approve their friendship request before they can see their profile.

Confirming what is stated in the self-declaration, minors' profiles are categorized as 'Private' by default on registration, this means that only users that are accepted as friends are able to access the profile or contact them. "Friends of friends" can see Minor1's name, thumbnail photo, hometown, gender, and interests. But if they try to open the minor`s profile the following message is displayed: *"You must be friends with this person to view their profile. Looks like you're not friends with this person yet and their profile is set to private. To see their full profile, invite them to be your friend on Bebo."* Friends of friends can send friend requests, but not personal messages.

Even though minors can configure their account settings to allow everyone to see their profile, there is context sensitive help in the privacy settings section strongly recommending that under 21s should not do this. Age, online status, and how long you have been a member of the site are displayed by default but can be hidden. There are options to make your profile searchable in search engines and to accept game challenges from strangers in Apps. It is possible to block other users and report abuse by clicking buttons on the profile, comment, or photo that offends.

By default, friends can post comments and whiteboards on minor's profiles. They can opt to allow users to post directly to their profile or they can moderate posts by non-friends only by selecting the appropriate radio button in their profile privacy settings.

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service

Main findings in relation to the self-declaration

As stated in its self-declaration, Bebo provides diverse, prominent and convenient mechanisms to report inappropriate content, contact or behaviour that violates their Terms of Service. They provide users with a Report Abuse system that includes, among other functionalities, the presence of Report Abuse links on each profile page, photo album, group and posted application. These links provide different options (remove someone from friends, block user, report abuse or filing a police report).

Bebo claims that they provide clear information and support so that users can make informed decisions regarding when and how to use each reporting option (e.g. by informing users about what information to supply with their report and also telling them how their report will be handled). According to the self-declaration, the reported information is sent to Bebo's abuse management team. They assess the report and if users are "found to be in breach of the Terms they are either issued a conduct warning or have their accounts blocked depending on the severity of the breach."

The self-declaration does not explicitly mention if the reports are acted upon *expeditiously.*

Main findings in relation to the website

Confirming the analysis of the self-declaration, once logged into Bebo, the report abuse link is prominently displayed on most content modules in the site. During the test a (fake) situation was created where one minor bullied another one by means of nasty pictures and comments. To report the bully, it was necessary to go to the bully`s profile page and click on the Report Abuse link under her profile picture. The category of abuse was chosen from a drop-down list. The reporting minor provided details of the harassment in the Reason for Reporting this Member field. She was asked to copy and paste an example of her harassment. This involves navigating away from a half-completed form and loosing the text that had already been inputted. Further, it was required to agree to all future reports being ignored in the case where invalid reports were made. This was done by checking a box on the form. This condition could act as a deterrent to reporting in particular because users are not told what constitutes an invalid report.

As opposed to the analysis of the self-declaration, Bebo did send an "acknowledgement" e-mail to the "victim" but only three hours after having sent the report. An email from Bebo Abuse was received saying that the report had been investigated and that any measures "deemed necessary" had been taken. However, no specific information on the actions taken was given and no report reference was quoted in the email. The offensive content that was reported to Bebo was not removed from the profile and no warnings were received by the user that posted the content. Thus, even though the reporting mechanism is user-friendly it proved to be quite ineffective.

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

According to its self-declaration, Bebo "has arrangements in place to share reports of potentially illegal content or conduct with relevant law enforcement agencies". Bebo claims that these reports are dealt with as "high priority". Bebo also supports the education of investigators about "how to lawfully obtain data from Bebo" (e.g. the UK Home Office`s Single Point of Contact training programme).

As previously mentioned (Principles 2 and 4), Bebo specifies in its self-declaration the mechanisms employed to identify, review and eventually remove offending content via both automated (e.g. scanning software) and human-based mechanisms.

Because of ethical reasons, Principle 5 was not tested in the website.

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

Main findings in relation to the self-declaration

As stipulated in its self-declaration users in Bebo can manage their personal information and privacy through a wide range of privacy options including, among others, the possibility to choose if one`s profile is viewable by "Everyone" (public) or to "My friends only" (private); whether one`s age is visible on their profile or not (by default not visible if date of birth is under 16) as well as being able to decide the minimum and maximum age of members who can contact them; etc.

According to the self-declaration, users are able to access and alter their privacy settings at any time – either via a link situated in a prominent place at the top of every page on Bebo, or via the 'edit profile' link underneath their photograph on their profile page. Details provided during registration are not directly mapped onto the user's profile, for instance the name provided during registration is not the user`s full name.

Main findings in relation to the website

All the privacy settings are located in the one place (Privacy Settings). These setting can be accessed at any time by clicking the Setting link on the header on all pages. They can be changed by selecting radio buttons and check boxes and saving the settings. There are only 12 options on the page, all are described in simple English. As stated in the self-declaration, users can toggle their profile between public and private. Users can also specify an age range for non-friend members that can see their profile. They can decide to hide some of their personal information such as age and profile views and to allow their profile to be found in search results. There is context sensitive advice recommending the friends only setting to minors. It is possible for users of any age to alter their privacy settings at any time. Also, even with their profile categorized as 'Public' it is also possible for Bebo users to block other users and configure their account to allow only 'friends' to post comments on their profile and can delete unwanted comments before they are published on their profile.

The testing showed that it is possible for Bebo users to cancel their membership. Details on how to do it are contained on the 'Settings' link on the navigation bar on any page. The procedure is straightforward. You simply have to click the 'cancel your membership' link located at the bottom of the 'Settings' page. You then click the YES button to actually cancel your membership. During the membership cancellation process, the tester was prompted "Cancelling your account will remove your details from Bebo. You will receive no further emails from us. This process can NOT be reversed." This seems to indicate that personal information is deleted (and not just deactivated) although it is not clearly stated.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

Main findings in relation to the self-declaration

In its self- declaration, Bebo states that they have established both “proactive and reactive means to identify potential Terms of Service violations” including “prominent and convenient ‘Report abuse’ mechanisms” and searching for inappropriate content (e.g. by scanning the Bebo site for potentially illegal content). The potential violations identified, including illegalities, are analysed and processed (See Principles 4 and 5).

Principle 7 was not tested in the website.

Summary of Results and Conclusions

Bebo has implemented Principles 1, 2, 3 and 6 very satisfactorily and Principle 4 rather satisfactorily. Some areas of attention include:

- Even though the reporting mechanism is user-friendly and users are sent an acknowledgement that their reports have been received, still the reporting mechanism proved to be quite ineffective.
- There is no way for non-members of the site to access the report abuse function.
- The advertisements displayed are not always selected based on the profile of the user.
- Simplifying The Terms of Service (TOS) so that they are easy-to-understand for younger audiences.

Assessment of all the Principles in the Self-declaration

Principle	*Very satisfactory*	*Rather Satisfactory*	*Unsatisfactory*
1	x		
2	x		
3	x		
4	x		
5	x		
6	x		
7	x		

Implementation of the Self-declaration on the SNS

Principle	*Very satisfactory*	*Rather satisfactory*	*Unsatisfactory*
1	x		
2	x		
3	x		
4		x	
6	x		

FACEBOOK

Cédric Fluckiger, University of Lille 3, France (tester French version)
Simon Grehan, NCTE, Ireland (tester English version)
Verónica Donoso, Appointed Research Coordinator by the EC

Introduction

Facebook is an online community where members can find and communicate with others as well as browse and share user-generated content. Users interact with friends' profiles, send messages to other users, join groups, become fans of pages, use third party applications and games, and upload and share photos and videos. Users must be 13 or older to use Facebook. Users can communicate synchronously with other users using the Facebook chat application.

Facebook was founded in 2004. It operates globally and in many different languages. Facebook is the most used social networking site in the world. According to Facebook there are more than 500 million active users and 50% of the active users log on to the site on any given day.

The following is a report of findings of the analysis of the self-declaration provided by Facebook and the testing of its website. Facebook was tested in Ireland (English version) and in France (French version) in December 2010 - January 2011.

Summary of main findings

The self-declaration provided by Facebook is overall in-line with the Safer Social Networking Principles. The implementation of its self-declaration in the website is rather satisfactory in both the English and the French versions of the site tested. In both language versions users may report photos, messages or persons, using the report abuse link, prominently displayed on most content modules on the site. Even though the available Reporting mechanisms are easy to use, the testing in both the English and the French versions of Facebook revealed that Facebook does not react expeditiously to user`s reports of inappropriate content/contact.

In terms of users' privacy, both versions of Facebook require users to provide only basic information about them during registration. Once registered, users may enter additional personal information. The tests in both versions of the site confirmed what is stated in the self-declaration, namely, that the profiles of minors are accessible not only by contacts in the users' contact`s list, but also by other Facebook users such as "friends of friends" and networks. Thus, one can conclude that profiles of minors are not set to "private by default[8]" as defined in the Safer Social Networking Principles[9]. However, Facebook suggests "Recommended Privacy Setting" for minors where mobile phone number, home address, and email address are restricted only to friends. The "Recommended Privacy Settings" are implemented by default when minors set-up a profile.

When signed in to Facebook as minor, some of the adverts displayed on the profile could be considered as inappropriate.

[8] "Ensuring that setting a profile to private means that the full profile cannot be viewed or the user contacted except by 'friends' on their contact list" http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

[9] For a full description of each of the Safer Social Networking Principles, please consult: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

In both versions, Facebook provides targeted, easy-to-understand safety information for parents, teachers and teens through the Help Centre available on the footer of all pages. The footer also contains relevant links to the Privacy Centre and the Terms of Service. However, more links to external web sites, resources or organizations are available in English than in French.

Analysis of Results by Principle

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner

Main findings in relation to the self-declaration

In its self-declaration Facebook states that they provide guidance, information and educational materials specifically targeted to children and young people on how to navigate their website safely through their Safety and Security pages. Additionally, Facebook claims it provides on every page a link to the "Statement of Rights and Responsibilities" of users. These Terms have been simplified in the "Community Standards" so that they are easy-to-understand for users of any age.

The self-declaration neither provides explicit information on what constitutes inappropriate behaviour on the site nor information on the actual consequences of breaching the Community Standards. However, it does provide links to relevant information on the Facebook site where this information can be found. The self-declaration does not give any information on if the website offers parents and/or teachers technical controls (e.g. parental filters) that support their involvement in the safer and more responsible internet use of their children, although it does provide general safety information specifically targeted at them.

Main findings in relation to the website

According to the test results and confirming what is stated in the self-declaration, Facebook in Ireland (English version) and in France (French version) provides targeted safety information for parents, teens, educators and law enforcement through the Facebook Safety page linked to directly from the Help Centre available from the footer of all pages. The footer also contains links to the Privacy Centre and the Terms of Service. Step-by-step 'how to' instructions are provided in the Help Centre section of the site detailing how to configure all aspects of the Facebook site including how to configure user profile settings. There is some preventive advice for teens on how to be safer on Facebook (e.g. how to report abuse on the site) as well as links to a Guide to Privacy on Facebook, Statement of Rights and Responsibilities, information on reporting abuse and several FAQs. The content for teachers and parents is comprehensive and contains links to information hosted by third-party organizations. The Safety Centre contains advice tailored to teen audiences and links to appropriate external resources. However, it was not possible to find information about the Hotline neither in Ireland nor in France.

In both the English and the French versions of Facebook, the Statement of Rights and Responsibilities outlines what Facebook considers as inappropriate behaviour on the website. The consequences of breaching these terms are included here as well as in the Privacy Help section. This information is appropriate, especially for adults, but certain parts may be difficult to understand for teenagers especially because of the use of long and complicated sentences.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience

Main findings in relation to the self-declaration

In its self-declaration Facebook states that the minimum age requirement is 13 years old. When signing up users are required to provide their date of birth to establish their age. Facebook also mentions that it employs cookies to make re-registration difficult and that it makes use of analysis of friends' connections by age to identify (and eventually correct or delete) profiles of users suspected to have provided a wrong age. Content on Facebook can be age-restricted via “built-in tools” and applications; however, no further specifications are made regarding what these tools are or how they work. Special restrictions are placed on advertising targeted to minors.

Facebook does not make clear when services are not appropriate for children and young people or where a minimum registration age applies. It only provides information on the mechanisms employed to restrict certain types of content to certain age groups such as “inappropriate advertising”. Specific information on what is considered as inappropriate content or advertising is provided via a link to the Advertising Guidelines http://www.facebook.com/ad_guidelines.php and the Platform Policies (http://developers.facebook.com/policy), however this information is not explicitly mentioned in the self-declaration.

No information is found on the ways in which Facebook promotes the uptake of parental controls to allow parents to manage their children’s use of the service.

Main findings in relation to the website

In both the English and the French versions of Facebook Statement of Rights and Responsibilities, it is clearly stipulated that the minimum age requirement is 13. As mentioned in the self-declaration, both versions of the site show that Facebook relies on self declaration of age by the user in the registration process as the key mechanism for ensuring that only children over 13 can become members of their website. When trying to register as a 9 year-old permission was, indeed, denied and it was not possible to immediately re-register as older from that machine. However, it was possible to immediately re-register once the browser (Firefox in both cases) was closed down and reopened, showing that the cookies had been removed.

Both in the English and the French versions of Facebook, the parental advice in the Safety centre states that it cannot allow parents to monitor or access the accounts of their children but it does encourage parents to engage with their children's activities on the site and provides information and advice to support this process. Furthermore, no parental control devices were found on any of the language versions tested.

When signed in to Facebook as a minor, advertising was displayed on the right-column under the subheading “Sponsored”. For instance in the English version, four adverts were displayed; one for fast-food, one for a celebrity gossip blog, one for a competition to win a €500 shopping spree in a local department store, and one for a virtual card game (Blackjack Extreme). When clicking on the Adverts that appeared to be for a celebrity gossip blog (Rihana or Fake?), it opened a video chat application called Rounds. This application opened the tester`s webcam and prompted the tester to “call a friend or meet someone new”. When the option “meet-someone new” was clicked the tester was informed that it was necessary to “have at least 100 friends on Facebook to join a random Round”. In the French version one of the ads about a game warned users that the game was “very addictive” and that it had been banned in the US. No ads about alcohol or tobacco adverts were found during the testing in any of the language versions of Facebook tested.

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

In relation to its self-declaration, Principle 3 has been rather satisfactorily assessed. Facebook refers to several mechanisms to empower users through the use of specific features implemented on its website. For instance, all users can control what individual friends can see or block specific people entirely. From the Account tab on every page users can always access their privacy settings and, supporting information and clear guidance on how to use these settings is provided. Furthermore, Facebook users have “granular control over every piece of content they create”. This means that users can share their content on the site with specified users or to delete individual pieces of content at their own will.

In the case of users ages 13-17, they have more restrictive default privacy settings than adults, although they cannot be considered as "*private by default*"[10] because they include "friends", "friends of friends", and "networks" which goes beyond the "user's approved contact list". Other mechanisms worthwhile mentioning are that users ages 13-17 cannot be found by external search engines (e.g. Google) and the geo-location product "Places" which limits the visibility of users younger than 18 to confirmed friends only.

Facebook offers safety information and tips for parents in order to help them protect children and young people, but no information on parental control tools is found anywhere in the self-declaration.

According to its self-declaration, Facebook regularly assesses the mechanisms to detect and remove inappropriate content or contact and its reporting mechanisms are continuously evaluated by senior management and through internal reports on their effectiveness.

Main findings in relation to the website

Both language versions tested show that Facebook has taken measures that can help minimise the risk of unwanted or inappropriate contact between children and young people and adults. Although not "*private by default"*, profiles of minors were not found by searching for them in search engines such as Google or Bing. In general, adults registered on the site can only find minor users if they know their email address or profile URL. Even then the young user must approve their friendship request before they can see their profile. However, if an adult user if befriended with a minor, the default profile settings of the minor allows all the adult`s friends to have access to the minor`s profile, except the contact information. Still, it is possible for the adult`s friends to send the minor private messages and friends` requests.

By default in both language versions tested, not only (adult) users that are accepted as friends are able to access the profile or interact with minors, but also their friends. While there are three general privacy settings that restrict access to all your information to either "friends", "friends of friends", or "everyone", it is possible to create a customised privacy setting by defining access rights to each information element. This is a straight-forward but time-consuming process. It is possible to block other users and report abuse by clicking buttons on the profile, comment, or photo that offends. Users can also delete unwanted content, unwanted comments and restrict access to their profile.

As stated in the analysis of the self-declaration, Facebook does not provide information about available tools to help parents protect their children online. However it does link to third-party sites that provide this kind of advice (although mostly in English), and also provides parents with general safety information (Principle 1).

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service

Main findings in relation to the self-declaration

Facebook provides abuse reporting buttons to report content or behaviour on almost every page of its site. On every video, picture or comment users have the opportunity to report content. However, the self-declaration does not explicitly mention if this procedure to report inappropriate conduct or content is age-appropriate or easily understandable for younger users. Users can also report unwanted or inappropriate contact or messages from other users and also block other users even if they are not friends.

[10] As stated in Principle 3 in the Safer Social Networking Principles.

According to its self-declaration, Facebook has developed sophisticated technology to prioritise and process notifications from users, which area managed by a dedicated team working 24/7. The self-declaration does not mention if these notifications are acted upon expeditiously or if reports are acknowledged. It also does not include any information on if users are provided with the necessary information they need to make an effective report, or if users are provided with an indication of how reports are typically handled.

Main findings in relation to the website

Once logged into Facebook, the report abuse link is prominently displayed on most content modules in the site. The Safety Centre provides information for teens, parents, and educators on how to use the reporting mechanisms. The easiest method for reporting abuse for Facebook users is to use the "Report" buttons that appear near the content itself (e.g. photos, messages, comments on the wall, etc.). There are also Report abuse forms available for people without a Facebook account, but they can also be employed by users. These report abuse forms are very difficult to find because no links to the forms are provided in the Safety Centre. However by searching for "how do I report abuse with no account" in the Help Centre it was possible to find report abuse forms to report users, photos, abuse in general, etc. In order to submit these forms all entries in all fields must be filled in; however some field labels may be rather difficult to understand especially for younger users (e.g. "URL (web address link) of the violating content" or the "description and steps to reproduce the issue fields").

During the testing, in both versions of the site a bullying situation was set up where one minor posted a bullying picture and nasty comments on another minor`s profile. In both sites the "bully" posted an offensive photograph with some accompanying nasty comments on the wall of the victim. The "victim" reported the incident by clicking the "report this photo" button underneath it. This brought a pop-up window with a list of options (e.g. "Nudity or pornography"; "Graphic violence" and "Attacks an individual or group"). The "victim" chose one of these options and received an acknowledgement that the report had been received. The bullied minor got no further communication and the content was not removed from any of the sites tested. The same happened when the "victim" used the "report a message" link to report one of the nasty comments received.

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

In its self declaration Facebook indicates that they have developed sophisticated technology to prioritise and process notifications from users, which are managed by a dedicated team 24/7 around the globe, however the service provider does not explicitly mention if these notifications are *expeditiously* reviewed or if offending content is quickly reviewed and, eventually, removed.

Even though Facebook has implemented real-time blocking and reporting systems based on lists on known internet URLs hosting child abuse images (provided by the National Center for Missing and Exploited Children in the U.S. (NCMEC)), the self-declaration does not specify how Facebook deals with other types of offending content.

Facebook has dedicated staff for responding to and working with law-enforcement in Europe. They also provide specific guidance in the Safety Centre for law-enforcement officials.

Because of ethical reasons, Principle 5 was not tested on the website.

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

Main findings in relation to the self-declaration

Facebook states that minors on Facebook have more restrictive privacy default settings than adults while all users can access a wide range of privacy settings on every page from the Account tab. According to the self-declaration, these settings are accessible at all times ensuring that users are in full control of what they share and with whom.

Through the Privacy Centre, accessible from every page, users can learn about privacy (settings) by means of easy-to-understand explanations and videos that demonstrate how to change one`s privacy options. There is also a Facebook Safety Page for users that provides regular tips and hints on how to stay safe (e.g. anti-bulling messages). Facebook also engages with a number of NGOs to help promote online safety messages.

Facebook neither specifies if they have taken into consideration the implications of automatically uploading information provided by users (during registration) onto their profiles nor if they notify them that this is happening. However, users are allowed to edit and make public/private the information (provided during registration) that is automatically uploaded onto their profiles.

Main findings in relation to the website

In both language versions of Facebook, the testing revealed that personal information specified by minors during registration is automatically mapped onto their profile (without being explicitly told that this would happen). However, the visibility of such information to other users depends on the privacy settings chosen. By default, in the case of minors, this information is available to friends, friends or friends and networks. Contact details, however, are only available to friends.

In both language versions of the site, Facebook provides a link to the Privacy section which contains both a guide on how to control access to your information on Facebook and videos demonstrating the settings that you can configure. However, when a user creates an account, they are not encouraged to visit the privacy settings page. In both language versions of the website, all the privacy settings are located in the Privacy Settings section. There are three general privacy settings that restrict access to all your information to either “friends”, “friends of friends”, or “everyone”, but, as mentioned in Principle 3, it is possible for users of any age to customise their privacy settings at any time. Facebook also suggests “Recommended Privacy Setting” for minors where mobile phone number, home address, and email address are restricted only to friends. The “Recommended Privacy Settings” are the default settings for minors.

As part of the testing, a fake user account had to be deleted. The test revealed that both in the English and the French versions of the site both deactivating[11] and deleting profiles permanently is possible. Deactivating a profile is quite straightforward and can be done from the “profile” page. Deleting a profile is less easy because it is difficult to find the “Ask for deleting” link.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

Main findings in relation to the self-declaration

According to its self-declaration, Facebook regularly assesses ways of optimizing its systems to detect and remove inappropriate content and conduct on the site and continuously tries to improve these systems especially to allow users to report conduct or content on the site, as well as to develop automated systems to identify ‘bad’ users or content. Internal reports on the effectiveness of these systems are permanently reviewed by senior management at Facebook to ensure the continuous improvement of such tools.

Facebook liaises with external agencies such as the IWF in the UK or the OCLCTIC in France to support the identification of prohibited content.

Principle 7 was not tested on the website.

[11] Deactivating a profile means that the information is no longer visible to users although it remains in Facebook database in case one wants to reactivate the profile later.

Summary of Results and Conclusions

The testing of Facebook website has demonstrated that Principle 1 has been very satisfactorily implemented on its website while the rest of the Principles have been rather satisfactorily implemented. Areas of attention on Facebook website include:

- Reports of inappropriate content/contact are not answered.
- Profiles of minors are not set to "private by default". This means that profiles of minors can be accessed not only by their friends but also by the friends of their friends and networks.
- Some advertising can be considered as not appropriate for minors.
- The mechanisms to avoid re-registration of underage users are inefficient.
- Lack of information on existing parental control mechanisms, e.g. the benefits of employing filtering software.
- Not all the sections in the Terms of Use are easy for children to understand.
- Lack of concrete information, especially targeted at children, on the consequences of breaching the Terms.

Assessment of the Principles in the Self-declaration

Principle	*Very satisfactory*	*Rather Satisfactory*	*Unsatisfactory*
1		x	
2		x	
3		x	
4		x	
5		x	
6		x	
7	x		

Implementation of the Self-declaration on the SNS website

Principle	*Very satisfactory*	*Rather satisfactory*	*Unsatisfactory*
1	x		
2		x	
3		x	
4		x	
6		x	

GIOVANI

Giovanna Mascheroni (PhD), Univ. of Torino and OssCom Catholic University of Milano, Italy
Verónica Donoso, Appointed Research Coordinator by the EC

Introduction

Giovani is an Italian SNS held by the Internet Company Banzai. The company has incorporated Studenti Media Group, an internet group born in 2007 which runs other community services targeted to young people such as Studenti.it, and Girlpower.it. Giovani has 2.807.222 registered users, as stated in the top left box on the homepage. The community is age restricted to those younger than 13 years old. The SNS offers users the possibility to create their own profiles, a personal blog, and a photo and/or video gallery. A further feature recently added to the service is the possibility to upload their photo albums on a photo sharing site managed by AltaVista (part of Banzai). Users can also join groups, and participate in discussions in the forum. The forum contains the following threads: Sex; love; news and politics; literature; music; TV and cinema; mobile phones; videogames; computer and the internet; sport; editorial staff forum; helpline; XXX (erotic content X-rated).

The following is a report of findings of the analysis of the self-declaration provided by Giovani and the testing of its website. The test was conducted in December, 2010 – January, 2011.

Summary of main findings

In general terms, Giovani has poorly implemented the Safer Social Networking Principles. On the website, Giovani has implemented a number of safety measures, though not always successfully. For instance, even though the minimum age requirement is 13, the test demonstrated that 12 year olds could register on this SNS without even having to fake being older to comply with the 13+ rule to become members of the site.

Two important weaknesses of the SNS concern the fact that reports on inappropriate content or conduct are inefficiently handheld and that profiles of minors are not set to "private by default". As the test revealed, reports from users are not acknowledged and users get no answer to their reports. Besides, even though inappropriate messages to the user are deleted, other types of content, also reported as inappropriate, are not.

Even though the profiles of minors are not set to private by default, users still have the possibility to set their profile as semi-private (accessible only to registered users or only to friends) or fully private (visible only by the user).

In relation to the safety information available on the site, the Help section provides relevant safety information and concrete tips specifically addressed to children to help them use the SNS safely. It also clearly explains the Terms of Use of the service. Safety information/tips for parents, teachers and carers are also available in the Help section.

Analysis of Results by Principle

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner

Main findings in relation to the self-declaration

In its self-declaration Giovani states that they provide a FAQ and a Helpline that are visible, prominent and linked on the whole social network. The helpline contains "2 sections with behaviour advices and explanations," one section is targeted at users and the other one to parents and teachers. Since the end of June 2010 Giovani counts with a new Helpline and a new Terms and Conditions section written in a clear and age-appropriate language. The new Helpline can be reached through direct links within each page in the Giovani.it site.

The self-declaration does not clearly specify what type of safety content is provided by Giovani, except from the rather vague "behaviour advices and explanations". The consequences of inappropriate behaviour are not mentioned in the self-declaration.

Main findings in relation to the website

Giovani has implemented a Help section (linked in the footer, and in each page of the profile) which contains information and tips for both children and parents/teachers/carers. In particular, the 'under 18's' page is targeted to children and contains relevant safety information and tips on inappropriate content and behaviour that violates the terms of use, and the consequences of engaging in prohibited behaviour; information on how to report an abuse; information on how to modify the privacy settings and on how to safely use the SNS. Specific risks mentioned include: pornography, sexting, grooming, violent or hate content, divulging personal information, spam, viruses and other commercial risks. The language used is plain, and although the information is only textual, it is articulated in short pieces of text that make reading easier. Bold characters facilitate skimming and help identify relevant information. Parents, teachers and carers are provided with information on safer internet use and with links to organizations and authorities active in promoting children's online safety.

The Terms of Use and Privacy Information are also accessible from the footer in the homepage link to the Studenti Media Group policies. They are written in a technical jargon and are, thus, difficult to understand for children.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience

Main findings in relation to the self-declaration

The self-declaration mentions that Giovani is targeted to young people aged 14-25, but it is not explicitly mentioned what the minimum age requirement is. According to its self-declaration to sign up to Giovani users need to provide their date of birth.

Giovani claims that underage users are placed in a "special user group" whose public behaviour, connections and profiles are daily controlled. However, the self-declaration does not specify how this is actually done. Further, no other (technical or legal) mechanisms to ensure the limited exposure of minors to potentially inappropriate content and contact are mentioned. No information is provided on the types of services that are considered as not appropriate for children and young people, either.

It is not clear from the self- declaration if or how underage users are prevented from registering on the website or what measures are taken by the provider in order to identify and delete under-age users from their services. Besides, no information is provided regarding the ways in which Giovani promotes the uptake of parental controls to allow parents to manage their children's use of the service.

Main findings in relation to the website

As opposed to the self-declaration, the Terms of Use in the Help section clearly indicate that only children aged 13 or older can become users of the SNS. Compliance with age restrictions is promoted in the registration process, where the date of birth field is pre-fixed and contains 1998 as the youngest option. Interestingly, at the time of testing (December 2010) all children born in 1998[12] were still 12 years old and, thus, below the

[12] Since February 2011 the youngest option has been modified to 1997. However this report refers to the findings from the period December 2010 - January 2011.

minimum age requirement, however, they were still able to become members of Giovani without even having to fake being older to comply with the 13+ rule to become members of the site.

When signing up to Giovani a disclaimer advice appears, and children have to guarantee they are assisted by parents in order to complete their registration (which is completed only after clicking on the verification link sent via email). The main limit of an age verifications system as the one described is that younger users can pretend being older and being assisted by their parents. The tester's attempt to register as a nine years old failed because she could only pick 1998 as the youngest date of birth. However, neither additional information to prove the child's true age was required nor any confirmation by parents (e.g. to send a fax or email to the SNS). Eventually, it was possible to register as a 12 year-old by simply picking 1998 (or any other one listed) as the year of birth.

As stated in the self-declaration, Giovani does not provide any parental control mechanisms, but the Help section targeted to parents and educators suggests the use of parental control software. However, it provides no links to external educational resources or websites where the software might be available.

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

According to its self-declaration Giovani permanently develops new tools which are quickly communicated to the users, but it neither specifies what these developments are nor in which way they serve to empower younger users. In its latest updated self-declaration Giovani committed itself to implement the following features by December 2010: 1) option to disable the online presence within the user profile page; 2) option to set as private the personal profile of the user and 3) option to set as private the personal blog of the user.

Nothing is mentioned in the self-declaration on the steps taken by the service provider to ensure that private profiles of users registered as under 18 are not searchable. Even though from December, 2010 users should have the option to set their personal profile as private, it is not mentioned if this will be the "default setting" for minors registered on the site.

Main findings in relation to the website

The testing of the site demonstrated that profiles of minors are not se to private by default, and so are by default visible to all users of the SNS. Profiles of minors can even be searched in the SNS search engine by users who are not registered to the community. Non registered users can also visit the minor's profile and access the personal information displayed there. However, these profiles are not searchable via external search engines such as Google. Minors can be searched and contacted by adults with no restrictions. Adults can also send friendship requests and add minors to their contact list without being warned about contacting a child. Minors are able to reject friendship requests, and block other users from contacting them and viewing their profile by adding them to the 'enemies' list. No option to pre-moderate content or comments on the wall is given. The default option is that all registered users can comment on one's profile, but minors can restrict comments on the wall only to their friends, or to nobody.

In the part of the Help section explicitly addressed to them, parents are provided with suggestions on how to help their children navigate safely. These include mainly social mediation strategies, such as telling their children to not give away personal information (such as address, phone number, school); sitting with them while their creating their profiles and checking the hard disk data and using filters to restrict access to X- rated websites.

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service

Main findings in relation to the self-declaration

According to its self-declaration Giovani offers a “Report an Abuse” hyperlink on every relevant page and on those places where users may have access to content provided by other users or where interaction with other users is allowed. Apart from these links, the helpdesk can be contacted. They provide answers daily and check out inappropriate content. There is also a Helpline easily accessible on every page.

No information is provided in the self-declaration on if the reporting procedures are age-appropriate or easily understandable for children and young people. Besides, it is neither mentioned if reports are at all acknowledged nor if they are expeditiously handled.

Main findings in relation to the website

Users can report any inappropriate content, contact or conduct using the ‘report abuse’ form, accessible from the Help section, on a user profile, when reading a message and when viewing other users’ galleries. As part of this study, a (fake) minor user reported that she had been bullied on this SNS. A realistic bullying situation was set up between the (fictitious) owners of profiles that were created for this assessment. The scenario consisted of one minor being bullied by two other minor users who posted a nasty comment on the wall of the “victim” and who uploaded and sent hurtful pictures. As the “victim” could not cope with the nasty comment put on her profile and the embarrassing pictures, she contacted the provider. The tester was able to report an offensive private message by clicking on the ‘Block user and report abuse’ link displayed under the sender’s nickname. To report inappropriate content on the wall, the tester had to click on the nickname of the person posting the offensive message, and then click the report abuse button under the picture of the abuser on her profile, which was not really easy to figure out. Finally the tester reported abuse by clicking on the report abuse button displayed under a photo in another user’s gallery. Independently from where and how the report abuse is accessed, to report any violation of the Terms of Use users have to fill in a form indicating the kind of inappropriate content or behaviour from a pre-filled list (pornographic content; inappropriate/offensive content; unauthorized personal information or photo; offensive comment; violation of copyright). A blank space for adding more details is also provided.

As indicated in the analysis of the self-declaration and demonstrated by the test, reports of misbehaviour and abuse are not acted upon expeditiously: users get no reply and the reported content (message on the wall or picture) is not deleted from the website. Private messages received by the user and reported as offensive have been deleted after more than a week from reporting. Moreover, the reporting mechanism is not user-friendly especially when it comes to deciding which reporting button one should use in each case as, for instance, when the the tester needs to go to the abuser profile to report an offensive message on the tester’s wall. In the latter case, the repoting button is clearly not placed close to the relevant content to be reported. Nevertheless, the link to the Help section is always searchable from every page. In addition, contrary to what is stated in the self-declaration, reports were not answered to and inappropriate content is not always checked out. Of the three kinds of content reported as offensive (a personal message, a message on the wall and a picture in another user’s photo gallery) only the personal message was checked out and deleted.

Advice on community guidelines and appropriate use of the SNS is provided in the Help section.

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

In its self-declaration, it is only mentioned that “since years Giovani.it collaborates with the police authorities for law enforcement in investigations and prosecutions.” No further specifications are provided on what this collaboration concretely implies. Besides, no information is provided on the processes and mechanisms that Giovani has put into place to expeditiously and appropriately review and remove offending content. Nothing is mentioned on if Giovani provides relevant links on its website to local agencies or organizations (apart from the Police authorities) that could support the process of reporting illegal content or conduct (e.g. InSafe, law enforcement agencies, etc.).

Because of ethical reasons, Principle 5 was not tested on the website.

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

Main findings in relation to the self-declaration

Giovani.it indicates in its self-declaration that they make users aware of the importance of protecting their own personal information. The FAQ contains an extensive chapter on how to minimize potential risks related to sharing personal information. Furthermore, Giovani has inserted specific privacy advice disclaimers in all the relevant pages where users may upload personal content.

Regarding specific privacy settings, as from the end of December 2010 Giovani claims it will have implemented implement the following features:

1. Option of disabling the online presence within the user profile page
2. Option of setting as private the personal profile of the user
3. Option of setting as private the personal blog of the user

Apart from these rather limited privacy options, no further information regarding other specific privacy settings is provided. Besides, no specific information is given regarding the properties of these privacy settings. For instance, it is not mentioned if these settings are prominent in the user experience or if they are accessible or visible at all times. Also, the service provider does not refer to the possible implications of automatically mapping information provided by users (during registration) onto their profiles and does not indicate if users are made aware when this happens.

Main findings in relation to the website

As shown in the test, users' profile are not private by default: without changing the default privacy settings, personal information provided at the time of registration is displayed on profiles of minors and included in their brief presentation that accompanies the 'search friends' results. This information includes: nickname, first name (only on the profile), age, gender, place of residence, education (only on the brief presentation and expressed as lower secondary school, upper secondary school, university), a picture of the user, the photo gallery of the user, contacts list, online status, comments and messages posted on the wall by other users. **U**sers are not made aware of this information being made automatically public. However, users can set their profile as private (accessible only by the user), or partially private (accessible only to friends or only to logged in users). They can also specify what kind of users are allowed to post comments on their profiles (all registered users – which is the default setting – only friends, or nobody) or on their blogs (nobody, everybody, only friends, all registered users, all registered users except 'enemies').

It is not possible to restrict only some parts of the profile (for example the photo gallery) to some specific users. Further privacy settings include the possibility to make their surname visible (it is invisible by default), to be invisible when viewing other people's profiles (visible by default), to remove the date of the latest login from the profile, or hide their online status in the online users' list (the options being: visible to everybody by default, visible only to friends, invisible). The function called 'block users' gives the possibility to filter groups of users (defined by age groups, number of friends, time spent in the SNS, amount of personal information included in the profile) allowed to contact them.

Privacy settings are easily accessible from the menu bar displayed on every page. Here the user finds all the privacy options provided by the website, articulated in 'general settings', 'comments', 'block users' and 'blocked/unwanted users'. These settings are easy to use. Moreover, as stated in the self-declaration, a disclaimer advice redirecting the user to information on how to protect one's privacy in the Help section is

displayed in every page where users can upload personal information or pictures.
It is easy to delete the profile, since the 'delete' button is easily accessible from the 'options' menu. The provider clearly states that the profile will be effectively deleted after seven days.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

Main findings in relation to the self-declaration

The self-declaration only mentions that "Giovani.it regularly improves the manual and automated tools that allow blocking and removing prohibited content/conduct." It is, therefore, not clear from the self-declaration if or how Giovani assesses the effectiveness of their services to identify potential safety threats.

Principle 7 was not tested on the website.

Summary of Results and Conclusions

Giovani has implemented Principle 1 rather satisfactorily and Principles 2, 3, 4 and 6 unsatisfactorily on its website. The testing on the website revealed several problematic areas, for instance:

- Profiles of minors are not set to private by default, and, thus, they are by visible to all users of the SNS.
- Minors' profiles can be searched for in the SNS search engine, even by users who are not registered to the community. Non registered users can also visit the minor's profile and access the personal information displayed there.
- Minors can be searched and contacted by adults with no restrictions. Adults can also send friendship requests and add minors to their contact list.
- Privacy settings are very limited.
- Even though the minimum age requirement is 13, the test demonstrated that children younger than the minimum age required could sign up easily bypassing the 13+ rule to become members of the site.
- Reports of inappropriate content or conduct are not user-friendly and are inefficiently handheld. Indeed, reports from users are not acknowledged and users get no answer to their reports. Besides, even though inappropriate messages to the user are deleted, other types of content such as offensive pictures are not.

Assessment of all the Principles in the Self-declaration

Principle	*Very satisfactory*	*Rather Satisfactory*	*Unsatisfactory*
1			X
2			X
3			X
4		x	
5			X
6			X
7		x	

Implementation of the Self-declaration on the SNS

Principle	*Very satisfactory*	*Rather satisfactory*	*Unsatisfactory*
1		x	
2			X
3			X
4			x
6			X

HYVES

Michel Walrave, MIOS, University of Antwerp, Belgium
Verónica Donoso, Appointed Research Coordinator by the EC

Introduction

Hyves is one of the most popular social network sites in The Netherlands and counts more than 10,6 million members[13]. This social network platform started in 2004 and is available in two languages (Dutch and English). The founders refer with the name of their social network site to a *beehive*, full of activity. Members can keep contact with friends and meet new people. Next to their profile, users can develop and consult blogs, post comments on profile pages, upload and browse through users' pictures and videos. Also 'gadgets' can be added to one's own profile (embedded third party applications). Next, classifieds can be published and games can be played online. Moreover, users can create groups ('Hyves') that gather persons sharing, for instance, the same interests. The social network site has also created a mobile application, giving the opportunity to be connected everywhere. Persons younger than 16 years old need parental permission to subscribe. According to a study, three quarters of the Dutch 8 till 17-year-olds has a profile on Hyves[14].

The following is a report of findings of the analysis of the self-declaration provided by Hyves and the testing of its website. The test was conducted in December, 2010 – January, 2011.

Summary of main findings

As far as minimum age requirements are concerned, Hyves states that users younger than 16 years need parental consent to subscribe. However, the test revealed that no parental permission was required to open an account on this social network site.

Users of Hyves are offered a broad range of privacy settings that are easy to find. However, tests concluded that profiles of minors are not set to "private by default"[15] as defined in the Safer Social Networking Principles[16]. As a matter of fact, not only friends, but also other registered users have access to some profile data of minor users including their name, likes/dislikes, hobbies, relationship status, pictures and comments posted by others). By default, other users (including friends) do not have access to contact details such as the home address, mobile phone number and location on Google maps. Only the (minor) user's e-mail is, by default, displayed to friends. The test also revealed that minors' profiles can be found by (adult) users through the social network site's search engine, although not via external ones such as Google.

Users of Hyves can easily report inappropriate content or conduct. A report abuse button is clearly visible and recognizable next to user generated content. An abuse report was sent to test this procedure. This led to positive conclusions on the speed and the adequacy of the reply sent.

Finally, information and hints on safety and security issues are easily accessible from the "Hyve safely" webpage. Also the FAQ-page is well organized, including a special section dedicated to *privacy, bullying and spam*. Moreover, links are included to several websites that offer more practical advice. Next to hints for young

[13] Including 9 million members in The Netherlands. Source: *Hyves in numbers* webpage (http://www.hyves.nl/about/facts/), information retrieved on the 16th of December 2010

[14] *Krabbels & Respect plz? Hyves en Kinderen*, September 2009, http://www.mijnkindonline.nl

[15] "Ensuring that setting a profile to private means that the full profile cannot be viewed or the user contacted except by 'friends' on their contact list".

[16] http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

users, a webpage is dedicated to parents, including some tips and a hyperlink to more educational material. By contrast, the length, formal phrasing and the inclusion of legal jargon in the Terms of Use may prevent (young) users to read this essential information.

Analysis of Results by Principle

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner

Main findings in relation to the self-declaration

In its self-declaration Hyves mentions that they provide "tips to hyve safely, not only textual but also with visuals to make it easier to understand for all users". It is also mentioned that Hyves runs educational campaigns with external partners (e.g. mijn kind online), but it is not clear from the self-declaration if the materials employed in these campaigns are also available on the website.

The self-declaration does not include explicit information on what constitutes inappropriate behaviour on the site or the consequences thereof. It does mention, however, that "pornographic or nude content with visible genitals is forbidden" on the site, but no other types of inappropriate content are mentioned. The self-declaration states that Hyves "will provide a parallel document to the Terms of Use, which will explain the rules and regulations in a clear and simplified matter."[17]

Hyves claims that they provide safety tips for parents. Besides, parents can have their IP address blocked to prevent their child from joining Hyves.

Main findings in relation to the website

At the bottom of every page, hyperlinks are included to several sections dealing with safety, security and privacy. This information is targeted as well to (young) users as their parents, for whom a dedicated webpage is available. Moreover, these links are not only clickable for *subscribed* users, but for visitors as well.

The Hyve safely ("Veilig hyven") webpage provides an overview of important safety and security issues. Concrete hints are formulated in short paragraphs that address several important topics, for instance, how to choose a 'strong' password, how to protect sensitive information (like phone number, e-mail, location). As this information is easy to understand, it is adapted to, amongst others, young social network site users.

Users are also informed on how to report abuse. This safety page ends by listing a number of websites dedicated to online safety and also external report centres (like the Dutch hotline combating Child abuse images on the Internet). These websites are not only dedicated to children and teens, but some also include information and safety tips for parents and teachers. Although these links to safety information are available on every webpage, they are not prominently placed. Links to the Privacy Policy ("Je privacy") and the Terms of Use ("Gebruiksvoorwaarden") can be found at the bottom of each webpage and are available to both registered users and visitors (not registered in Hyves).

The Terms of Use ("Gebruiksvoorwaarden") webpage extensively outlines prohibited behaviour and content and how to report abuse. It also clarifies how unacceptable uses will be dealt with, for instance, by removing the user's account temporarily or permanently, or deleting specific content. Yet, the Terms of Use constitute a very long legal text that is not adapted and is, therefore, not appealing to young users.

[17] This document is live as of the first week of January 2011 and can be found on

http://www.hyves.nl/useragreement/short/

However, a simpler version[18] of these Terms of Use is available[19]. The Privacy Policy (« Je privacy ») informs users about the uses of disclosed personal information, automatically generated data, that advertisement is adapted to the user's profile, etc. Again, this text is quite long.

The footer of each webpage also includes a link to the FAQ-page. Here, a specific section is dedicated to "*privacy, bullying and spam"* and concrete tips are given on how to deal with these issues and on how to safely manage your profile.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience

Main findings in relation to the self-declaration

In its self-declaration Hyves states that no minimum age requirements apply. However, minors younger than 16 need parental permission to be able to become members of this social network site. In its self-declaration Hyves refers to diverse mechanisms through which the service provider ensures limited exposure to potentially inappropriate content and contact for children, for example pornographic or "nude content with genitals exposure" is forbidden, accounts that violate the Terms are deleted, no inappropriate ads (e.g. alcohol) are allowed on the site, etc. Furthermore, a notification link ("Flag as offensive" button) is posted below all types of content and if certain content has been reported "multiple" times, then the content in question is temporarily deleted and is reviewed.

The self-declaration indicates that Hyves promotes the uptake of parental control by allowing parents to have their IP address blocked to prevent their children from joining Hyves.

Main findings in relation to the website

Hyves does not state explicit minimum age requirements. Yet, according to the Terms of Use and the Privacy Policy, users younger than 16 need parental permission to subscribe on the site. However, subscribers are only informed that «If you are not yet sixteen (16) you may only create an account subject to the prior consent of your parents or guardian»[20], still no parental consent is required to be able register on the site as a minor. As a matter of fact, when registering, users are asked to select their year of birth from a drop-down menu (reaching from 1900 till 2010). It was possible to subscribe as a 9 year-old without further questions or remarks. No parental consent was asked by using a parental consent form or any other procedure.

Although the social network site provides a specific webpage including safety hints and specific advice for parents (see Principle 1), no information is provided about tools that are available for parents to manage/control their child's social network site use. This contrasts with the self-declaration wherein the provider states that parents can ask the provider to block their IP address to prevent their child to have access to the social network site. Yet, no information for parents on this specific functionality could be found.

When subscribing as a minor user, advertising was found for the social network site's mobile service, travel and online shops (where presents can be bought). Also classifieds, put online by other users, can be found. Moreover, companies' brand pages can be consulted (e.g. banks, airlines).

[18] According to the provider, this simpler version of the Terms of Use is the shortest version they could provide due to Dutch jurisdiction.

[19] A simpler version of the Terms of Use can be consulted on http://www.hyves.nl/useragreement/short/

[20] «By accepting these Terms of Use you guarantee that you are aged sixteen (16) or over or have the consent of your parents or guardian to create an account », see: http://www.hyves.nl/useragreement/

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

The self-declaration states that "new profiles for under 16s are automatically defaulted to private" and that "no user can search for under 16s". The self-declaration refers to several mechanisms employed by the service provider to assist children and young people in managing their experience on their service, particularly with regards to inappropriate or unwanted content, including, among others, that all users can block contacts, set their profiles to private and can decide which piece of content to share with whom.

Main findings in relation to the website

Concerning the default privacy settings of minors, the test demonstrated that profiles of minors are not set to "private by default"[21] as defined in the Safer Social Networking Principles[22]. As a matter of fact, not only friends, but also other registered users have access to some profile data of minor users (e.g. name, likes/dislikes, hobbies, relationship status, pictures and comments posted by others). By default, other users (including friends) do not have access to contact details such as the home address, mobile phone number and location on Google maps. Only the (minor) user's e-mail is, by default*,* displayed to friends.
However, if the minor selects his/her school and adds a link to the schools profile page, the location of the minor could, eventually, be available by default.

The test also revealed that minors' profiles can be found by (adult) users through the social network site's search engine, although not via external ones such as Google. The adult user (created for this test) was, indeed, able to access the profile page and send a friendship request. Furthermore, the (adult) user could add a personal message to the friendship request. Yet, the minor had to confirm this request. These observations are not in line with the self-declaration stating that « New profiles for under 16s are automatically defaulted to private » and « no user can search for under 16s». In sum, profiles of users younger than 16 are not defaulted to private as defined in the Safer Social Networking Principles[23].

However, users can adapt the access to their personal data. They can restrict the access to their profile, set their profile to private, or make their profile more accessible (friends of friends, all Hyvers, everyone). However, (minor) users cannot select categories of persons (by age or region, for instance) to have access to their profile (or specific information). Subscribers can also refuse a friendship request and add contacts to a *blocklist*. An easily accessible and recognizable button can be used to block a contact.

By default all subscribers can post comments and pictures in a user's profile without pre-moderation by the (young) user. Yet, profile owners are informed by a private message that another user has put a comment on their profile.

If the user is confronted with inappropriate content or conduct, easy-to-use procedures are in place to erase this content and report abuse (see Principle 4). A subscriber can also restrict posting comments and also the access to comments to specific groups. Users can also choose which images (photo albums) will be visible for friends, their friends or everybody. Finally, users can conceal their online status.

[21] "Ensuring that setting a profile to private means that the full profile cannot be viewed or the user contacted except by 'friends' on their contact list".

[22] http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

[23] http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service

Main findings in relation to the self-declaration

Regarding the mechanisms to report inappropriate content, contact or behaviour, in its self-declaration Hyves indicates that users can easily report abuse either by contacting the community management or by means of report abuse procedures that can be accessed "wherever user-generated content appears". Users can report any type of inappropriate content or behaviour including spam e-mail or more serious violations of the Terms of Use. Hyves claims that reports of abuse are acknowledged immediately and acted upon expeditiously by dedicated teams. Hyves also claims that "every user that contacts the community management gets a personal answer".

Main findings in relation to the website

When assessing the report mechanism in the social network site, it was observed that users can easily report inappropriate content and conduct in two ways. First, via an online contact form reachable from the Terms of Use, the FAQ-page and the Hyves Safety pages; and second, via the abuse button found near user-generated content. This easily accessible and recognizable button leads to a pop-up form offering the user the opportunity to select a category of abuse (bullying/stalking, spam, discrimination/racism, porn, etc.) and to add a few comments[24]. Users are also made aware about the consequences of their report and are clearly asked not to make reports on innocent users. No information is added on how reports are typically handled.

As part of this study, a (fake) minor user reported that she had been bullied on this social network site. A realistic bullying situation was set up between the (fictitious) owners of profiles that were created for this assessment. The scenario consisted of one minor being bullied by two other minor users who posted a nasty comment on the wall of the 'victim' and who uploaded and/or sent hurtful pictures. As the 'victim' could not cope with the nasty comment put on her profile and the embarrassing pictures, she contacted the provider via a contact form. When the abuse report was sent by the victim, a message appeared on the screen confirming that the report had been sent. The same day, an answer was received via e-mail. Confirming what is stated in the self-declaration, an extensive and personal answer was sent. It focused on concrete tips on how to deal with this situation, amongst others, how to block a user. The moderator concluded by informing the user that, if further assistance was needed, the 'victim' could send more information to the moderator like screenshots for instance, as proof.

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

The analysis of the self-declaration shows that Hyves has effective processes in place to expeditiously review and remove offending content. Hyves claims that their "dedicated" security team identifies potential problems and reacts personally and promptly (within 24 hours) whenever confronted with (sensitive) security issues. Hyves also states that they cooperate with the Dutch Police (KLPD) as well as with other individual law enforcement units to provide them with "information and knowledge on how to use social networks for citizen safety".

Because of ethical reasons, Principle 5 was not tested in the website.

[24] If the user needs more space, the provider refers to the contact form. A hyperlink is provided, but does not directly lead to the form.

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

Main findings in relation to the self-declaration

According to its self-declaration, users of Hyves are provided with a range of privacy setting options and with supporting information to help them make informed decisions about the information they post online. For instance, contextual tips not to share information with strangers are provided; all users can set their profiles or parts of it (e.g. pictures) to private or they can conceal their 'online now' status.

The self-declaration does not specify if the privacy settings options/status are prominent, visible and/or accessible at all times. It also does not refer to if the service provider automatically maps information provided by users (during registration) onto their profiles or if users are made aware when this happens.

Main findings in relation to the website

In order to register in Hyves, users (including minors) must provide their real name, e-mail and date of birth. Yet, the form also includes questions about the place of residence and mobile phone number. Although these fields are not compulsory to subscribe, users could be tempted to fill in this information. Some of this information (name, date of birth, place of residence) is also included in the profile and is visible to users beyond the minor's accepted friend's list. However, the e-mail address is only visible to friends. The mobile phone number is, by default, not integrated in the profile. Nevertheless, it can be made visible, by adapting the privacy settings.

New subscribers are asked to check a box near a sentence stating that they agree with the Privacy Policy and Terms of Use. Therefore, users that are filling in the online form are invited to check this important information. Furthermore, an opt-in check-box is used to ask members if they wish to receive commercial e-mails from partners. Besides, a CAPTCHA[25] (to prevent the use of automated systems to subscribe and engage in spam) was also included in the subscription form. Moreover, an e-mail verification system is used to prevent unwanted subscriptions.

When adding information on the profile a link asking « Who may see this? » is placed next to each piece of information. This leads to the privacy settings where a user can see the default settings and easily restrict or open up access to specific personal details.

A subscriber can easily change his/her privacy settings and restrict the access to friends, friends of friends or make personal data visible to all users. On every webpage, a link can be found to the privacy section. Supporting information on how users can protect sensitive data, adapt their privacy settings and delete their account, is provided throughout the site. Yet, users' awareness on how to use these privacy settings is not raised in the privacy settings section itself.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

Main findings in relation to the self-declaration

According to the self-declaration, Hyves assesses their service to identify potential risks to children and young people and it automatically deletes inappropriate content (after being reported several times). The self-declaration also mentions that (flagged) inappropriate content is reviewed by specially trained community managers.

[25] *Completely Automated Public Turing Test to tell Computers and Humans Apart* is a challenge-response system test designed to differentiate humans from automated programs (searchsecurity.com).

It is not clear from the self-declaration if Hyves' community managers are in real-time contact with children. The self-declaration only mentions that these community managers are "educated to deal with sensitive issues on a personal note within 24 hours". However, the self-declaration does not mention what steps are taken by Hyves to minimize the risk of employing candidates who may be unsuited for work involving real-time contact with children or young people.

Principle 7 was not tested in the website.

Summary of Results and Conclusions

Hyves has implemented Principle 1 and 4 very satisfactorily, and Principles 2, 3 and 6 rather satisfactorily on its website. The testing on the website revealed some areas of attention, for instance:

- Profiles of users younger than 18 are not set to "private by default" as defined by the Safer Social Networking Principles. As a matter of fact, not only friends, but also other registered users have access to some profile data of minor users (e.g. name, likes/dislikes, hobbies, relationship status, pictures and comments posted by others).

- As far as minimum age requirements are concerned, the provider states that users younger than 16 need parental consent to subscribe to the site. However, in order to register on the site no proof of parental permission was required.

Assessment of all the Principles in the Self-declaration

Principle	*Very satisfactory*	*Rather Satisfactory*	*Unsatisfactory*
1		x	
2		x	
3		x	
4		x	
5		x	
6		x	
7		x	

Implementation of the Self-declaration on the Social Network Site

Principle	*Very satisfactory*	*Rather satisfactory*	*Unsatisfactory*
1	x		
2		x	
3		x	
4	x		
6		x	

IRC-GALLERIA

Niina Uusitalo, Tampereen yliopisto, Suomi
Verónica Donoso, Appointed Research Coordinator by the EC

Introduction

IRC-Galleria is available in Finland and in the Finnish language. IRC-Galleria has existed since December 2000. The current number of users is 451047 (14.12.2010 http://irc-galleria.net/). The age requirement is 12 years. Users of IRC-Galleria may create profiles, add pictures, videos and blog texts, make questionnaires for other users, post comments on other users' profiles and join site communities. By buying applications, users can for instance update their guest list, add logos or applications to their profile or add their picture or community on the front page of the site.

The following is a report of findings of the analysis of the self-declaration provided by IRC-Galleria and the testing of its website. The test was conducted in December, 2010 – January, 2011.

Summary of main findings

The site's minimum age requirement is 12 years. In fact, when trying to register as a 9 year-old, the site does not allow the minor to complete the registration process for being under the minimum age required by the site. However, by simply changing the birth date on the registration form to a "suitable" older one, it is possible to complete the first step of the registration process.

The provider has efficient mechanisms in place to report inappropriate content: Each individual piece of content has a reporting button next to it which the user may click. During testing inappropriate pictures and comments were reported to the administrators through the report button. The administrators removed the reported pictures in one day. Inappropriate conduct was also easy to report to online administrators who gave a swift response in half an hour. Inappropriate conduct and bullying could also be reported to the general administrator, where the response bounced back from the e-mail account at first and was answered in a week's time. The other reporting mechanisms found on the site were user-friendly, age appropriate and rather easy to find on the site, however, they were not as efficient as the reporting buttons.

When registering the site did not clearly report which information would be made public for all users. Most information posted on the profile was made public for all users when using the default settings. Profiles of minors are, thus, not set to "private by default". Users could protect their privacy by choosing not to post certain information (place of residence, birthday, date of registration, dating status). Certain information could also be made private for the user alone. The user could choose which information of their activities on the site to make public in their "Flow" (for instance joining groups, adjusting profile information etc.). After posting pictures users could move posted pictures into a private album where pictures were visible for the user alone. Users could also create new albums where pictures could be made visible for specific groups of people. Customising picture visibility could not be done in the default album (Oletusalbumi). Blocked users could view the user's public profile even after having been blocked. The self declaration states that users can prevent name searches on their profile, but this information was not evident, and there were no clear instructions on how to do this.

IRC-Galleria provides some tips for children and young people on how to use the site safely in the code of conduct or "Rules". These rules are specific and easy to understand for minors. Users are given clear information on do's and don'ts on the site. The Terms of Use -section includes technical jargon what makes it hard to understand for minors.

Analysis of Results by Principle

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner

Main findings in relation to the self-declaration

In its self-declaration IRC-Galleria states that they provide clear guidance for children and young people on how to navigate their website safely, for instance by means of giving users safety tips when building their profiles and using the community. The self-declaration stresses that constant safety education is provided on the site and through campaigns with relevant safety organizations.

In its self-declaration IRC-Galleria claims that they provide clear instructions and rules for the users, which are shown upon registration and which can be easily found in the site navigation. These instructions, clearly separated from the Terms & Conditions, explain in an age-appropriate and easily understandable language how the service should be used. IRC-Galleria states that clear information about what constitutes inappropriate behaviour is also provided through the "House Rules" and the "do's and don'ts" sections.

The self-declaration indicates that IRC-Galleria reports inappropriate behaviours. Images, texts or other illegal content is removed from the site and saved for eventual police investigation. The consequences of other types of inappropriate behaviour are not explicitly mentioned in the self-declaration. The self-declaration does not state if the website offers parents, carers and/or teachers targeted links, educational materials or other technical controls to support children`s responsible and safer internet use.

Main findings in relation to the website

As the testing shows, The SNS gave clear instructions on how to navigate the SNS safely, what kind of behaviour was forbidden, and the consequences of forbidden conduct, although there were very few tips on how to navigate the internet safely in general. Safety tips concerning conduct on this specific site were easy to find in the "Rules" (Säännöt). Safety information in the "Rules" section was written in clear, understandable and age-appropriate language, easy for minors to understand. Safety tips were only provided in writing, and there were no other educational materials such as videos about internet safety or the safe use of the specific SNS.

The Terms of Use contained technical and administrative jargon and long sentences, and was thus difficult for minors to understand. Safety information was not very visible on the sites homepage, one had to find a small link at the top or the bottom of the page called "Information" to find the pages concerning safety. The site provided clear information for parents or teachers on the functioning of the site. They were also given tips on wider internet safety in a special section for parents (Vanhemmille). Parents were provided with links to educational organizations concerned with child safety and their educational materials, although two of the links did not work at the time of the testing.

The main weakness of the site in relation to principle 1 is that children were not provided with extensive information of safe internet use in general, although under 18-year-olds were given 4 concrete safety instructions warning them not to post provocative pictures on the site, what to do if one is teased or harassed on the site, to ask their parents' permission to join the site and not to meet new internet friends in the real world without company.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience

Main findings in relation to the self-declaration

According to its self-declaration, IRC-Galleria has a minimum age requirement of 12 years old. IRC-Galleria is not able to verify users' age, though. Still, human moderators monitor user behaviour and remove identified under-age users from their service. Apart from the use of human moderators no further information is provided regarding the steps taken by the provider to prevent users from attempting to re-register with a different age if they have previously been rejected for being below 12.

Regarding the risk of exposure to inappropriate content for children and young people, the self-declaration states that users are provided with “lots of age-targeted” content, in particular, campaigns and advertising. However, no explicit mechanisms are mentioned to ensure limited exposure to potentially inappropriate content and contact.

The self-declaration does not refer to the mechanisms employed by IRC-Galleria to promote the uptake of parental controls to allow parents to manage their children’s use of the service. It also does not specify any functionalities put at the disposal of content providers, partners or users in order to label, rate or age restrict content where appropriate.

Main findings in relation to the website

The site’s minimum age requirement is 12 years. In fact, when trying to register as a 9 year-old, the site does not allow the minor to complete the registration process for being under the minimum age required by the site. However, by simply changing the birth date on the registration form to a “suitable” older one, it is possible to complete the first step of the registration process. The user gets, then, only a limited visitor status until their e-mail account is verified and a recognizable photograph of their face as profile picture is submitted. After fulfilling these two steps, the user gets full access to the site and its services. The fact that users must provide a recognizable picture of their faces may, in some cases, help restrict very young under-aged users from registering on the site, but it may not be so effective in the case of 10 or 11 year old children who may not “look” so different than a 12 year old child. Besides, this mechanism does not prevent under-aged users from posting a fake picture of someone older on the site.

According to the “Rules”, only age-appropriate contents should be posted on the site. However, the SNS does not specify what services or contents are considered as (in)appropriate for minors. When signed in as a child, some advertising was available on the site’s homepage. The main banner on the homepage advertises a blog on the SNS and its online community (More to Love). The blog has Samsung as a sponsor, and the company’s logo is inserted in the banner. The main banner also had an advertisement for Hotmail. On the side banner there was a logo “Made in Finland”, which is a certificate for products made in Finland, in this case IRC-Galleria being one of those products. On the homepage there is also advertisement for IRC-Gallerias own services, for instance the chargeable guest list.

As previously mentioned, IRC-Galleria has not committed itself to promote the uptake of parental controls in its self-declaration and this is also reflected on their website by the absence of information on this respect. Nevertheless, under-aged children are encouraged to consult their parents before using the service. Also parents are encouraged to help their children solve eventual dilemmas they may be confronted with on the internet by discussing (safe) internet use with their children.

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

In its self-declaration IRC-Galleria indicated that they offer many tools for their users to customize their user experience and privacy levels. For instance, users can choose what information to make visible in their profiles, they can restrict commenting on their profile or create “black lists” of blocked users.

The self-declaration does not state if the service provider ensures that the default full profiles of those registering under the age of 18 has been set to "private by default"26 as defined in the Safer Social Networking Principles27. Besides, the steps taken by the service provider in order to ensure that private profiles of users registered as under the age of 18 are not searchable are not clearly specified (apart from the fact that can prevent being searched via their name).

The self-declaration does not mention if or how IRC-Galleria educates parents about available safety tools/information such as filtering or parental control tools.

Main findings in relation to the website

As demonstrated by the test, specific minors' profiles were not searchable through any external search engines, but they were searchable through the site's internal search engine. Other users could find accounts only if they knew the user name, but pictures of new users were also posted in the section announcing "newcomers" on the front page (Käyttäjät -> Uudet käyttäjät). Any registered user can, for instance, search users of a certain age.

By default, all posted information in the minors` profile is made visible to other registered users. Thus, the information one chooses to post in their profile is automatically visible to any registered user who happens to find the profile with the exception of the e-mail address which can only be made public after the user's consent. There was no option to make the whole profile information visible to friends only. The only available options were to make the profile information "private" (only visible to the user themselves) or simply "public" (visible to all registered users). The real last name of a minor cannot be made public at all.

The user could restrict other users from commenting their site by putting other users on the "black list". The blacklisted person cannot post comments on the user's profile or vice versa. However, the person on the black list can still see the same information on the profile that friends and other users can see. One could also restrict commenting altogether, but then one also had to give up their own right to comment. Users could also reject friend requests. Furthermore, users or even friends could not post pictures on each other`s profiles or tag each other. Users could not allow only friends to post or delete comments or pictures on the user's profile. Comments left on one's own page could not be pre-moderated before they were published.

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service

Main findings in relation to the self-declaration

In its self-declaration IRC-Galleria refers to two mechanisms available to report inappropriate content, contact or behaviour that violates the Terms of Service, namely a One-click Reporting Tool and the possibility to contact IRC-Galleria staff through a Contacting Form. IRC-Galleria claims that the report button is easily findable in the main navigation. Here, users can select the type of violation experienced (e.g. inappropriate images, copyright violation, unofficial advertising, terms of violations or harassing behaviour). Even though a one-click reporting mechanisms suggests a child-friendly approach to reporting abuse, some of the labels provided to classify the type of abuse may be difficult for children to understand as rather complex legal terms are employed (e.g. copyright violation).

[26] "Ensuring that setting a profile to private means that the full profi le cannot be viewed or the user contacted except by 'friends' on their contact list".

[27] http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

The self-declaration also mentioned the cooperation with three "real-life policemen" from the Helsinki Police who "get a lot of reports in local police matters". But it is not clear from the self-declaration what such cooperation involves or what the policemen are entitled to do on the site.

The self-declaration neither includes information on if the reports are acknowledged and acted upon expeditiously nor if users are provided with an indication of how reports are usually handled. Also, no information is found regarding how users are provided with the information they need to make an effective report.

Main findings in relation to the website

As the test reveals, the SNS provides efficient reporting mechanisms for children to report inappropriate content, contact or behaviour. The user could report inappropriate content or behaviour through sending e-mail to the general administrator, by asking online administrators for advice or by clicking report buttons placed next to each individual picture, comment and blog text. Reporting mechanisms were available only for users. They were user-friendly, age appropriate and rather easy to find on the site, however, as the test shows, not all them were equally efficient. In the testing two (fake) minors posted bullying comments on another minor's page. One "bully" also posted offensive pictures of the "victim" on their own site and informed the "victim" of the pictures via a private message and via public comments on the page of the "victim".

Reporting abuse via e-mail is easy once the user has found the small link at the bottom of the page called "contact" (Yhteydenotto). E-mail reports of abuse go via the site to a general administrator. In the testing the bullied minor sent an e-mail report to the general administrator on December 13th 2010. An automatic message informed the user that the report was being processed and an answer would be given in three days. Apparently the answer from administrators bounced back from the minor's e-mail at first. The user was informed of this problem. The e-mail answer arrived on the 21st of December 2010. Here, the administrator advised the user to click the reporting button next to the content in question indicating that reporting abuse via e-mail is neither the most expeditious nor the most appropriate reporting mechanism available on the site.

Online administrators could also be sent a private message asking for advice on reporting problems. In the testing the bullied minor asked for help from two online administrators on December 13th 2010, one administrator provided advice in 27 minutes on how to report inappropriate pictures by clicking the report button. Another administrator did not answer. Finally, pictures, blog texts and comments can also be reported by an easy-to-use button placed next to each piece of content. This was the most prominent and readily available reporting mechanism. The bullied minor reported the bullying pictures on December 16th 2010. After reporting bullying pictures and comments through the report button, the administrators removed the pictures in one day demonstrating the effectiveness and the efficiency of the reporting button mechanism as opposed to e-mail based ones.

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

The self-declaration indicates that IRC-Galleria treats reports about illegal content and conduct as "top priority" and handles them "urgently". Any piece of content that is found to be illegal is immediately removed from the site, but is kept by the provider in case the police may further need to investigate the case. IRC-Galleria cooperates with local authorities and "immediately reports illegal content or conduct to them."

It is not mentioned in the self-declaration if the service provider includes relevant links to any local agencies or organizations in order to support the process of reporting illegal content or conduct.

Because of ethical reasons, Principle 5 was not tested in the website.

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

Main findings in relation to the self-declaration

In its self-declaration IRC-Galleria claims to provide its users with plenty of privacy tools (See Principle 3). Users also get safety messages when building their profile and using the community: e.g. when posting pictures users are reminded to consider the implications of posting their personal information online.
The self-declaration does not specify if the privacy settings options/status are prominent, visible and/or accessible at all times. It also does not refer to if the service provider automatically maps information provided by users (during registration) onto their profiles or if users are made aware when this happens.

Main findings in relation to the website

As the test demonstrates, on this SNS, minor users are only required to publish their user name. Also a recent profile picture of the user's face is required to acquire user status. The user does not have to share any other information with other users. The main privacy problem identified on the site is that users cannot customize their privacy settings to allow only specific users or groups to access (specific parts of) their profile information. Once published, the information is either public for all or for no one. Besides, certain information could not be made private. For instance, if one chooses to join communities or write information on the place of residence, dating status or motto, this information becomes automatically public. Users can, however, create picture folders that are visible only to specific groups.

Privacy settings are accessible from the profile and from every page, by clicking "Settings" (Asetukset). However, the privacy settings are not entirely visible when adding information to the profile. Users must click a separate link to get to privacy settings. While building the profile, users did not get information on which information would automatically be made publicly visible. After posting profile information the user could choose to hide certain information (date of birth, real name, place of residence etc.) from other users. However, once made private no one can see that information, not even friends.

Users were not given any supporting information to help them make appropriate decisions regarding their personal privacy settings. It was mentioned briefly in the "Rules" (Säännöt) that pictures posted on the site may stay on the internet even after being removed from the site. Deleting one's profile was very easy and convenient.

By going to the profile page, the user can delete the profile within a few clicks. The instructions are easy to understand. The site gives the user opportunity to sign in again within the next 48 hours to resume the user profile. The site informs the user that after 2 weeks the account would be removed. The provider neither stated if they would collect/retain any information from the user nor if this information would be used in any way after deleting the profile.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

Main findings in relation to the self-declaration

In its self-declaration IRC Galleria indicates that their Moderation team are "social media experts trained to identify illicit activities inside the community", for instance detecting fake accounts or any other type of suspicious, inappropriate or illegal activities (e.g. bullying). According to its self-declaration the provider employs a "preventive approach" towards privacy and other safety-related issues including educating users on how to use the Internet safely.

It is not explicitly mentioned if the moderators are in direct contact with children. Although the self-declaration states that these candidates are "properly trained to identify illicit activity" on the site, nothing is mentioned in the self-declaration regarding the steps taken by the provider to minimize the risk of employing candidates who may be unsuited for work involving real-time contact with minors.

Principle 7 was not tested in the website.

Summary of Results and Conclusions

IRC-Galleria has implemented Principle 4 very satisfactorily on its website, Principles 1 and 2 have been rather satisfactorily implemented while Principles 3 and 6 have been unsatisfactorily implemented. The testing on the website revealed some problematic areas, for instance:

- The default full profile of minors is not set to 'private by default' as defined by the Safer Social Networking Principles.
- Under-aged users can easily register on the site by simply changing their age birthday on the registration form.
- Users cannot customize their privacy settings to allow only specific users or groups to access (specific parts of) their profile information.
- Once published, the profile information can be made public for all or for no one. Besides, certain information could not be made private at all.
- Reporting mechanisms (other than the Reporting buttons located next to user-generated content) are user-friendly, age appropriate and rather easy to find on the site. However, they are neither effective nor expeditious.
- Only few tips targeted at minors on how to navigate the internet safely in general are provided.

Assessment of all the Principles in the Self-declaration

Principle	*Very satisfactory*	*Rather Satisfactory*	*Unsatisfactory*
1		x	
2		x	
3			x
4			x
5	x		
6			x
7	x		

Implementation of the Self-declaration on the SNS

Principle	*Very satisfactory*	*Rather satisfactory*	*Unsatisfactory*
1		x	
2		x	
3			x
4	x		
6			x

MYSPACE

Tester English version: Simon Grehan, NCTE, Ireland
Tester Spanish version: Charo Sádaba, School of Communication, Univ. of Navarra, Spain
Verónica Donoso, Appointed Research Coordinator by the EC

Introduction

Myspace is an online community where members can find and communicate with others as well as browse and share content. Users interact with friends' profiles, send messages to other users, join groups, become fans of bands, use third party applications and games, and upload and share photos and videos. The site is focused on the 13-35-year-old demographic and users must be at least 13 years old to create a profile. Myspace has traditionally focused on music and friends but its new goal is to become "the leading entertainment destination that is socially powered by the passions of fans and curators." Users can integrate their Myspace with their Twitter and Facebook accounts. It operates globally in over 20 different languages.

The English version and the Spanish version of Myspace were tested[28] in Ireland and Spain, respectively, in December 2010 - January 2011.

Summary of main findings

The Myspace Terms of Use Agreement states that users must be at least 13 years old to register. However, in both the English as in the Spanish version of Myspace it was possible to complete the registration by simply changing the date of birth[29].

As observed during the testing of both language versions of Myspace the profile of a minor user created for this test was defaulted to "private" as defined by the Safer Social Networking Principles[30]. As a matter of fact, in both language versions of the site, even though this profile could be found by an adult "non-friend" user of the site, this "non-friend" only had access to a thumbnail of the profile picture of the minor, the gender and the first and last names and no other personal information was returned in the Myspace search function. Besides, as demonstrated by our test "non-friends" cannot interact with minors in any way, not even by sending friend requests.

By searching in the major search engines such as Google or Bing no information on any of the minors created for this test could be found. Furthermore, as the test demonstrated, profiles of the minors created for this test could only be contacted by their approved list of friends.

Other features implemented by Myspace include the use of context-sensitive help and child-friendly access control technologies to help young users make informed decisions regarding the publishing of their personal information and the possibility for users to delete unwanted content and block other users. Reporting

[28] Myspace recently executed a complete redesign of the Myspace website in November 2010, prior to the testing by the Commission. This may have implied that some of the functionalities tested were not fully functional or were not yet optimally working at the time of testing.

[29] According to Myspace, the site's design transition led to some uneven implementation of the minor signup session cookie.

[30] "Ensuring that setting a profile to private means that the full profile cannot be viewed or the user contacted except by 'friends' on their contact list".

mechanisms are prominent on the site, easy to use, and the reports were dealt with promptly and effectively during the tests.

Finally, plenty of relevant safety information, advice, and tools for users, parents and teachers are prominently available on the site. However, in its Spanish version all the available safety audiovisual information is in English and none of the external links provided are from Spanish institutions or organizations working for a safer Internet experience.

Analysis of Results by Principle

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner

Main findings in relation to the self-declaration

In its self-declaration Myspace states that it provides clear, targeted guidance and educational materials for children and young people on how to navigate their website safely, for instance, through the Safety tips located at the bottom of each page. According to the self-declaration, under 18s receive periodic safety reminders upon login and when uploading content. Myspace also provides clear information about what constitutes inappropriate behaviour and the consequences thereof through the Terms of Use. These are clearly communicated and all users need to accept them before using this SNS. However, the self-declaration does not explicitly mention if this information is easily accessible on the website or if it is especially targeted at the youngest segment.

The “Safety tips” link at the bottom of every page includes links to parental monitoring and blocking software plus relevant e-safety information such as harassment and cyberbullying. There are tips specially targeted for parents and teachers available, for example, from the Parent Safety Tips page, the Myspace parent guide or the Myspace school guide. Myspace has also organized “aggressive education campaigns” through Myspace and other relevant third- party partners including several school associations.

Considering the amount and quality of the e-safety educational materials and resources available at Myspace, Principle 1 has been very satisfactorily assessed.

Main findings in relation to the website

In both language versions of the site tested, Myspace offers practical and complete information to minors about how to have a safe experience on the SNS. Tips, Q&A and audiovisual safety resources are available to both users and non-users. Myspace has a Help section prominently linked to from the navigation bar and the footer on all pages. There is also a Safety Tips section tailored for teens, parents, and educators and parental software is also available. Additionally, Myspace has developed targeted Myspace Internet Safety guides for Parents and Families, Teens, and School Administrators, however they are only available in English and some of the information relates to older versions of the website.

Both the English and the Spanish versions of MySpace provide videos for teens that promote positive behaviour and raise awareness on the consequences of negative online behaviour, however, once again, all the videos are in English and are, thus, difficult to understand for the Spanish-speaking segment.

When minors register on any of the language versions of the site they are given “a quick little safety reminder!” in the form of a pop-up window. This reminder outlines what constitutes inappropriate behaviour on the site and its consequences in a child-friendly and easy-to-understand way. When logged in as a minor in any of the language versions, context-sensitive advice was provided during key steps in the registration and content sharing process.

Apart from targeted e-safety information, MySpace offers its users detailed information on what constitutes inappropriate content in the Terms of Use page. Here, the consequences of breaching the Terms are also specified (e.g. content elimination, cancellation of the profile or even reporting to the authorities). This information, however, is presented via a long text, with small font and with a legal tone, not easy for minors to understand.

Regarding the main weakness of Myspace in relation to Principle 1, is the reduced amount of e-safety resources available in the Spanish version of the site as compared to the English one. In particular no videos, parental guides or links to Spanish institutions working on Internet safety are offered in the Spanish version of the site.

In sum, the fact that Myspace provides relevant, concise and concrete Information in diverse formats specifically targeted at children, parents and educators indicates that Principle 1 has been very satisfactorily implemented in the English version of the site. However, the rather limited amount and variety of resources in the Spanish version of Myspace reveals that this Principle has been less satisfactorily implemented in the Spanish version.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience

Main findings in relation to the self-declaration

The self-declaration does not explicitly state what the minimum age requirement for using Myspace is, however it does indicate that the minimum age requirement is stated in the Terms of Use of the website. According to its self-declaration, in order to identify and delete under-age users from their services, a session cookie is placed in the registration page. Myspace also employs a search algorithm (based on common terms used by underage users) to identify/search and delete "individuals misrepresenting their age".

In its self-declaration Myspace claims it ensures the limited exposure of children to potentially inappropriate content and contact through diverse mechanisms including, among others, the blocking of inappropriate URLS from being posted on the site, or the blocking of user accounts that upload pornographic content or not targeting certain types of ads to users under 18 (e.g. alcohol-related ones). Additionally, Myspace works closely with commercial content providers to ensure that users can make informed choices regarding content, for example, through warning messages and restricting access to content based on time of day.

Myspace claims it promotes the uptake of parental controls by providing links to parent monitoring software and other e-safety information.

Main findings in relation to the website

The Terms of Use Agreement states that users must be at least 13 years old to register. Myspace relies on self-declaration of age by the user in the registration process as the key mechanism for ensuring that the services they provide are restricted to children younger than 13. In both language versions tested, the testing revealed that when trying to register as 9 year-old permission was denied (without being told why membership had been refused). However, in both the English as in the Spanish version of Myspace it was possible to complete the registration by simply changing the date of birth without even having to close down the browser. This indicates that the session cookie was either not installed or it simply did not work.

Confirming what is stated in the self-declaration, advertising, both in the Spanish as in the English version of the site, is age-appropriate. In the Spanish version of the site advertising messages are displayed for minors while surfing the SNS. These ads include banner ads and Interstitials for products such as telecoms, television programmes or music contests. When logged in as a minor in the English version of the site the only advertisement displayed was for "MySpace Celebrity". This banner and right-column ad looks like another content module on the site but it says "Advertisement" underneath it. The ad clicks through to a section of the site that lets users follow celebrities and get news, photos, videos, events, and more information from around the web about them.

In relation to third-party applications, there are separate Terms of Use Agreements for Application developers that define prohibited content specifying the types of content that need to be restricted for under 18 and under 21 year old users.

In relation to parental control tools available on the site references are made to a software download called ParentCare in the parenting information in the Safety section. They say this installable application helps parents to determine if their children have a Myspace profile and to monitor some of their information on the site. However, the link was not working during the dates the tests took place.

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

According to its self-declaration, Myspace has taken a number of steps to empower young users such as new profiles of under 18 are automatically defaulted to "only friends"; no user can browse for users under 16; users under 16 are tagged as unsearchable by age on search engines. Adults can never add users under 16 as a friend unless they know the user's last name or email. Users under 18 cannot access age-inappropriate areas such as Romance and Relationship forums and groups or other mature groups. Besides, Myspace claims it has implemented a pornographic website database that restricts users from posting mature links on their profile.

Additional features for all users include, among others, the option of only allowing friends to post comments on their profile, to block other user and to conceal the users 'online now' status. By default, users under 18 must pre-approve comments made on their profiles.

Myspace claims it supports the safety education of parents in order to help them protect children and young people (e.g. via safety tips/information at the bottom of every page online, and links to parent monitoring software and other e-safety information).

Main findings in relation to the website

As observed during the testing of both language versions of Myspace the profile of a minor user created for this test was defaulted to "private" as defined by the Safer Social Networking Principles[31]. As a matter of fact, in both language versions of the site, even though this profile could be found by an adult "non-friend" user of the site, this "non-friend" only had access to a thumbnail of the profile picture of the minor, the gender and the first and last names and no other personal information was returned in the Myspace search function. Besides, as demonstrated by our test "non-friends" cannot interact with minors in any way, not even by sending friend requests.

By searching in the major search engines such as Google or Bing no information on any of minors created for this test could be found. There is an option in the privacy settings to "allow users over 18 to contact me". However, confirming what is stated in the self-declaration, the test showed that despite having checked this box and saved the changes adults (who were not 'friends' of minors) were still unable to access the minor`s profile or send them messages. Furthermore, as the test demonstrated, profiles of the minors created for this test could only be contacted by their approved list of friends.

In both versions of Myspace tested and, as indicated in the self-declaration, by default, the profiles of the minors created only allowed friends to post comments on their profile and the user had to pre-approve the comments before they were displayed publicly. Similarly, when minors were tagged in photos, they needed to be pre-approved before they were displayed on their profile. It is possible to remove the comment approval requirement by choosing the appropriate check box in the Settings page.

Delete buttons are prominently displayed beside content modules on the user's profile, on their newsfeed and in the directories. Users can block other users, and friends, and then unblock them easily. Controls are also

[31] "Ensuring that setting a profile to private means that the full profile cannot be viewed or the user contacted except by 'friends' on their contact list".

prominently placed on users' profiles that allow others to block them, remove them from their friends list, and to report them.

When uploading photos context sensitive information was displayed detailing the technical requirements, the types of content not permitted and links to the Photo Policy. When updating status comments, a warning about disclosing personal information was displayed.

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service

Main findings in relation to the self-declaration

In their self-declaration Myspace refers to several easily-accessible, age-appropriate and at all times available mechanisms for (young) users to report inappropriate content, contact or behaviour that violates the Terms of Service including, among others: Report abuse procedure available from every Myspace webpage and whenever user-generated content appears; users can directly report sexually explicit conduct in UK and USA to specialised centres by choosing the "inappropriate contact" report abuse option; users can easily "report abuse" in all site area that contain user-generated content such as images, videos, messages and blogs; users are easily able to provide reasons when reporting images for Terms of Use violations; links to relevant local agencies and organisations are provided, e.g. depression, suicide and bullying.

The self-declaration stresses that users` reports are "acknowledged immediately and acted upon expeditiously" by specialised teams by means of the following process: Myspace reviews the reports, takes appropriate measures and responds back to the user explaining what actions were taken.

Main findings in relation to the website

As demonstrated by the test, in both versions of Myspace users can report inappropriate content and contact in an *easy to find* and *easy to understand* way. The Report Abuse form is linked to directly from the Information footer on all pages. A report abuse button is prominent beside all photos and videos; when it is clicked a report abuse form is displayed with information such as name and email address already completed. You can choose from a drop-down list to categorise the abuse. There is no specific report abuse mechanism on comments although there are buttons that allow you to block users and delete comments by clicking a button.

As part of the testing process, a (fake) minor was tagged in some pictures and nasty comments were added to her profile. The (fake) bullied minor filled in a reporting form and sent it to Myspace explaining the situation and asking for help and advice. In the Spanish version of Myspace no acknowledgement of receipt was sent to the user explaining how her complaint would be handled. However, a reply to her reporting form was sent 26 hours later by email. It included general information (also easily available to users on the SNS) and some ideas about how to proceed if what was reported effectively constituted an offense (e.g. go to the Police, recording everything as proof, etc).

In the English version of the site the same testing procedure took place. Here, an acknowledgment of the form being sent was displayed on screen. Besides, an automated email response was immediately received letting the "bullied" minor know that Myspace had received her message and that someone on the team was reviewing her question and would get back to her soon. The message quoted a unique reference number. Six hours later a second email was received providing detailed instructions on how to block the offending user and providing useful information relating to blocking. These instructions were easy to follow. After the offending minor was blocked, she could still access the bullied minor's profile although the live feed was not updated by activity that occurred after the blocking. It was possible, though, to click on photos and access the photo gallery including photos and comments in the gallery that had been posted since being blocked. However, the blocked minor could not interact with any content.

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

According to its self-declaration "Myspace proactively reviews images and videos and enforces compliance with the Terms of Use". Myspace not only deals with notifications from users, but also with those from non-users' such as parents, teachers and other local and international parties concerning a variety of safety issues (e.g. inappropriate content, general support, cyberbullying, etc.).

MySpace claims that the Policy Enforcement Team handles high priority and highly sensitive user reports by means of "an around the clock telephone hotline". They also collaborate with law enforcement and government agencies. On its turn, the Security Abuse Enforcement Team aims at preventing and responding to malicious use of the site and at investigating such activity.

According to its self-declaration, Myspace has implemented specific arrangements to share reports of illegal content or conduct with the relevant law enforcement bodies. It supports local, state, federal and international law enforcement in investigations and prosecutions and a 24/7 dedicated hotline and email have been specially created for law enforcement. Myspace not only provides "ongoing training to cyber crime units on how to investigate and prosecute cyber criminals using Myspace", but also a Law Enforcement Guide and a Quick Reference Guide to "help law enforcement agencies understand Myspace ad investigate cases."

Principle 5 has been rather satisfactorily assessed because even though Myspace states that they proactively review images and videos and enforce compliance with the Terms of Use, the service provider does not explicitly mention if they expeditiously review and remove offending content. They also do not specify what concrete mechanisms are in place to remove content found offending.

Because of ethical reasons, Principle 5 was not tested on the website.

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

Main findings in relation to the self-declaration

According to its self-declaration, Myspace offers its users a wide range of privacy setting options allowing users, where appropriate, to edit and make public/private the information (provided during registration) that is automatically mapped onto their profiles. Users are also provided with supporting information to help them make informed decisions about the information they post online. In particular, in the "Safety Tips" pages, users find targeted information for teens, educators and parents (See Principle 1). In addition, specific safety measures have been implemented to protect the privacy of users under 18 (See Principle 3).

In relation to their privacy (settings), the self-declaration states that each application in Myspace offers granular settings allowing users to control different types of content from being shared with specific users. The same privacy controls that are in place for members apply to all available applications. "An application can only get information from the user if the user installs the application and thereby grants the application permission".

In terms of communication, there are plenty of communication preferences available that allow users to restrict communication as strictly or as leniently as they choose, save for the default settings.

Nothing is not mentioned in the self-declaration regarding if privacy settings options /status are prominent in the user experience or if they are accessible at *all times.* Still, because Myspace does encourage and enable young users to employ a safe approach to safety Principle 6 has been very satisfactorily assessed in the self-declaration.

Main findings in relation to the website

In both versions of Myspace, when creating a profile users are only required to supply basic information such as name, profile picture, gender and age. By default, this "mandatory" information is automatically inserted into the users` profiles, but users are informed that this information will be made public and, if they wish so, they can also conceal this mandatory information. When a user has created a profile they are invited to supply further information (e.g. interests, location, body-type, ethnicity, etc.). It is not explicitly stated that this information will be displayed on their public profile. By default, this information can only be seen by friends. However, users are always allowed to change their privacy settings.

Although not explicitly mentioned in the self-declaration, all the privacy settings are accessible at all times by clicking Privacy Settings from the My Stuff drop-down list on the header on all pages. They can be configured by clicking radio buttons and check boxes in the Privacy section. In both the English and the Spanish versions of the website, all labels are simple and easy to understand. Besides, the Privacy page for minors is presented with a comprehensive list of tips and ideas on how to use Myspace safely. This information is written in an adequate tone and language, easy for children and young people to understand.

In both language versions, context sensitive information is displayed when uploading photos detailing the technical requirements, the types of content not permitted and links to the Photo Policy. When updating Status comments a warning about disclosing personal information is displayed.

An important privacy setting available in Myspace is that, by default, minors under 16 cannot be contacted by adults. Nevertheless, the minor can change this option and, eventually, be visible to adults. Still, in order to add a minor as a friend, the adult has to prove he knows the minor by providing their email address.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

Main findings in relation to the self-declaration

As mentioned in Principle 2 and Principle 5 Myspace has implemented diverse mechanisms to ensure the limited exposure to potentially prohibited content and contact by children and employs different types of procedures to promote compliance with the Terms of Service, for instance, inappropriate URLS are blocked from being posted on the site or user accounts that upload pornographic content are blocked.

Myspace claims it proactively reviews images and videos (See Principle 5). Additionally, Myspace has implemented arrangements to share reports of illegal content or conduct with the relevant law enforcement bodies.

Myspace states that they proactively review images and videos and enforce compliance with the Terms of Use. They also review reports of abuse and take appropriate actions. Principle 7 is, thus, very satisfactorily evaluated.

Principle 7 was not tested on the website.

Summary of Results and Conclusions

Myspace has implemented Principles 3, 4 and 6 very satisfactorily and Principles 1 and 2 rather satisfactorily on its website. However, it must be said that Principle 1 has been better implemented in the English version of the site than in the Spanish one. The testing on the website revealed some areas of attention, for instance:

- In spite of the minimum registration requirement, both in the English as in the Spanish versions of Myspace it was possible for a child younger than 13 to create an account by simply providing a "suitable" date of birth.
- Profiles of minors could be found by an adult "non-friend" user of the site. However, this "non-friend" only had access to very limited personal information of the minor and could neither contact the minor via messages nor send friend requests.

- Limited availability of safety resources in the Spanish version of the site.
- The Terms of Use may be rather difficult for the younger age segment to understand.
- No parental control tools available during the testing. Links were available, but they were not active at the time of testing.

Assessment of all the Principles in the Self-declaration

Principle	*Very satisfactory*	*Rather Satisfactory*	*Unsatisfactory*
1	x		
2	x		
3	x		
4	x		
5		x	
6	x		
7	x		

Implementation of the Self-declaration on the SNS

Principle	*Very satisfactory*	*Rather satisfactory*	*Unsatisfactory*
1		x	
2		x	
3	x		
4	x		
6	x		

NASZA KLASA (NK)

Aldona Zdrodowska, Warsaw School of Social Sciences and Humanities, Poland
Verónica Donoso, Appointed Research Coordinator by the EC

Introduction

Nasza-Klasa (Our-Class) is a polish language social networking service available to users of all ages. The site begun operating in November 2006 and is very popular among polish internauts, with more than 13 million registered and active users by the end of 2010. The main idea in the beginnings was to provide a communication platform, where users could find “old” colleagues from school and stay in touch with their classmates, schoolmates and friends. Throughout years, Nasza-Klasa evolved into a full-featured social networking service, where users can create profiles, post comments, publish multimedia content, communicate with others and play games. Among the main functionalities available on NK site are: profiles for classes and schools where current students and alumni gather, groups and forums, micro-blogging service (“Śledzik”), internal communicator NKtalk and mobile version of the service. From 2010 Nasza-klasa started using the brand name “NK”. The website addresses are: nk.pl, nasza-klasa.pl.

The following is a report of findings of the analysis of the self-declaration provided by Nasza Klasa (NK) and the testing of its website. The test was conducted in December, 2010 –January, 2011.

Summary of main findings

Users of NK site are provided with a range of privacy settings along with supporting information to help them make informed decisions about the information they post online. Although by default, most of the crucial information that minors post in their profile is only visible to people who are listed on the youngster’s “friends list”, minors can still be contacted by users who do not belong to their contacts lists. Additionally, minors' contacts list is also visible to non-friends. Therefore, the full profile of minors is not set to “private by default” as defined by the Safer Social Networking Principles. NK users’ profiles are invisible for external search engines such as Google. In NK’s internal search engine, no results were returned when typing in the first and the last name of the minor created for this profile. Only after adding the minor`s place of residence (“Paulina Nowak”+Warszawa) the profile of the minor created for this test appeared in the results**.**

Reporting inappropriate content and conduct in NK is quite straightforward. It can be done via e-mail or by simply clicking on clearly identifiable “report abuse buttons” prominently placed next to user-generated content (e.g. photos, comments, etc.). Reports are acknowledged and handled effectively, although not expeditiously. It took 4 days for the reporting user to get an answer from the provider, as opposed to the maximum responding time of 48 hours stated in the self-declaration.

The safety and privacy information provided on NK website is easy to find and covers many online safety issues from general advise and tips on how to use the internet safely and wisely, to instructions on how to cope with specific types of abuses. The “Safety” section provides considerable amount of various information targeted at children, young people, parents and teachers, as well as the general public. NK provides easy-to-use and easy-to-access mechanisms designed to limit users’ exposure to inappropriate content and/or to restrict unwanted communication and interactions with other users.

Analysis of Results by Principle

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner

Main findings in relation to the self-declaration

According to its self-declaration NK provides *clear* guidance and safety information specifically targeted at children and young people on how to navigate their website safely (e.g. via The use of cartoon characters Sekurion and Proteka to provide personalized safety tips to children and alert them about new safety content). According to the self-declaration, the Safety section provides dedicated sections for parents and patrons as well, but not for teachers. Here general safety information is provided as well as links to relevant local safety organizations (e.g. Kidprotect.pl).

According to the self-declaration, the Terms of Use and privacy Policy specify appropriate and inappropriate behaviour on NK. Key information about the Terms is provided in "strategic places" throughout NK so that users can be timely reminded of the conditions ruling the site. However, the self-declaration does not mention if this information is age-appropriate or easy for children and young people to understand. However, a simplified version of the terms especially dedicated to youngsters is foreseen (Vademecum of Terms of Use).

No explicit information on the consequences of inappropriate behaviour on the website is stated in the self-declaration. No information on the available technological tools for parents in order to monitor their children is found on the self-declaration, either.

Main findings in relation to the website

The "Safety" ("Bezpieczeństwo") section of the site has areas specially dedicated to children, young people, parents and teachers. It contains relevant safety information such as dealing with personal information protection issues (legal and practical), how to report an abuse, how to ask for help on the site, etc. Specific information and tips on coping strategies are also gathered in the "Abuse" ("Nadużycia") subsection.

The information is presented in many different formats, suitable for the different aforementioned target groups. For instance, in the "Children" ("Dzieci") subsection there is a comic story about internet risks and how to avoid them with links and telephone numbers to child safety organizations provided. "Children" and "Young people" ("Młodzież") subsections also contain video formats and textual advise – in both cases the language is appropriate for the intended audience. In a subsection addressed to both children and parents surfing the internet together ("Common play", "Wspólna zabawa") there are printable PDF documents "netiquette" ("netykieta") and "refrigerator contract" ("umowa lodówkowa"). The latter consists of a set of rules for navigating the web safely and responsibly - to be printed, signed by a child and parent(s) and placed in a visible place at home, e.g. on a refrigerator.

Privacy policy issues are addressed in several areas of the site: in the "Privacy Policy" section of the site, in the "Help" and "Safety" sections and in article 5 of the "Regulations" document. Safety section as well as privacy section are easily accessible and provide plenty of relevant information for users and non-users of the site regarding general advice and tips on how to use the internet safely and wisely, to instructions on how to cope with specific types of abuses on NK site.

Content and conduct that is not allowed on NK site and the consequences thereof are defined in the "Terms of Use" in the "Regulations" document ("Regulamin"). "Terms of Use" article may be discouraging and difficult to understand for children and younger users due to the formal language it adopts. No clear and concise "Code of Conduct on NK website" targeted specifically at younger children was found.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience

Main findings in relation to the self-declaration

NK self-declaration does not mention what the minimum age requirement is to register on NK or if a minimum age requirement applies at all. It only states that "a person under 18 must have adult permission to use nk.pl". Apart from requiring parental permission to register on the site, NK does not refer to any other mechanism to ensure that underage users do not register on the site or any other measures to identify and delete under-age users from their services. However, the latter would only be relevant in case NK applies a minimum age requirement, what cannot be inferred from its current self-declaration.

In its self-declaration NK refers to the mechanisms through which the service provider ensures limited exposure to potentially inappropriate content and contact by children, e.g., access to profiles of minors is restricted (although their basic information can be searched via the internal search engine); "alien" users cannot provide any actions on the minors' accounts; a "wrong links validator" deactivates dangerous links (but it is not specified what "dangerous" links are); a family filter helps to find and remove swear words; etc.

NK does not refer to the ways in which this service provider promotes the uptake of parental controls in its self-declaration.

Main findings in relation to the website

Nasza-Klasa is available to users of all ages. Therefore, no minimum age requirements apply to subscribe to this SNS. Even though the "Regulations" document states that an official carer's consent is required from minors who want to become NK users, parental consent was not verified (nor prominently reminded of) during the registration process.

During the testing two additional mechanisms designed to limit users` exposure to inappropriate content were found. First, a pop-up notification for users uploading single photos (not visible while uploading multiple ones) warning them that erotic and inappropriate photos would be deleted from the site. Second, the option to "automatically add those who use swear words on my profile to a black list". The "swear words" filter is set to "off" (not "ticked") by default. During the testing, a message containing swear words was posted on the minor's profile (created for the testing purposes). Also two of the pictures - published in that profile - were commented with swear words. These offensive comments were not spotted by the system when the filter was set to "off". At first, setting the filter to "on" (without removing offensive comments first) did not result in "swearing" being put to a black list. Apparently, the filter is not retroactive. However, when the filter is set to "on", an attempt to post a new comment containing swear words was unsuccessful. A system message was displayed with a request to correct the inappropriate message. A further attempt to post an offensive comment – without removing the swear words - resulted in blocking the offending user. Still, it was possible to put offensive comments under pictures in minor's profile (in the gallery). The system did not react to it in any way. To sum up, it was found in the testing, that the filter is partly effective.

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

In its self-declaration NK refers to several tools and technologies to assist children and young people in managing their experience on their service, among others the possibility to control relationships made in the service; option to reject friend's requests, to block unwanted guests (Black list) and to remove comments; possibility to report photos that violate the Terms of Use, etc. If they wish, users are allowed to hide their profiles and make them invisible for search engines.

It is not clear from the self-declaration if profiles of minors are set to "private by default"[32] as defined in the Safer Social Networking Principles[33]; however NK claims that by default, any crucial information (e.g. photos, school name, age, etc.) that minors post in their profile is only visible to users who belong to the youngster's friends list.

The self-declaration does not include any information on the available safety tools to help parents protect young people, although, as previously mentioned, it does provide targeted safety information.

Main findings in relation to the website

During the testing, several mechanisms to assist (minor) users in managing their experience on NK site were found confirming what is stated in the self-declaration, for instance, the possibility to remove unwanted content or prevent postings on one's profile. Users of NK website may delete any kind of content they have posted/published on the site. They are also able to delete comments that others have posted on their profile (by clicking "remove comment" button) and to untag a picture ("remove a pin") tagged with their name. The "Remove post" functionality, mentioned in the self-declaration was not found in forums.

In a newly created minor's account, the profile is set to "private" ("profil prywatny") with limited information visible to those who are not "friends" of a user and more restricted than a default adult profile. Personal information visible to "non-friends" in the default "Private Profile" comprises: real first and last name and gender (required during the registration process and inserted automatically to a user's profile) as well as minors' contacts list and some additional information such as the place of residence (but not the address) and games (to which a user subscribed). Even though the profile of the minor created for this test contained more personal information (e.g. telephone number or pictures), this information was not revealed to non-friends. By default, "non-friends" are not able to put comments on one's profile, to comment and/or rate his/her photo or to add one to a "followed persons" list. However, the "default "private[34]" settings of a profile do not prevent minors from being contacted by others (e.g. adults), who are not one's "friends". To prevent "non-friends" from being able to view any part of a user's profile or to contact a user in any form, one has to block that particular person. In sum, the default "private" setting of minors in NK does not match the definition of "private by default"[35] of the Safer Social Networking Principles, namely "that the full profile cannot be viewed or the user contacted except by 'friends' on their contact list".

By default, the search for a minor's profile in external search engines – Google, MSN Search and Yahoo – did not return any results. When typing in the first and the last name of the minor created for this profile In NK's internal search engine (as a non-friend), no results were returned, either. However, when adding the minor`s place of residence ("Paulina Nowak"+ Warszawa) the profile of the minor created for this test appeared in the results, but, as previously stated, it only revealed limited personal information to "non friends"**.**

The default privacy settings can be changed to less or more private according to the user's wish. When set to "invisible", which is not the default privacy setting for minors in NK, the profile does not even appear in the internal engine search results. Yet, some personal information (first and last name and gender) is visible to visitors entering one's profile from links (list of "friends") in other users' profiles. Those visitors will also be able to send a message or an invitation to become a "friend". Only blocked users (in the black list) are totally denied access to one's profile, which also means that they are not able to contact him/her.

[32] "Ensuring that setting a profile to private means that the full profile cannot be viewed or the user contacted except by 'friends' on their contact list".

[33] http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

[34] There is an option in privacy settings allowing a user not to receive messages, comments and invitations form "fictional" accounts. By default it is set to "off".

[35] http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

During the testing, no mechanisms to restrict or limit contacts between minors and adults – based solely on age differences - were found on NK site. There are, however, mechanisms available to restrict (entirely or to some extent) unwanted communication and interactions with other users in general (e.g. "friend" – "non-friend" status, and ability to reject a "friends" request and/or other forms of communication (from strangers), etc.).

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service

Main findings in relation to the self-declaration

The self-declaration refers to several mechanisms to report inappropriate content, contact or behaviour: a 'Block user' button is placed in every profile; a 'Report abuse' and a Remove comment' button are placed under every picture published, under every comment and next to each micro blogging post and comment; a 'Remove post' is found in every forum. Furthermore, a link to 'contact', where users can notify their issue, is placed on every page of NK.

The self-declaration includes specific information about how users` general requests, and reports of abuse, in particular, are handled: Every user gets a standard e-mail acknowledging receipt of their notification. These notifications are then reviewed and users are sent a reply within 48 hours. In case of reporting "any kind of abuse the actual reaction time is less than couple of hours".

Main findings in relation to the website

As stated in the self-declaration, NK users are provided with several easy-to-access and easy-to-use mechanisms, which allow them to report abuse including a general contact form or by clicking an easy-to-use and easy-to-find "report abuse" button placed next to every piece of user-generated content (e.g. pictures, comments and posts). The "Help" and "Safety" sections provide comprehensive information on how to report an abuse, how the report will be handled by NK and other options to get help.

A general "Contact form" can also be used to report abuse. This form is placed in the footer of each page of the site. When reporting an inappropriate content through a contact form, apart from composing a message, a user is required to provide a link to a page where the content is posted. As a part of the testing, a message was sent reporting on a bullying situation involving bullying pictures and nasty comments. A message was sent through a general contact form. According to the advice found in the "Help" pages. A "report an abuse related to pictures" topic was chosen from options available in the form and a link to a "nasty" picture was provided in the message. As a result, the reporting mechanism sent an acknowledgement e-mail within a few minutes, providing a case number and information on how long it typically takes to receive an answer (48 hours). The full reply to the potential user at risk was sent four days later stating that a warning message had been sent to an indicated user with request to remove the questioned picture and, if that user did not remove it in two days – the picture would be removed by the provider. The "bully" did receive a message with the request to remove the bullying picture. Therefore, the reporting mechanism on NK website proved to be effective, although not as expeditious as expressed in the self-declaration.

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

Nk.pl employs human and automated forms of moderation in order to identify potential risks for minors. In order to detect potentially illegal or prohibited content (e.g. obscene photos, swear words, etc.) the Customer Service scans the site and removes the inappropriate/illicit content as soon as possible. They also employ filters to catch illegal comments, data and subtitles. User-generated reports are also employed to identify potential safety threats.

NK states that they work closely with lawyers and police officers and in case of suspicion of a crime being committed, Nk.pl specialists report it to the corresponding civil services.

For ethical reasons, principle 5 was not tested on the website

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

Main findings in relation to the self-declaration

According to its self-declaration, users of NK are always allowed to modify their privacy setting options and are provided with supporting information to help them make informed decisions about the information they post online. Indeed, the Privacy Policy provides information on how to manage personal data. NK also encourages users to treat their personal data seriously via different ways including periodic privacy raising awareness campaigns. There are 3 main privacy settings available in NK: "open profile", "private profile", and "closed profile". Besides, individual privacy settings can also be customized.

The self-declaration specifies that the privacy settings options are prominent and accessible at all times. The self- declaration does not explicitly mention if the information provided by minors during registration is (not) automatically mapped onto their profiles, however it does state that during the registration process users can hide all the information about themselves.

Main findings in relation to the website

Supporting the analysis of the self-declaration, users of NK are provided with a range of privacy settings along with supporting information to help them make informed decisions about the information they post online.

In spite of the wide range of available privacy options, privacy settings are quite easy to manage. Most of the available options seem self-explanatory. There are three predefined settings – "Private", "Closed" and "Open" profile - but no clear description of predefined settings was found. Privacy settings and preferences are easily accessible through a link "Edit profile" ("Edytuj profil") placed in the right top corner of every page in the service.

NK users are able to choose what will be visible - to "friends" and "non-friends" respectively - in their profiles. In the privacy settings a user may also decide whether "non-friends" will be allowed to post comments or rate a picture/photo on a user's profile or to add a user to "followed persons" list. It is also possible to prevent others from tagging a picture with a user's name and a link to his/her profile.

Testing also showed that it is easy to delete an account on NK site. After deleting an account, a user (former user) is notified that some personal information will be retained in the provider's databases, although it is not clear what information exactly. If a user wants his/her personal information to be deleted permanently, he/she needs to contact provider.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

Main findings in relation to the self-declaration

As mentioned in Principle 5, Nk.pl employs human and automated forms of moderation to identify potential risks for minors including illegal or prohibited content. These mechanisms include the use of filters, user-generated reports and/or human moderators to expeditiously review and, if necessary, remove the inappropriate/illicit content. It s not clear from the self-declaration how NK assesses the effectiveness of their services to identify potential safety threats.

Nk.pl makes sure to provide selected employees from customer service with special training so that they can appropriately deal with ‘tough cases’ (how to respond, how to act with sympathy, etc)”.

Principle 7 was not tested in the website.

Summary of Results and Conclusions

According to its self-declaration, NK has implemented Principles 1, 2 and 6 very satisfactorily and Principles 3 and 4 rather satisfactorily on its website. The testing on the website and the analysis of the self-declaration revealed some problematic areas, for instance:

- Although by default, most of the crucial information that minors post in their profile is only visible to people who are listed on the youngster’s friends list, minors can still be contacted by users who do not belong to their contacts lists. Additionally, minors' contacts list is also visible to non-friends. Therefore, the *full* profile of minors is not set to “private by default” as defined by the Safer Social Networking Principles.

- Reporting inappropriate content and conduct in NK is quite straightforward. Reports are acknowledged and handled effectively, although not expeditiously. It took 4 days for the reporting user to get an answer from the provider, as opposed to the maximum responding time of 48 hours stated in the self-declaration.

Assessment of all the Principles in the Self-declaration

Principle	*Very satisfactory*	*Rather Satisfactory*	*Unsatisfactory*
1		x	
2		x	
3		x	
4	x		
5	x		
6	x		
7	x		

Implementation of the Self-declaration on the SNS

Principle	*Very satisfactory*	*Rather satisfactory*	*Unsatisfactory*
1	x		
2	x		
3		x	
4		x	
6	x		

NETLOG

Tester Dutch version of Netlog: Michel Walrave, MIOS, University of Antwerp, Belgium
Tester German version of Netlog: Monika Taddicken, University of Hamburg, Germany
Verónica Donoso, Appointed Research Coordinator by the EC

Introduction

Netlog is a social networking platform, targeted towards European youngsters, with more than 72 million members. Netlog was founded in 2000, first as a social network site in Belgium, but rapidly spread inside and outside the European Union. The SNS provides tools to build an online identity (profile) to connect and communicate with friends and other persons. Moreover, members can play online games, post and watch videos, share information on events and music. Netlog users also can access information on brand pages by becoming fan of a company or brand, leave comments and participate at polls. A mobile application gives subscribers the opportunity to be connected everywhere. Subscribers must be at least 13 years old.

The following is a report of findings of the analysis of the self-declaration provided by Netlog and the testing of both the Dutch and the German versions of the website in Belgium and in Germany, respectively. The tests were conducted in December, 2010 – January, 2011.

Summary of main findings

Even though Netlog stipulates that subscribers must be older than 13 to register on the site, users younger than 13 can easily register by simply "faking" their year of birth[36.] Netlog offers a broad range of sophisticated privacy options. However, the default privacy settings of minors are not set to "private by default"[37] as defined in the Safer Social Networking Principles[38]. In fact, registered users, even adults that are not befriended with the minor, can see nearly the whole profile information including the school they attend, pictures or blog entries; but no contact details. Yet, users can easily restrict access to their profile or block specific users if they wish so. Moreover, SNS visitors who are not registered cannot view the profile. As far as contact possibilities are concerned, adult users can send a friendship request to minor users, but no accompanying personal messages can be added to motivate their requests.

Regarding the types of content minors are exposed to, when signed in as a 15 year-old child in both the German and the Dutch versions of the site, different types of advertising were displayed. Some of the banners included (fake) prize winning notifications and invitations to take part in lotteries by providing contact information. Although no advertising about alcohol was found, it was still possible for minor users to access some pages dedicated to alcohol brands by inserting brand names of famous alcoholic beverages in the brand pages search engine.

In relation to the reporting mechanisms provided by Netlog, these are user-friendly and age appropriate. Besides, Netlog provided a rather satisfactory personalised answer to the "bullying" report created for this test,

[36] The provider states that if moderators have doubts on a profile owner's age, e.g. because the user on the profile appears to be too young, ID is asked for.

[37] "Ensuring that setting a profile to private means that the full profi le cannot be viewed or the user contacted except by 'friends' on their contact list".

[38] http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

although only in the German case. The Dutch report remained unanswered and the offending content remained on the site.

Regarding the online safety information available on the site, The Safety Centre informs users on important safety issues such as privacy, grooming or cyberbullying and provides information and links to educational websites as well as tools for young people, parents and teachers.

Analysis of Results by Principle

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner

Main findings in relation to the self-declaration

According to its self-declaration Netlog provides *clear* guidance and safety information specifically targeted at children and young people on how to navigate their website safely (e.g. via diverse media, cartoons, videos, etc.). Most of this information is found in the Online Safety Centre which also provides useful links for parents and teachers in all Netlog languages. The Terms & Conditions, Privacy Statement, Code of Conduct and FAQs are easily and clearly formulated. Moreover, Netlog members are reminded about privacy options on various places throughout the site.

No explicit information on the consequences of inappropriate behaviour on the website is stated in the self-declaration. No available technological tools for parents in order to monitor their children are found on the self-declaration, either.

Main findings in relation to the website

As stated in its self-declaration, the Dutch version of Netlog dedicates several web pages to e-safety. The Safety Centre is divided into dedicated sections for youngsters, parents, teachers and police forces, next to a general online safety webpage. The safety information includes links to the Terms of Use, Privacy Statement, FAQ, etc. and is accessible for both registered and non-registered users from the footer of the homepage and each other page. The German version of Netlog does not provide any targeted information or educational materials for parents and teachers on how to foster children's responsible and safer internet use[39].

In the section targeted to young users in the Dutch version of Netlog, e- safety tips are formulated in short and easy to understand paragraphs (e.g. choosing a strong password, being careful with personal data, etc.). Users are also informed about possible abuses and contact-related risks such as cyberbullying or grooming. The German version of the site, however, provides very little safety targeted guidance and educational materials. In both language versions, although some links to other awareness raising organizations are announced at the bottom of the online safety page dedicated to youngsters, these links could not be found during the test.

The Safety Centre in the Dutch version of Netlog provides some cartoons and videos on popular e-safety issues. However, the majority of the videos are from foreign awareness raising campaigns in English. Yet, they are accompanied by short and practical texts in Dutch that summarize specific risks and tips to cope with them. On the contrary, the German version of Netlog did not provide any audio-visual material at the time of testing, although later on it was possible to find such information on the site.

In both language versions, the Terms of Use are only presented in textual format. They explain different aspects of forbidden uses and behaviours on the site. Although this text is well structured, some paragraphs include specific jargon (e.g. "legal competence", "free from liability") that may be difficult for young users to

[39] According to the provider the new version of the Security Center would be launched on February 8th, on the Safer Internet Day.

understand. Moreover, the text is long and, thus, not appealing to a (young) audience. A Code of Conduct summarizes prohibited conducts, in short and generally easy to understand paragraphs. However, in some parts specific (judicial) jargon (e.g. intellectual property) is still used in both language versions of this text.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience

Main findings in relation to the self-declaration

In its self-declaration Netlog states that the minimum age requirement to create an account in Netlog is 13. Minors (older than 13) can register on Netlog but they need parental permission to be able to do it. Parental consent is, thus, the only mechanism through which this service provider promotes the uptake of parental controls. If Netlog happens to find out that someone is lying about their age, the account is blocked. The self-declaration does not include information on the steps taken by the provider in order to prevent users from attempting to re-register with a different age if they have previously been rejected for being below the minimum age.

Netlog refers to several mechanisms to ensure the limited exposure to potentially inappropriate content and contact by children (e.g. "closed" privacy settings of minors which do not allow adults to contact or search for minors; pictures and videos are moderated upon upload and blocked items are hashed so it is not possible to upload them again; etc.). Netlog also restricts some brand pages, ads and applications (e.g. alcohol-related ones) to ensure that they are only accessible to adults while only safe advertising banners are displayed on the site. Furthermore, content on Netlog is automatically filtered according to the user`s age and location so as to ensure that minors only see content posted by other minors and not by adults.

Main findings in relation to the website

In both language versions of Netlog, the provider clearly states in the Terms of Use that minimum user age is 13 and that nobody below that age can register. Netlog promotes the uptake of parental controls by writing in their Terms of Use and the Security Centre that minors need parental permission to register on the site. However, no documents signed by parents or any other proof of parental consent needs to be handed in order to become a registered user.

In both language versions of Netlog tested, when a visitor wants to register, some basic personal data have to be provided, including the date of birth. The year of birth has to be selected from a drop-down menu (earliest year is 1997). Although in theory, visitors younger than 13 cannot select their real year of birth, the test in both language versions showed that children younger than 13 can easily subscribe by selecting a *suitable* year from the list. To subscribe (young) users need to entrust some personal data (forename, family name, gender and birth date) and if they wish so, they can add their place of residence, studies, school and contact details like e-mail, MSN, Skype account. In what the provider calls the *interview*, a user can add a lot more personal information ranging from hobbies to favourite brands. However, contact details are not accessible for adult users who access the profile, only minor users.

The welcome page of Netlog includes the so-called spotlight: Pictures and blog entries other users want to present in this 'spotlight' are displayed here. When signed in as a minor, only contents provided from other minor users were shown. Even though in its self-declaration Netlog claims that content is automatically filtered according to the user`s age and location (so that minors can only see content posted by other minors and not by adults), the test in both language versions of the site revealed that minors can visit profiles of adults and see their content (e. g. pictures, videos and so on) without any restrictions.

Regarding advertising, when signed in as a 15 year-old child in both the German and the Dutch versions of the site, different types of advertising were displayed. Some of the banners include (fake) prize winning notifications and invitations to take part in lotteries by providing contact information. Small banners as well as *intermercials* (an internet commercial for a new movie, for instance) were also found. As opposed to what is claimed in the self-declaration, in the *brand pages'* section, it was possible for a 15 year old to consult pages about alcohol brands.

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

Although in its self-declaration Netlog indicates that "privacy settings of all minors are "closed" (Principle 2), the self-declaration also indicates that *all* users have the possibility to "tailor their availability and visibility to others" through an extensive range of privacy settings" so it is not really clear to what extent the profiles of minors are effectively "closed" especially considering that users can "choose who can contact them". Furthermore, the definition of "closed" profiles of minors does not fit the definition of "private by default", i.e. only available to user`s approved contact list, stipulated in the Safer Social Networking Principles.

Apart from requiring parental consent of minors to register on the site (Principle 2), the self-declaration does not provide any further information on how Netlog supports parents be aware of the existence of other available safety tools/information (such as filtering tools or parental controls) to help them protect young people online. The self-declaration does not explicitly mentions how the safety tools and technologies employed by this SNS to ensure a safer experience for children and young people are assessed to ensure their effectiveness, either.

Main findings in relation to the website

In both language versions tested the profiles of minor Netlog users are not set to "private by default"[40] as defined in the Safer Social Networking Principles[41]. As a matter of fact, all Netlog users (including adults who do not belong to the minor`s approved contact list) have access to minors` profiles and are even allowed to send friendship requests by simply inserting the forename of the minor in the Netlog search engine. By contrast with adult users, minor users can also send personal messages. Adult users are not able to send personal messages, except when they are befriended. This contradicts the self-declaration`s statement that "Privacy settings of minors are "closed", i.e. they cannot choose to show their profile to everyone.

As revealed by the test, profiles of minors can only be found by other Netlog users, though, (and not via external search engines) and adults trying to access minors' profiles are warned that they are going to access a profile of a minor. Yet, access is given immediately after closing this warning. Adults can, thus, easily see nearly the whole profile information of minors, such as personal data, pictures, blog entries with the sole exception of the minor`s contact details.

When visiting the profile of the minor and trying to write a comment in the guest book or next to pictures, a warning is given. Due to the fact that the profile owner is a minor, adult visitors (who are not friends) are not able to post comments; however, they are still able to send a friendship request to minors, without comments, and may eventually become their friends. In other words, adult users can only send an unmotivated friendship request to a minor.

As the test in both language versions shows, by default, when friends post comments, they appear immediately on the profile. However, this can be restricted so that the (young) user can approve comments before they are published. Users can also delete comments that have been inserted by their friends. When clicking on the "more settings" link, a user can decide whether ratings and comments are permitted on their profile or not (by default permission is given), or who can see their pictures (by default every Netlog member). In short, technical guidance is given and privacy settings can be adapted. Although no specific warnings are given when uploading a picture, the user can see the privacy settings next to the uploaded photo. Direct access is given to adapt

[40] "Ensuring that setting a profile to private means that the full profile cannot be viewed or the user contacted except by 'friends' on their contact list".

[41] http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

viewing, commenting and rating by other users. Besides, users are informed by e-mail when another user has tagged them in a picture.

Besides, in both language versions tested, users had the option to make their profile only accessible to members of Trust[42], i.e. Netlog users who are committed not to abuse the site. Profile owners can choose who is able to contact them also by using a «whitelist» and block certain users from accessing their profile by means of a «blacklist». These options can be easily found in the profile settings section. Brief and clear explanations are given in this section as well as the FAQ.

As the testing in both language versions shows, in general, most privacy settings are clearly defined and easy to adapt and users can restrict the access to their profile to friends and eventually the friends of their friends. Users can also restrict access to specific age groups. When registering as a 15 year-old, for instance, and selecting the option to restrict profile access to some SNS users, it is suggested to restrict the profile to users between 13 and 20 years old.

Apart from the parental consent referred to in Principle 2, Netlog does not provide any other tools or information to educate parents about available mechanisms to help them protect their children online.

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service

Main findings in relation to the self-declaration

The self-declaration indicates that all Netlog visitors, registered and not, can easily report inappropriate content by clicking on the report abuse button found next to all types of user-generated content (profiles, pictures, blog messages, etc.). To facilitate reporting a list with the most common reasons for submitting a report is provided so that users can easily select the type of abuse they have been confronted with. Apart from the report abuse buttons it is possible to send reports via specific e-mail addresses, postal address, helpdesk and fax. Trained Community Managers and Assistants check these reports 24/7 and prioritise them according to the amount of complaints. Besides, there are Netlog volunteer moderators who can support users solve their enquiries.

The self-declaration neither includes information on if the reports are acknowledged nor if users are provided with an indication of how their reports are typically handled.

Main findings in relation to the website

Both language versions of Netlog provide two mechanisms to report inappropriate content: First, a report abuse button is provided. As stated in the self-declaration, this button can be found next to user generated content (e.g. comments on a profile, e-mails, pictures/videos). It is easily accessible and clearly identifiable as it represents the figure of a policeman. A click on this button opens a short and easy to use online form where users can indicate which kind of abuse they have been confronted with (e.g. sexually explicit material, child abuse, violence, etc.). Reporting can also be done via email. This might be not so easy to do for young people as they first have to search the email address located in the Code of Conduct or in the Terms of Use.

In both versions of Netlog tested, although the report mechanisms are clearly present in several parts of the SNS, no information could be found explaining how the reports are handled. In the Terms of Use the provider states that if the complaint is grounded, measures will be taken (like putting offline the illicit content). However,

[42] Trust is Netlog`s security label that confirms the users `commitment not to abuse the site “for spamming, uploading pornographic material, disturbing users, stalking, paedophilic activity, or using the site for ulterior purposes for which it was not intended”. Trust members are thought to be less likely to breach the Code of Conduct because in case of abuse from a “Trusted member”, they can be identified /blocked by using a mobile phone number instead of an IP address.

which concrete steps are taken and the time needed to respond, are not dealt with. The documentation about how users can report abuse and misbehaviour includes textual information about possible punishments of abuse. In the Dutch version of the site users are given information on how to contact eCops, the Belgian governmental contact point for internet abuse. Registered users can also find the number of the Belgian hotline and its e-mail address. In the German version a link to eCops is provided, but no further information on how to contact them.

As part of this study, a (fake) minor user reported that she had been bullied on this SNS. A realistic bullying situation was set up between the (fictitious) owners of profiles that were created for this assessment. The scenario consisted of one minor being bullied by two other minor users who posted a nasty comment on the wall of the "victim" and who uploaded and sent hurtful pictures. As the "victim" could not cope with the nasty comment put on her profile and the embarrassing pictures, she contacted the provider. In Belgium, the "victim" sent a report via the report-abuse button that was visible next to the embarrassing pictures. An online form popped up where the user could select a reason for the report (in this case *bullying*, «*pesten*», was selected). The online form included also a field where the user entered more details concerning the abuse. After sending the form a message appeared on the SNS webpage confirming that the report had been sent. The same day, a message was received confirming the reception of this report and that a moderator would deal with the abuse. However, no further reply was received during the month following the abuse report. Moreover, the embarrassing pictures and comments used in this bullying scenario were not removed and no measures were taken against the "bullies". In Germany the same bullying situation was set up, but this time the bullying report was sent via email. The test e-mail was answered the day after. It was friendly and explained that it was possible to put the two bullying users on the blacklist. The personal answer was written explicitly for the test bullying report (no standard text was sent). However, this message only told that it was possible to put the two bullying users on the blacklist but not how to delete the content. The 'victim' sent another email asking how to delete the bullying content (December 20th, 14:49). This e-mail was replied by Netlog 2 days later asking where the offending pictures were located, but not instructing Astrid on how to delete the offending content. This last e-mail was never replied by the minor. However, explicit information regarding where the offending content was located and who the bullies were had been explicitly provided in her first e-mail. Still, the embarrassing pictures and comments were not removed from the site and the bullies were not reprimanded for their inappropriate behaviour.

In sum, the reporting mechanisms provided by Netlog are user-friendly and age appropriate. Besides, Netlog provided a rather satisfactory personalised answer in the German case. However the Dutch report remained unanswered.

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

Netlog states that they report all law violations (racism, child porn, etc.) to eCops, an online reporting service of the Belgian federal Computer Crime Unit. In case of international crimes, Netlog transfers the issue to their international associates. But it is not explicitly mentioned if they have effective and expeditious processes in place to review and remove offending content.
In case of offences that are prosecuted only upon complaint, Netlog guides the members to the right authority.
Netlog claims to liaise with police officers from the Federal Crime Unit about actions taken by Netlog and constantly receives information from the police on new techniques employed by, for instance, paedophiles. With this feedback Netlog is not only able to improve and develop automated tools to protect its younger members, but also to continue training the Community Managers and Administrators so that they can detect such behaviour. Finally, Netlog saves all data in case the police may need it.

Because of ethical reasons, Principle 5 was not tested in the website.

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

Main findings in relation to the self-declaration

According to its self-declaration, users of Netlog are provided with a range of privacy setting options and with supporting information to help them make informed decisions about the information they post online. Indeed, Netlog's safety centre and FAQ provide information on how to ensure online safety in general. Trained staff safeguards users` safety and reacts promptly if users` privacy is endangered. During registration, Netlog asks very basic information only. Users then decide by themselves what other information they want to share on their profile.

The self-declaration does not specify if the privacy settings options are prominent and accessible at all times. Netlog does not include information on if users' information (provided during their registration) is automatically uploaded onto their profiles.

Main findings in relation to the website

As stated in the self-declaration, in both language versions tested, Netlog provides clear and easy to use privacy settings. Besides, during the registration procedure, a user only has to provide few mandatory personal data (name, e-mail, date of birth, chosen password)[43]. While registering, a link is provided to the Terms of Use (including a link to the privacy statement). Registration is only active when the new user clicks on a hyperlink sent to the disclosed e-mail address. By default, all the personal information that is provided by the user, such as information in the interview, pictures, comments on pictures and videos, is shown in the profile of minors. However, the user can decide not to include personal information in the profile by "unchecking" the box next to a specific piece of information. Users can also conceal their online status.

Netlog provides a range of privacy settings regarding the four categories "To be found", "Access to profile", "Communication" and "Logs" (comments and changes of the profile visible for friends). Members can also choose one of the following basic settings: use their profile to meet new people (choice for basic privacy settings or high level of privacy protection), or to keep contact with the friends they already know (with also two levels of privacy). The privacy settings provide other functionalities as well, such as allowing users to pre-approve comments published to their profile.

The starting page of the privacy settings gives a clear overview of the settings linked to a specific privacy set. Yet, individual settings can be viewed and be easily adapted at any given time. In the Dutch version of the site additional information regarding privacy issues is given in other parts of the SNS as well. In the Safety Centre, for instance, users are informed about how they have to protect sensitive data like passwords and how they have to react on requests to provide sensitive information.

Although the Privacy policy is long (60 lines with a total of more than 600 words), it is well structured and essential information is included. The categories of personal data that are processed as well as the purposes of the data processing and users' privacy rights are summarized. Some technical terms are also clearly defined in footnotes, e.g. cookies.

Finally, if a user wants to delete their profile, this can be found under settings, in the account section where a user is given the possibility to delete the profile. Moreover, information is inserted on how to delete your account in the FAQ-page (settings section).

[43] Also a CAPTCHA is used in the subscription form: *Completely Automated Public Turing Test to tell Computers and Humans Apart* is a challenge-response system test designed to differentiate humans from automated programs (searchsecurity.com).

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

Main findings in relation to the self-declaration

According to the self-declaration, Netlog assesses their service to identify potential risks to children and young people by engaging in debates with users, NGOs, police authorities and governments to assure that all these systems are constantly improved. Among others, Netlog participates in regular brainstorming meetings with the Belgian Federal Computer Crime Unit to update and build automated tools to protect its younger members (See Principle 5).
Nothing is mentioned on the steps taken by Netlog to minimize the risk of employing candidates who may be unsuited for work which involves real-time contact with children or young people.

Principle 7 was not tested in the website.

Summary of Results and Conclusions

According to its self-declaration, Netlog has implemented Principles 1, 3 and 4 rather satisfactorily, Principle 6 very satisfactorily and Principle 2 unsatisfactorily on its website. The testing on the website revealed some problematic areas, for instance:

- Although the privacy settings are said to be «closed» for minor users, still all registered users can, by default, have access to the minor's profile. In other words, minors' profiles are not set to "private by default" as defined in the Safer Social Networking Principles.

- Even though the minimum age requirement is supposed to be 13, visitors younger than 13 can easily register on the site.

- Even though the self-declaration states that parental permission to register on the site is required, this was not validated in the testing.

- Even though in its self-declaration Netlog claims that content is automatically filtered according to the user`s age and location so that minors can only see content posted by other minors (and not by adults), there are no restrictions for minors to visit profiles of adults and see their profile content (e. g. pictures, videos, etc.).

- As opposed to what is claimed in the self-declaration, in the brand pages' section it was possible for a 15 year old to consult pages about alcohol brands.

- The reporting mechanisms provided by Netlog are user-friendly and age appropriate. Besides, Netlog provided a rather satisfactory personalised answer in the German case. However the Dutch report remained unanswered.

Assessment of all the Principles in the Self-declaration

Principle	*Very satisfactory*	*Rather Satisfactory*	*Unsatisfactory*
1		x	
2		x	
3		x	
4		x	
5		x	
6		x	
7		x	

Implementation of the Self-declaration on the SNS

Principle	*Very satisfactory*	*Rather satisfactory*	*Unsatisfactory*
1		X	
2			x
3		x	
4		x	
6	x		

ONE.LT

Rita Žukauskienė, Mykolas Romeris University, Lithuania
Verónica Donoso, Appointed Research Coordinator by the EC

Introduction

ONE.LT is a SNS in Lithuania operating in Lithuanian and Russian languages. The total number of users is not known, however, statistics show that by December 2010, ONE.LT had 709, 200 active users[44]. ONE.LT was founded in 1999. It is an online community where members can find and communicate with others as well as to browse and share user-generated content. Users must be 14 or older to use the service. Users interact with friends' profiles, send messages to other users, join groups, upload and share photos and videos. Each member creates their own personal page called a *profile*, on which they can post their own content. Among other functionalities, users can create profiles containing personal photos, establish friends' connections with other users on the site, exchange private in-site messages, post notes to forums attached to individual user profiles or user groups, rate user photos, etc.

The following is a report of the findings of the analysis of the self-declaration provided by ONE.LT and the testing of the Lithuanian version of its website. The test was conducted in December, 2010 – January, 2011.

Summary of main findings

Minors younger than the minimum age requirement of 14 years old were able to sign on ONE.LT and were not restricted to any (adult) information available on the website (including sexual content, violence, descriptions of human abnormalities, etc.). Moreover, they could be contacted by unknown adults and there were no restrictions to add adults to their "friends".

Minors' profiles are not set to "private by default" as defined by the Safer Social networking Principles and so practically any user of ONE can have access to their profile information and even contact minors (e.g. by writing in their forum). The main problem is that ONE.LT demands a considerable amount of personal information during the registration process including details of the user's real name, age, place of residence and mobile phone number. All this information is automatically inserted into the profiles of minors and is made available beyond the user`s approved contacts list.

ONE.LT provides some privacy setting options. Privacy settings include the option to choose if personal information such as the telephone number is visible to everyone, to friends only or to nobody, and if the person can be reached by friends only or by anyone.

Seeking help because of inappropriate contact, content or conduct is possible only via e-mail. However, as the test on the site shows the reporting mechanism is not really efficient. Only ten days after having contacted the provider to report a test "bullying" situation the "victim" received a reply from ONE.LT stating that her message had been received and that the photo album with offensive pictures had been removed. However, the nasty comments posted on the minor`s profile remained on the site and no actions were taken against the "bullies".

ONE.LT provided basic safety information for Internet use for children and parents, but the available information for parents is mostly focused on basic principles of good parent/child communication and health issues related to computer use rather than on effective and concrete safety measures.

[44] http://w27.ONE.LT/welcome?language=lt&tkn=6851 (Retrieved on Dec. 15 2010)

Analysis of Results by Principle

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner

Main findings in relation to the self-declaration

According to its self-declaration ONE.LT provides plenty of textual and audio-visual guidance and safety information for its users and their parents on how to navigate the website safely, for instance it claims to maintain a dedicated “Your Safety” section easily accessible from every page on the site. ONE.LT also claims to provide educational video materials (in prominent positions on the site) as well as sending its users “periodic safety reminders” containing tips on key safety issues.

The self-declaration does not specifically refer to the existence of “Terms of Use” or any other specific document containing the rules that govern the site. However, it does specify what is considered as inappropriate behaviour on the site (e.g. attempts to distribute or collect child pornography or any other type of “age-inappropriate content”). Besides, it provides information on the consequences of inappropriate behaviour on the website including the temporary suspension or permanent removal of user accounts and the reviewing and eventual removal of inappropriate or illegal visual content, user groups or their components.

The self-declaration does not mention if the website offers parents and/or teachers any types of technical controls to support the safety of children online apart from the general safety and privacy information aforementioned which, by the way, is not specifically targeted at teachers, but at general users and their parents.

Main findings in relation to the website

Testing found that not only the “Your Safety”, but also the “Privacy” section and the “Terms of Service” (Naudojimo Taisyklės) are accessible from a hyperlink in the footer of the homepage (and also on every page of the site).

Confirming the analysis of the self-declaration, testing shows that ONE.LT provides safety information for parents and young users, but it does not provide educational materials for teachers. ONE.LT maintains an easily accessible “Your Safety” section where concrete tips and advice are given to users on how to ensure their safety online. The general safety information is easy-to-find and easy-to-understand. The same cannot be said of the Privacy and the Terms of Service information, though. This information is quite dense and is full of legal and technical jargon. However, adapted child-friendly information concerning the rules governing the site was found in an especially dedicated section for Youth. These rules include information on what constitutes inappropriate behavior on the site and the consequences of breaching such terms.

The information for parents is very basic and is only related to general (safe) Internet. In particular, parents are neither informed about the types of personal information children are required to provide in order to register on the site nor are they given any explanations about the (personal) data their children might be able to post on the portal or any other potential contact or conduct risks associated to using SNSs in general. The safety information for parents and youth is text-based only. Links to external safety information (“Safer internet”, http://www.draugiskasinternetas.lt/en) are also provided in the safety information section devoted to parents.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience

Main findings in relation to the self-declaration

In its self-declaration ONE.LT states that the minimum age requirement to create an account on this SNS is 14. In relation to the steps taken by the provider to prevent users from attempting to re-register with a different age if they have previously been rejected for being below the minimum age, ONE.LT demands users to provide a valid mobile phone number during the account registration stage. ONE.LT claims that this mechanism would "limit the ability of young users to create multiple profiles at will" and would facilitate "parental control". Apart from this no other mechanisms to promote the uptake of parental controls are mentioned in the self-declaration.

In its self-declaration ONE.LT refers to diverse mechanisms through which the service provider ensures limited exposure to potentially inappropriate content and contact for children, for example by means of the "collaborative peer review" process of profile pictures, by not allowing "adult-oriented" content/advertising on the site (although it is not clearly stated what is considered as "adult-oriented" content), or by filtering inappropriate words/expressions in user messages and forum posts.

Main findings in relation to the website

ONE.LT relies on the self-declaration of age by the user in the registration process as the key mechanism for ensuring that the services they provide are age-appropriate for their audience. ONE.LT self-declaration indicates that users must be 14 or older to use ONE.LT. However, the test on the site demonstrated that children below the minimum age requirement can still register on the site without any trouble, even by providing their real age. Thus, it was possible to sign up as a 9 and as a 13 year old. Indeed, while creating these profiles, age was calculated and automatically inserted into the underage user profile so that their real age (9 and 13) was displayed on their profiles in spite of the minimum age requirement of 14.

During registration a valid telephone number is required. This telephone number is automatically inserted into the user profile and is, by default, only made available to the users' accepted contacts list. Although, this information could, eventually, be made available to users who pay for the "search for all" functionality, explained in detail under Principle 3.

Once registered, the user may change their age in the profile as many times as they wish and they can display their age to "friends only", or to nobody. During the period the test lasted no (visible) steps were taken by the provider to delete the "under-age" users (created for this test) from its services. Besides, no effective parental control tools were found on the site, either. Indeed, during the test it was observed that users are asked to use a valid mobile phone number account at the registration stage. Theoretically, and as stated in the self-declaration, this control mechanism should limit the ability of young users to create multiple profiles and could make parental control easier. However, in practice it is not fully effective because, as demonstrated by this test, minors could still buy cheap pre-paid mobile phone cards to create multiple profiles.

In relation to the type of information accessible, when signed in as a minor (13 and 15 year olds) minors have access to the photo albums of all (adult) registered users, including "top" photo albums which usually contain highly sexy photos and not always appropriate comments about them. Regarding advertising displayed on the site no potentially inappropriate content for minors (e.g. alcohol, cigarettes, etc.) was observed. Eventually, users have the possibility to (temporarily) block advertising (including banners) if they pay a certain amount of money.

The mechanism offered by ONE.LT to filter inappropriate words/expressions was also tested. Swear words in Lithuanian were submitted to one of the minors' forum (created for this test). Immediately, this message appeared in the victim's forum. However, the offensive language was neither banned nor removed from the site, what suggests that the filtering mechanism to detect inappropriate words/expressions is not really effective.

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

According to the self-declaration, ONE.LT stipulates that all user profiles can be searched by using the internal profile search, but that the actual content of user profiles (not only of minors) can *only* be viewed by "people belonging to the user`s extended circle of trust (friends, friends of friends). Clearly, the “extended circle of trust” involves more than only ‘friends’ on the minor`s contact list and thus, we can conclude that the profiles of users younger than 18 are not set to “private by default”[45] as defined in the Safer Social Networking Principles[46].

The self-declaration refers to some mechanisms employed by ONE.LT to assist children and young people in managing their experience on their service, particularly with regards to inappropriate or unwanted content or conduct, for instance, users can control their personal data and can decide who can view/access their personal information, “collaborative peer review process” to identify and spot potential inappropriate content, new friend connection invitations submitted by users who have been previously blocked by a user are ignored and not displayed to the user. Furthermore, the self-declaration also mentions that “apart from the front page (login screen) no section on the site can be viewed by an unregistered user regardless of his/her age which would make profiles unsearchable from external search engines, and would, thus, limit the risk of children being contacted by strangers.

The self-declaration does not provide any further information on how ONE.LT supports parents be aware of the existence of other available safety tools (such as filtering tools or parental controls) to help them protect young people online. However ONE.LT claims to offer parents, carers and/or teachers targeted links and educational materials.

Main findings in relation to the website

Regarding the searchability of minors `profiles, and as stated in the self-declaration, it is not possible to avoid being found via the internal search engine of the SNS, however, the information made available to other ONE.LT users depends on the personal privacy settings set by the user. The default profiles of minors (or of any other ONE.LT user) are not searchable via search engines such as Google, Yahoo, etc. When searched inside the SNS, "not friends" cannot get immediate access to a user`s personal profile because the internal search engine only offers, by default, the option to “search among friends”. However, there is an “alternative” paid search option called "search for all” that allows registered users (who pay approx. 0.58 €) to search for as many contacts as they wish for during a 30 day period. This “search for all” engine enables registered users, even adult strangers, to see the whole minor’s profile (which by default includes personal information such as the minor`s telephone number) plus photo albums and messages in the minor’s forum. However, if the minor has set additional privacy settings to protect their personal information, then this information is kept as “private” even for users who have paid to “search for all”.

Furthermore, minors can always be contacted by any user via posting a message in their forum or via e-mail (if their e-mail address is not set to “private”). On ONE.LT it is possible to “reject” friends` requests. However it is not possible for users to configure their account to allow only ”friends” to post comments on their profiles or to pre-moderate or to delete unwanted content/comments before they are published onto their profile. However, users may choose to change their settings to more private or public at any time.

It is possible to block a user, to delete a posted message, and to report unwanted contact/content via e-mail to ONE.LT. Besides, it is also possible to delete own/others messages in the forum; however, what the self-declaration does not mention is the fact that ratings and comments on photos can be deleted only by paying a specific amount of money (charged via the telephone account).

Confirming the analysis of the self-declaration, we can conclude that full profiles of minors in ONE.LT are not set to “private by default” because minors can be viewed and even contacted by people beyond their approved contacts list.

[45] “Ensuring that setting a profile to private means that the full profile cannot be viewed or the user contacted except by ‘friends’ on their contact list”.

[46] http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service

Main findings in relation to the self-declaration

The self-declaration refers to several mechanisms to report inappropriate content, contact or behaviour. In particular, ONE.LT claims that uploaded images can be reported by simply clicking on the corresponding reporting button placed close to every picture. This would initiate a review of the reported image(s). In relation to reporting other types of content, the self-declaration indicates that users are encouraged to send a message to the customer service whenever they "suspect inappropriate behaviour or content". In their message they should include a link to the "inappropriate" content in question.

The self-declaration does not explicitly mention if the reporting procedures are *easily understandable* for children and young people or if they are *age-appropriate.* But it does mention that reports are *efficiently* handled. Finally, users are provided with the information they need to make an effective report via periodic reminders sent to them in the form of administrative messages or as internal banner ads.

Main findings in relation to the website

ONE.LT provides a mechanism for reporting inappropriate content, contact or behavior. Seeking help because of inappropriate contact or conduct (e.g. bullying in the case of this test) is only possible via e-mail.

As part of this test a bullying situation was created where one of the "minors" (created for this test) was "bullied" by another one by posting nasty comments in the forum of the "victim". It was not possible for the "bully" to upload abusive pictures on the "victims' forum", however, the "abuser" created a photo album on her own profile including the offensive pictures and shared the link with others. As the "victim" could not cope with the nasty comment put on her profile and the embarrassing pictures, she contacted the provider.The only way for her to reach ONE.LT was to send an e-mail to administration. The report message appeared in the "victim's" "sent" messages folder indicating that the report had effectively been sent. Only ten days later, the "victim" received a reply from ONE.LT stating that her message had been received and that the photo album had been removed. However, the nasty comments remained on the site and no actions were taken against the "bullies". In sum, the test shows that the reporting mechanism is not really efficient.

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

In the self-declaration ONE.LT claims to have designed and implemented efficient internal procedures for responding and acting upon notifications of illegal or inappropriate content or conduct observed within the site environment. They also claim to efficiently review and verify the received reports and the potential offending content and to take appropriate actions accordingly. These may include, for instance, removing the verified inappropriate or illegal visual content, suspending or eventually permanently removing user accounts, etc. Finally, direct hotlines connecting ONE.LT customer service staff on duty with appropriate safety-related networks such as INHOPE, Cyberpolice unit, etc. have been installed.

Because of ethical reasons, Principle 5 was not tested in the website.

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

Main findings in relation to the self-declaration

According to its self-declaration, users of ONE.LT are provided with a range of privacy setting options and with supporting information to help them make informed decisions about the information they post online. For instance, at any time ONE.LT users can easily customize their privacy settings and determine which part of their data (including the user's age, phone number and email address) to share with whom (everyone, just first-level friends, or no one). In the "Your Security" section ONE.LT offers "accessible" information and advice for users on how to safely manage and protect their personal information and privacy while using the site (e.g. how to protect the user's passwords, how to properly log out of the site after finishing a usage session, etc.).

The self-declaration does not mention if the service provider automatically maps information provided by users (during registration) onto their profiles or if users are made aware when this happens.

Main findings in relation to the website

On its website ONE.LT provides some privacy setting options. Privacy settings include the options to choose if private information such as age, telephone number and the e-mail address are visible to friends only, to nobody or to everyone. Minor users can also set their profile to be contacted by friends only or by anyone. Disclosing of mobile phone number and e-mail address is optional. Users are able to access and alter their privacy settings at anytime. There is a possibility to show or hide online status, but this option (as well as several other functionalities on the site) is not free. It is also possible to choose which actions will be seen by others or not, e.g. when a person starts a new group, writes messages, starts a friendship, and joins a new group.

ONE.LT asks for a considerable amount of personal information during the registration including details of the user's gender, age, place of residence, and mobile phone number. This information is automatically inserted into their profiles of minors without making them aware that this is happening. However, the site also provides accompanying safety information and gives users advice on the importance of protecting their personal data (e.g. Tips on how to protect one`s password or how to properly log out from the site).

In conclusion, default privacy settings do not secure that private information will only be made available to the "extended circle of trust", therefore minor users will need to perform additional steps to acquire real privacy. These steps may include changing one`s privacy settings or acquiring VIP status (for extra money). VIP status allows users to protect themselves from "Invisible guests" and to become a "guest" (i.e. a privileged user who can see any profile on ONE.LT, rate the personal albums of any person visited on this SNS, etc.). During the testing it was discovered that once a user pays, it is possible to see any person's photos and online/offline status, including those of minors. However the VIP user could eventually be blocked, thus preventing them from having access to one`s profile.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

Main findings in relation to the self-declaration

ONE.LT claims to ensure the continuous improvement of its reporting mechanisms for inappropriate and illegal content/conduct by means of the feedback gathered from relevant stakeholders such as users, NGO`s, government regulators and law enforcement.

As mentioned in Principle, ONE.LT claims their Customer service staff to efficiently review and verify the received reports and if potential offending content is identified, they take appropriate measures accordingly. ONE.LT also claims to continually track their staff and record their performance internally "to ensure that they are able to identify actionable cases and have the knowledge required for taking appropriate action in every case". Besides, this tracking system would also ensure the "optimization of respective procedures and policies." It is not clear from the self-declaration if these employees are in real-time contact with children or young people or if they only review the reports.

Principle 7 was not tested in the website.

Summary of Results and Conclusions

According to its self-declaration, ONE.LT has implemented Principles 1 and 4 rather satisfactorily, and Principles 2, 3 and 6 unsatisfactorily on its website. The testing on the website revealed problematic areas such as the following:

- Even though the minimum age requirement is 14, visitors younger than this age can easily register on the site.
- Minors' profiles are not set to "private by default". The main problem is that ONE.LT asks for a considerable amount of personal information during the registration including details of the user's real name, age, place of residence and mobile phone number. All this information is automatically inserted into the profiles of minors and can be made available, without the minor user knowing, beyond the user`s approved contacts list.
- Seeking help because of inappropriate contact, content or conduct is possible only via e-mail. However, as the test on the site shows the reporting mechanism is not really efficient. Only ten days after having contacted the provider to report a test "bullying" situation the "victim" received a reply from ONE.LT stating that her message had been received and that the photo album with offensive pictures had been removed. However, the nasty comments posted on the minor`s profile remained on the site and no actions were taken against the "bullies".
- Minors younger than 14 years old were able to sign up and were not restricted to any information available on the website (including sexual content, descriptions of human abnormalities and violence).

Assessment of all the Principles in the Self-declaration

Principle	*Very satisfactory*	*Rather Satisfactory*	*Unsatisfactory*
1		x	
2		x	
3		x	
4		x	
5	x		
6		x	
7	x		

Implementation of the Self-declaration on the SNS

Principle	*Very satisfactory*	*Rather satisfactory*	*Unsatisfactory*
1		x	
2			x
3			x
4		x	
6			x

RATE

Andra Siibak, University of Tartu, Institute of Journalism and Communication, Estonia
Verónica Donoso, Appointed Research Coordinator by the EC

Introduction

Being launched in May 2002, SNS Rate is the oldest and most popular national language based SNS in Estonia. As the site is only available in Estonian, the majority of its 290 000 users (http://www.rate.ee/ads.php?act=1&lang=2) are Estonians or Russian-speakers living in Estonia. The main aim of the site is to offer a photo-rating service but also to provide the users with additional opportunities e.g. sending messages to other users, chatting in forums, keeping a blog, reading horoscopes, converging among different communities, playing games, etc. Additional "advantages" (e.g. upload one's photos to the site before the others; get a VIP status in a chat room, use the Compatibility-Meter in order to test one's compatibility with certain users from the opposite sex, etc.) are only made available for the users who have purchased SOL's, the monetary unit only applicable on the *Rate* website. There are no minimum age requirements.

The following is a report of findings of the analysis of the self-declaration provided by Rate and the testing of its website. The test was conducted in December, 2010 – January, 2011.

Summary of main findings

Both non-registered users of the site as well as users not belonging to the friends list of minors have, by default, access to their profile images, videos, blogs as well as almost all the personal information contained in the MSN account of a profile owner are made private by default.

Findings of the testing of SNS Rate indicate that Rate has taken steps to ensure their users` safety by informing the users about inappropriate behavior and content in their Terms of Use. A general overview about the Internet safety issues (both for children and parents) and links to additional information can be easily found on the site. Several opportunities are provided for reporting inappropriate content (images, private messages, comments, videos); users can easily reject "friends' requests" or block other users. All profile images (up to 10) need to be approved by the moderators.

Still, gaps in the safety issues remain, for instance, all the profile images and the majority of textual parts of the profiles are accessible to non-users; no parental controls are provided, only certain parts of the profile could be made "private" or "accessible to friends only"; misleading information is provided about blocking one's profile i.e. although the text under the box "block one's profile" claims hiding one's profile from other users i.e. so that the profile cannot not be found by the internal search engine, clicking the box also means that the entire Rate environment becomes automatically inaccessible for the profile owner; one is unable to delete the account at once, only to deactivate it. When reporting about inappropriate content e.g. inappropriate tagged images, the content is quickly marked as "forbidden" however it is not deleted by the moderators and hence it is still publicly available.

Analysis of Results by Principle

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner

Main findings in relation to the self-declaration

According to its self-declaration Rate provides clear guidance and safety information specifically targeted at children, young people and their parents on how to navigate the internet safely including information on the dangers associated to the internet and practical tips. In it self-declaration Rate does not specify if targeted materials for teachers or educators are provided and it does not include any information on specific educational materials, either.

The self-declaration indicates that the Terms of Service are easily and clearly formulated and are accessible from the footer of each page. The provider claims that the Terms of Service provide simple information regarding inappropriate behaviour on the site (e.g. "disclosing personal information to other people") as well as the consequences thereof (e.g. accounts may be suspended for breaching the Terms). The example given in the self-declaration is contradictory, though, because considering that the essence of any SNS is disclosing to some degree or another (some) personal information to share it with others, then almost all the activities of users on this SNS would have to be considered as "breaching the Terms".

No information on the available technological tools/controls for parents to support their children`s safe use of the internet (e.g. parental filters) is found in the self-declaration.

Main findings in relation to the website

Parents and children are able to find information about safety in the Internet Safety ("Internetiohutus") section. Information is provided as a short text, followed by a couple of links to additional websites. Confirming the analysis of the self-declaration, there are no educational materials targeting teachers. Besides, the available information is easily accessible from every page and mainly written in age-appropriate and non-technical language. Parents are advised to create a profile in Rate in order to monitor the online practices of their children. In case of problems, parents are suggested to contact Customer Service "Kasutajatugi"), or contact the police. In the Terms of Use the users are informed about what is considered as inappropriate content and behaviour on the site (e.g. one is not allowed to advertise one's company or services by sending or posting information about it anywhere on the site; users under 18 years of age are not allowed to post photos with alcohol, smoking tobacco/drugs or water-pipe; one is not allowed to use someone else's personal information on one's own profile, etc.) and users are reminded that in case of abuse the user will be punished (e.g. a warning may be sent by the moderators or the profile may be blocked without any further notice). Hence, in the Terms of Use the information mainly focuses on the appropriate use of images and much less on general user privacy and safety issues. Indeed, these issues are not even presented with clear section labels (e.g. Processing the Data ("Andmete töötlemine" and Terms of Use for OpenSocial applications "OpenSocial rakenduste kasutustingimused") so it may be difficult for minors (and for users in general) to figure out what type of safety information could be found under which section.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience

Main findings in relation to the self-declaration

The self-declaration does not refer to any specific steps taken by the provider to identify under-age users or to prevent them from attempting to re-register on the site. The self-declaration does not state any minimum age registration requirement, either. However, it is not clear from the self-declaration if this is because no minimum registration age applies in Rate or simply because the aforementioned information is missing.

The information that Rate provides in its self-declaration regarding the mechanisms to ensure the limited exposure of minors to potentially inappropriate content is very precarious. In fact, Rate only refers to one general available mechanism, namely, that the profile pictures are subject to the approval of the site's moderator (e.g. " adults posting pictures of children is not permitted", pictures displaying drugs or alcohol are not allowed on the site, etc. thus, pictures containing alcohol or children could be banned from the site.).

The self-declaration does not specify what types of services are considered as not appropriate for children and young people on the site (apart from alcohol-related content). Besides, it does not refer to the ways in which this service provider promotes the uptake of parental controls, apart from providing them with general safety information and tips (see Principle 1). Finally, the self-declaration does not refer to the existence of any means put at the disposal of users or content developers to age restrict, rate or label content where appropriate.

Main findings in relation to the website

There is no information provided about age restrictions i.e. the site is open to anyone, e.g. also for a nine-year old child, as the test on this website demonstrated. The age restrictions are clearly stated only in terms of uploading certain images. For example, the Terms of Use state that no photos of children from 0-6 should be uploaded on the site and no adult can post photos of children (not even photos of themselves as a child). It is also stated that photos that display minors consuming alcohol/drugs/tobacco/water-pipe cannot be uploaded, and the moderators have a right to decline photos where people appear to be drunk. When looking through the images most recently uploaded on Rate ("Uued") the users can automatically see the entries made by the users who belong in the same age group, however, confirming the analysis of the self-declaration, no additional means are provided by the SNS to age restrict, rate or label the content where appropriate. Parental controls are also not promoted by the site, but parents are advised to create a profile of their own in order to monitor their children.

When registering on the site both adults and minors need to fill in the same registration form, e-mail verification is needed only in order to make changes to one's profile. Users are unable to change their date of birth previously provided in the registration form unless they pay. The cost for changing the birth date is 3 SOL's. Several other services are available only in case you pay, e.g. uploading, changing and editing photos; rating the photos with the highest score; the amount of time it takes for the moderators to process your photos, etc. The cost of these services depends on the way one pays for them e.g. paying through an e-bank (1 SOL = 0.11 EUR), via SMS (1 SOL = 0.19 EUR), by making a phone call to a paid service (1 SOL =0.20 EUR), or by a special phone-card (1 SOL = 0.14 EUR). When signing in as minor, banner ads can be seen. The services and products advertised are not specifically targeted to minors, but they are not (potentially) inappropriate, either.

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

Rate self- declaration does not provide any information regarding if the profiles of minors are set to "private by default"[47] as defined in the Safer Social Networking Principles[48]. Besides, the self-declaration does not provide any information about the steps taken by the service provider to ensure that private profiles of users registered as under the age of 18 are not searchable via their services.

In relation to the tools and technologies employed by the service provider to assist children and young people in managing their experience on their service (particularly with regards to inappropriate or unwanted content/conduct), the self-declaration refers to only a few functionalities, namely, users can decide which parts of their profiles to make visible to whom (visible to friends or public), they can delete unwanted comments from their profiles (but nothing is mentioned about other types of content posted to their profiles), they can

[47] "Ensuring that setting a profile to private means that the full profile cannot be viewed or the user contacted except by 'friends' on their contact list".

[48] http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

block contacts and reject friendship requests and they can report inappropriate contact (nothing is mentioned about inappropriate content, though).

Apart from providing general e-safety information (and guidance) for parents (see Principle1), no specific tools to promote the uptake of parental controls (e.g. filtering software) or specific information about them are mentioned in the self-declaration.

Main findings in relation to the website

Profiles of minors are easily searchable by their nickname both in the service search engine and via Google (but not through Yahoo! or MSN search). No search engine (neither in service search engine nor Google, Yahoo, MSN search) is able to find Rate users by their full name. Full profiles of minors are not set to private by default. In other words, both non-registered users of the site as well as users not belonging to the friends list of the profile owner have, by default, access to their profile images, videos, blogs as well as all the textual information on the profile (e.g. birthday, place of residence, education, profession, etc.) except the e-mail and MSN account of a profile owner. These are available for the people in the friends list only, by default. All profile images (max. 10) need the approval of moderators; only photos in the photo albums need not to be approved.

Adults can send friend requests to minors even if they are not in the friends list of the minor, which the latter can easily decline. All registered users of the site are allowed to comment the photos of minors, however, the option is not available to non-registered users. All users can also easily delete comments, personal messages, and character descriptions they do not like. Deleting that content is free of charge. Deleting a contact from the friends list is also easy; however, even though the contact will not appear in the friends list of the user initiating the blocking, no changes occur in the friends list of the person being deleted from the list. Users can also easily block persons they do not want to get access to their profile. Although blocking seems efficient at first, after having been blocked the system informs the “blocked” person that even though they have been blocked it is still possible for them to have access to as much information contained in the profile of the user who blocked them as any other “non-friend” of the user, i.e. by default, basically all the private information except the contact details (see Principle 3).

Users can also block their own profiles; however, blocking in that context actually leads to the deactivation of one’s own profile (two months after the user`s last login). Hence the information given by the system provider is misleading because even though it rightly states that after blocking one’s profile the profile will not be searchable through a search engine and will not be accessible to other users, it is also true that after blocking one’s profile the entire profile is deactivated even for the profile owner themselves.

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service

Main findings in relation to the self-declaration

The self-declaration refers to two mechanisms to report inappropriate content, contact or behaviour, namely reporting abuse via the “Reporting Abuse Button” (e.g. for reporting pictures) and sending an e-mail to the webmaster in case of any violation of the Terms of Service. However, contacting the webmaster in case of violations of the Terms of Service does not seem the most appropriate nor the most logical option for users to report abuse because webmasters are normally associated with reporting technical problems rather than violations of the Terms of use.

The self-declaration neither includes information on if the reports of abuse are acknowledged nor if users are provided with an indication of how their reports are typically handled. The self-declaration neither provides information on if the reporting mechanisms are *easily accessible, easy to understand*, *age-appropriate* or *available at all times*.

Main findings in relation to the website

Rate provides several user-friendly and all time available options for reporting inappropriate content and behaviour. The “Report Abuse button” used for reporting about inappropriate content and behaviour can be easily found under every comment, community, photo, scrap, video, private message, etc. on the site. In case of problems users may also send a note to the Customer Service (“Kasutajatugi”) and not the webmaster, as stated in the self-declaration. The Terms of Use section also provides information about how to make an effective report and how the reports are usually handled (e.g. if the reply has been provided by the Customer Service, a notification in sent through the inside message system to the user who made the report). Moderators can also be asked for help by posting in a special section of a forum titled “rate.ee discussion” Link to the forum can be accessible from every profile by clicking on the application “In addition” (“Veel”) on the menu bar and choosing application of Forum.
Still, the site does not inform the users about these mechanisms in the Terms of Use. During the test a cyber bullying situation was simulated which consisted of sending nasty comments and photos to an underage user. As part of the test a bullying letter was sent to the Customer Service on the evening of December, 15. No acknowledgement and no reply was received. In the afternoon of 16 December the “Report Abuse button” was used for informing the moderators about the bullying situation. Using the “Report abuse button” is very convenient and easy and the moderators` response to the problem took approximately 2.5 hours). Even after receiving a positive automated reply in answer confirming that the tagged photos were “forbidden by the site”, the tagged photos were only deactivated and not entirely deleted. Thus, both photos used in the “bullying test” were still publicly available on the site both on the profile of the abuser (original large image), as well as one the one of the abused (in small icons). Therefore, the abusive comments below the photos were present as well. The images were still up on the site by the time the test was completed and nothing happened to the “bullies”.

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

The self-declaration does not include specific information on if Rate has effective processes in place to expeditiously review and remove offending content upon receipt of notification of alleged illegal content or conduct. Nothing in mentioned on the mechanisms to decide what (offending) content to review and, eventually, remove from the site, however the self-declaration does mention that Rate responds to complaints daily and that “regular and frequents reports are generated flagging possible violation of the Terms of Service”. The self-declaration also mentions that Rates cooperates with “the law enforcement agency provided the complaint is filed with the police. However, proactive pursuit of potential perpetrators by the service provider is in violation of state laws.”

Because of ethical reasons Principle 5 was not tested on the site.

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

Main findings in relation to the self-declaration

Rate self-declaration does not clearly specify which privacy setting options are available for its users. It does mention though, that user privacy settings are “prominently made available on user’s profile page” and that “confirmations are asked before user submissions”. Still, this information is very vague and it is not possible to infer from it what specific privacy options are available for (minor) users on this SNS.

The self-declaration does not specify if the privacy settings options/status are visible and/or accessible at all times, either. It also does not refer to if the service provider automatically maps information provided by users (during registration) onto their profiles or if users are made aware when this happens. However the self-declaration does mention that users can control “what parts of their profile are visible to friends or public” (See Principle 3).

Regarding providing users with supporting information to help them make informed decisions about the information they post online, Rate claims to display “contextual warnings” throughout the site. However, the self-declaration does not specify what type of content these “contextual warnings” display nor when they are displayed (next to all types of user-generated content? Whenever a user uploads a picture? Etc.).

Main findings in relation to the website

Only a few sections of the profiles (e-mail, phone number, msn account, last name, date of birth, photo album, and additional information for friends) can be made private by all users, including minors. All the other information on the profile is available to all, even non-registered users and it cannot be made private as there are no privacy settings that could be used. E-mail and Instant Messenger accounts of users are private by default, i.e. this information is only available to the users in the contact lists. While filling in one's profile a short notification about the privacy settings is displayed “e-mail and msn messenger accounts are by default made available to contacts in the friends list". Later on the users can always adjust their privacy settings according to their own needs, i.e. if they want, they can make their e-mail and msn account available to all or to no one.

Users may also have a private rate.ee mailbox, so that only people on one’s friends list and the ones who have given maximum points for one’s photos, are able to send messages. As opposed to what the self-declaration states, namely that privacy settings are “prominently made available on user’s profile page”, privacy settings mainly appear when making changes to one’s profile and cannot, thus, be found easily.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

Main findings in relation to the self-declaration

It is not clear from the self-declaration how the service provider assesses the effectiveness of their services to identify potential safety threats. Besides, no information on the mechanisms employed by the Rate to determine the most appropriate procedures for reviewing reports of illegal or inappropriate content or conduct is provided in the self-declaration. However, it does mention that “Regular and frequent reports are generated flagging possible violations of the terms of service”.

Regarding the steps taken by Rate to minimize the risk of employing candidates who may be unsuited for work which involves real-time contact with children or young people, Rate claims that their moderators and “super moderators” are not only carefully selected but also that “unsuitable moderators are replaced”. It is not clear from the self-declaration, though, who these moderators are, if they are in direct, real-time contact with minors, or what their monitoring tasks imply (e.g. reviewing content, replying to queries from users, etc.). However, Rate claims that they “play a large role in ensuring community`s adherence to rules”. How this is achieved is not mentioned in the self-declaration.
Principle 7 was not tested in the website.

Summary of Results and Conclusions

According to its self-declaration, Rate has implemented Principles 1 and 4 rather satisfactorily and Principles 2, 3 and 6 unsatisfactorily on its website. The testing on the website revealed several problematic areas, for instance:

- Users are unable to change their date of birth previously provided in the registration form unless they pay.
- Profiles of minors are easily searchable by their nickname both in the service search engine and via Google (but not through Yahoo! or MSN search).
- Both non-registered users of the site as well as users not belonging to the friends list of the profile owner have, by default, access to Minor`s profile images, videos, blogs as well as all the textual information on the profile (e.g. birthday, place of residence, education, profession, etc.) except the e-mail and MSN account of a profile owner.
- Adults can send friend requests to minors, but these can be easily declined.

- Although blocking seems efficient at first, the system informs the “blocked” person that they can still have access to the profile of the user who blocked them by simply logging out from the site.

Assessment of all the Principles in the Self-declaration

Principle	*Very satisfactory*	*Rather Satisfactory*	*Unsatisfactory*
1	x		
2			x
3		x	
4			x
5			x
6			x
7		x	

Implementation of the Self-declaration on the SNS

Principle	*Very satisfactory*	*Rather satisfactory*	*Unsatisfactory*
1		x	
2			x
3			x
4		x	
6			x

SCHUELERVZ

Monika Taddicken, University of Hamburg, Germany
Verónica Donoso, Appointed Research Coordinator by the EC

Introduction

The platform schuelerVZ is one of the three social networking sites of VZnet Netzwerke Ltd. provided for the German market (studiVZ and meinVZ are the other two). It is aimed at German pupils from 12 to 21 years. SchuelerVZ exists since four years ago. Today, 5.8 million pupils are users of schuelerVZ.[49] Registered users are represented by a profile site where they publish certain personal information like hobbies, favourite music or popular movies as well as pictures. They can add other users as their “friends”, create or join groups where they can engage in discussions about topics they are interested in, and use channels for interpersonal communication such as direct messages or chat. SchuelerVZ is a stand-alone platform that is not open for general registration (new users need an invitation of an actual user to be able to join) and allows no interaction (e.g. no messages or friend requests) with users of studiVZ or meinVZ.

The following is a report of findings of the analysis of the self-declaration provided by VZ-Netzwerke and the testing of schuelerVZ website. The test was conducted in December, 2010 – January, 2011.

Summary of main findings

SchuelerVZ is an invitation only system that, in theory, only allows users aged between 12 and 21 years old.[50] A person younger than 12 (and older than 21) receives a message explaining that he/she is not allowed to register as a schuelerVZ user because of the age requirements that apply on the site. However, in practice, a person younger (or older) than what is established in the age requirements can re-do their registration process with the same invitation and subscribe by simply selecting a suitable date of birth.

The default privacy settings are very strict and the profiles of new registered users are set to “private by default”. This implies that because they do not allow access to any other Internet user and profiles of minors cannot be searched or contacted neither inside the social networking site nor outside (e.g. via search engines such as Google or Yahoo!) except by confirmed “friends” on the contact list. Possibilities to set privacy options are varied and sophisticated including “ignore function” and the possibility to pre-approve photo tags. Deleting a complete profile is easy-to-do and can be done by the “my account” section. One weakness has to do with the inefficiency of the reporting mechanism: Although reporting abuse is easy to handle for minors, the test revealed that SchuelerVZ neither reacted expeditiously nor efficiently to a bullying test report.

SchuelerVZ provides a wide variety of clear and targeted guidance and educational materials for young users as well as for parents and teachers. A lot of information specifically targeted at children including educational videos and concrete tips on relevant e-safety issues is provided to raise the awareness of users regarding their privacy as well as their safety online. Besides, a child-friendly code of conduct in the form of videos created by users of the SNS is also provided.

[49] Source: http://www.schuelervz.net/l/schueler/3/, accessed Dec. 17th, 2010.

[50] The researcher who tested schuelerVZ for this assessment used an existing fake account to get ‘inside’ the system.

Analysis of Results by Principle

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner

Main findings in relation to the self-declaration

According to its self-declaration schuelerVZ provides *clear* guidance and safety information specifically targeted at children and young people on how to navigate their website safely. schuelerVZ also claims to provide useful information/links for parents and teachers.

The self-declaration indicates that schuelerVZ has developed an age-appropriate and clearly formulated internal Code of Conduct in the form of videos (including the consequences of breaching the Terms) especially designed for children and young people. This Code of Conduct specifies, for instance, that "every user who breaches the internal code of conduct gets reprimanded, temporally locked or deleted". Although no specific information about *what* constitutes inappropriate behaviour on the site is explicitly mentioned in the self-declaration, a link to the internal Code of Conduct ("Verhaltenskodex") with specific information about what constitutes inappropriate behaviour on the site is provided.

No information on the available technological tools for parents in order to monitor their children is found on the self-declaration, either, although the self-declaration does mention that SchuelerVZ provides phone consultation with educational experts for parents and teachers as well as comprehensive information (targeted at them) regarding the general functioning of the site and specific technical help on each platform.

Main findings in relation to the website

As stated in the self-declaration, SchuelerVZ provides clear and targeted guidance and educational materials designed to give children and young people the tools, knowledge and skills to navigate their services safely. Audio-visual fragments (mainly short videos) are used to explain the safety information. The written text is formatted with sub heads and bullets and presented in short pieces that facilitate information skimming. The provided information is of an accessible and easy-to-understand format for children and young people. However, because of the big variety of the provided information users (specially the youngest ones) might be overwhelmed.

Confirming the analysis of the self-declaration, the Code of Conduct ("Verhaltenskondex") provides clear information on what constitutes inappropriate behaviour and on the consequences of such behaviour. Misbehaving users can get blocked and/or deleted by schuelerVZ. Besides, very comprehensive documentation regarding not only privacy, but also self-disclosure (e.g. managing their online identity) is provided. For example schuelerVZ advices young users (leaving school) on how to manage and improve their personal information on the SNS profile with regards to applications for part-time jobs and apprenticeships.

SchuelerVZ provides clear and targeted information for parents and teachers on how to foster children's responsible and safer internet use. Educational materials are provided. External links as well as a contact telephone number for parents and teachers are presented. However, during the test it remained unclear why the provided telephone number is only meant for parents and teachers and not for users as well[51].

[51] According to schuelerVZ, specially trained staff is responsible for contact with parents and teachers. Thus, it is easier and quicker to handle these contacts through separate contact channels.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience

Main findings in relation to the self-declaration

In its self-declaration SchuelerVZ states that the minimum age requirement to create an account in this SNS is 12. Regarding the steps taken by the provider in order to prevent users from attempting to re-register with a different age (if they have previously been rejected for being below the minimum age), the self-declaration mentions that "profiles of younger persons who get reported will be deleted" and that the "email addresses of deleted users are locked". However, apart from the fact that under-aged users may be reported, no other mechanisms to identify under-age users are mentioned.

In its self-declaration SchuelerVZ refers to diverse mechanisms through which the service provider ensures limited exposure to potentially inappropriate content and contact for children, for example by being an "invitation-only"[52] system and by setting a maximum age limit of 21 year olds so as to ensure that children and young people cannot be inappropriately contacted by adults. Furthermore, SchuelerVZ claims to have implemented several measures such as avoiding that users can change their age (although it is not specified how this is achieved); allowing the possibility to restrict content in discussion groups for users who are 16 or older and (temporarily) reprimanding, locking or deleting users who breach Code of Conduct.

The self-declaration does not specify what types of services are considered as not appropriate for children and young people. Besides, it does not refer to the ways in which this service provider promotes the uptake of parental controls in its self-declaration, apart from providing them with safety information (Principle 1).

Main findings in relation to the website

As stated in the self-declaration, SchuelerVZ is an invitation-only system: To register as a user an invitation of an existing user is necessary. In theory, it is not possible to register as a user being younger than the required 12 years. This is realized by a mandatory question about date and year of birth. A person younger than 12 years receives a message that he/she is not allowed to register as a schuelerVZ user because of the age requirements. However, in practice, a younger (and older) person can re-do their registration process and subscribe by simply selecting a suitable date and year of birth.

Confirming the analysis of the self-declaration, because schuelerVZ is aimed at pupils not older than 21 years, all the functionalities and content available on the platform are suited for the 12-21 age group only. Besides, it is not possible for users of schuelerVZ to interact with users of the other VZ-social networking sites or with any other non-registered user of the site.

Regarding specific commercial content, different advertising banners are displayed on different places within the SNS. Banners advertising inappropriate content such as alcohol or cigarettes were not shown during the test, but only banners displaying well-known brands and companies (e. g. Clearasil, Coca-Cola). None of the banners displayed linked to fake winning notifications or invitations that asked users to provide their contact information.

Supporting the analysis of the self-declaration, no information could be found on schuelerVZ site regarding the functionalities provided to users (or other content providers) to enable them to label/rate or age restrict content, except the possibility for users to set up a discussion group restricted for users younger than 16 years.

[52] By "invitation-only system" SchuelerVZ means that "people must receive an e-mail invitation sent by an existing schuelerVZ user. It is not possible to register an account without such an invitation."

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

SchuelerVZ declaration clearly indicates that the profiles of “new registered users are set completely private by default”, i.e. they are unsearchable on search engines and their profiles “are not visible for non registered persons”. But this does not necessarily mean that their profiles are “private by default”[53] as defined in the Safer Social Networking Principles[54] because it is not clear from this if “the full profile cannot be viewed or the user contacted except by ‘friends’ on their contact list”.

In relation to the tools and technologies employed by the service provider in order to assist children and young people in managing their experience on their service (particularly with regards to inappropriate or unwanted content/contact), the self-declaration refers to several functionalities including, among others, a “delete button” for every single piece of user-generated content such as posts, photos, message, etc.; “Ignore function” for users who are in trouble with each other or pre-approving of photo tags.

The self-declaration does not provide any further information on how schuelerVZ supports parents be aware of the existence of other available safety tools/information (such as filtering tools or parental controls) to help them protect young people online. Although it does provide general safety information targeted at parents and specific guidance about what this SNS is and how it works (see Principle 1).

Main findings in relation to the website

The testing of schuelerVZ demonstrates that the privacy settings are set to “private by default”[55] as defined in the Safer Social Networking Principles. However, even though the test confirmed that the profiles of minors cannot be searched neither in the internal nor in the external search engines like Google or Yahoo!, it is still possible for “friends of friends” to have access to limited information from those profiles, namely, the profile picture, the first name and the initial of the family name of the minor as well as the name and the city of the school the minor attends. “Friends of friends” cannot interact with the minor although they can send a friend request.

Default privacy settings can still be considered as quite secure in the sense that no interactions and no content exchange is allowed to “friends of friends” or beyond. Besides, no contact information is displayed to anyone outside the minor`s approved contact list while only “friends” are able to post comments or pictures to the pinboard (= guestbook). No other user is allowed to tag the user on pictures.

Users can choose one of three basic settings: “access to everybody” (“Profil offen für alle”) (= users can find the profile via an internal search engine and view the whole profile), “access to friends” (“Profil offen für Freunde”) (= users can find the profile via an internal search engine, but only friends and friends of friends can see the whole profile) and “no access” (“Profil geschlossen”) (= users cannot find the profile via the internal search engine, only friends can see the whole profile, other users can only see first name, profile picture and name of

[53] “Ensuring that setting a profile to private means that the full profile cannot be viewed or the user contacted except by ‘friends’ on their contact list”.

[54] http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

[55] “Ensuring that setting a profile to private means that the full profile cannot be viewed or the user contacted except by ‘friends’ on their contact list”.

the school children attend). In addition to these basic settings, users are able to customize their own privacy settings by deciding which specific profile categories to make available to which users. These categories include “Profile” (“Mein Profil”), “Messages” (“Buschfunk und Nachrichten”), “Search” (“Suche”) and “Diverse” (“Verschiedenes”) which includes the visibility of the online status. It is not possible to pre-approve comments before they are displayed.

Users can block other users from interacting with them via a blacklist (“Ignorieren”). While visiting other users’ profiles, an embedded “ignore” button is displayed. This button is easy to find and use. It is also possible to easily delete undesired pinboard content (via an embedded delete button).

As stated in the analysis of the self-declaration, apart from providing general e-safety information and guidance for parents (see Principle1), no specific tools to promote the uptake of parental controls (e.g. filtering software) or specific information about them are found on the site.

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service

Main findings in relation to the self-declaration

The self-declaration refers to the following mechanisms to report inappropriate content, contact or behaviour on schuelerVZ: easy-to-find and use Reporting Buttons and general reporting via email or online form. According to the self-declaration all types of user-generated content as well as individuals or groups can be reported including discussion groups, pictures, postings, status updates and specific user profiles. The provider claims that reporting links are integrated on *every page* of the site and that especially trained employees screen these reports and “act promptly 365 days a year.”

The self-declaration neither includes information on if the reports of abuse are acknowledged nor if users are provided with an indication of how their reports are typically handled.

Main findings in relation to the website

SchuelerVZ provides comprehensive and age-appropriate documentation about how users can report abuse and misbehaviour on the site, mainly via audio-visual fragments. The information, that encourages users to report safety breaches, is easy to find. The employees who handle the reports are named and users are told that they will help them as soon as possible.

As stated in the self-declaration, two mechanisms to report inappropriate content and misbehaviour are provided: First, users can find embedded report buttons in the profile or next to the content (e. g. pictures, comments on pinboards). Mostly, these buttons are easy to find as they are displayed at prominent places next to user-generated content. However, sometimes these buttons only appear via mouse-over-effect while in other cases the button is permanently displayed. Buttons to report pictures, profiles or discussion groups are always displayed permanently. Buttons to report comments and posts appear via mouse-over-effect (the exclamation mark button). Only the first button for reporting comments or posts is shown permanently on every page.

As the test demonstrates, the report buttons are easy to use. After clicking on them, an online report form appears that asks details about the issue that is being reported. A drop-down list of possible reasons for the report as well as an open text field to describe the problem in more detail is included in the form. The second reporting mechanism, sending an email to report abuse, is less user-friendly, and also less age-appropriate in the sense that young people first have to find the relevant email address. Besides, the contact e-mail address, located in the Terms of Use (“AGB”), is not really easy to find.

As part of this study, a (fake) minor user reported that she had been bullied on this SNS. A realistic bullying situation was set up between the (fictitious) owners of profiles that were created for this assessment. The scenario consisted of one minor being bullied by two other minor users who posted a nasty comment on the pinboard of the “victim” and who uploaded some hurtful pictures of the “victim” on their profiles. For some of the bullying content in the pinboard an embedded report button was displayed (exclamation mark button). The “victim” clicked and filled in all the necessary fields and supporting information before sending the form. The test bullying report remained unanswered, the bullying content remained on the site and none of bullies received any warnings or notifications. In sum, we can conclude that the even though the reporting button mechanism provided by SchuelerVZ is user-friendly, it is also ineffective.

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

According to the analysis of the self-declaration the process in place to expeditiously review and remove offending content relies on user-generated reports. Once users contact the support and abuse team (via e-mail or reporting system) these reports are sent to specialized personnel who “screen reports and act promptly”. There are dedicated teams for dealing with requests from parents, teachers, and public authorities and law enforcement agencies. VZnet Netzwerke also cooperates with relevant organizations such as jegedchutz.net and the FSM, which provide hotlines for objectionable conduct or content on the internet. However, it is not clear from the self-declaration what this cooperation concretely involves or if specific info/links to these institutions are provided on the website.

Because of ethical reasons, Principle 5 was not tested in the website.

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

Main findings in relation to the self-declaration

According to its self-declaration, users of schuelerVZ are provided with a range of privacy setting options and with supporting information to help them make informed decisions about the information they post online. For instance, “substantial and sophisticated privacy settings based on friend lists”, strict default privacy settings, “comprehensive control of personal data”, by filling in a “VCard” for every single application users ensure that their profile data is not transferred to third parties, etc. In the self-declaration the provider also claim that users are given age-appropriate and easy-to-understand information regarding their responsible use of private data and copyrights.

The self-declaration does not specify if the privacy settings options/status are prominent, visible and/or accessible at all times. It also does not refer to if the service provider automatically maps information provided by users (during registration) onto their profiles or if users are made aware when this happens. Finally, the service provider indicates that users can easily delete their complete profile by clicking on the respective button found in the “my account” section.

Main findings in relation to the website

Confirming the analysis of the self-declaration, schuelerVZ provides a broad range of privacy settings. Users can choose one of three basic settings: “access to everybody” (“Profil offen für alle”), “access to friends” (“Profil offen für Freunde”) and “no access” (“Profil geschlossen”) or create their own privacy settings by means of the categories "Profile" ("Mein Profil"), "Messages" ("Buschfunk und Nachrichten"), "Search" ("Suche") and "Diverse" ("Verschiedenes"). With this, it is possible to restrict the search for the name ("do not want to be found under my name"). Other examples for the possibilities of privacy options are setting limitations for tagging, presenting the name only via first name, not being recognized as a visitor of other profiles and limiting the possibility for recommendations from other users.

The privacy setting options are easy to use by minors. They are easy to find and can be viewed and/or changed at any given time. Supporting information on how to use these settings is also provided in clear and age-appropriate language. This information also alerts schuelerVZ users on the types of information that third party application providers might retain from them. In sum, SchuelerVZ provides plenty of age-appropriate materials to support users make informed decisions regarding the personal information they disclose online. Some of the sections where users can find relevant information regarding privacy are "Advices" ("Tipps & Hinweise"); "Impression management & privacy" ("Selbstdarstellung & Privatsphäre") and "Plain texts" ("Klartexte") which are personalised safety tips from schuelerVZ employees (e. g. "Trust in the net" ("Vertrauen im Netz") or "Data protection" ("Datenschutz")).

Finally, the test also confirmed that users of schuelerVZ can easily delete their account. An easy to find and use button in the section "My Account" ("Mein Account") is provided. It is clearly explained that some disclosed information (comments on pinboards and pictures) should be deleted first. Pictures in photo albums of others that show the user who wants to leave schuelerVZ can be reported for deleting.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

Main findings in relation to the self-declaration

According to the self-declaration SchuelerVZ assesses their service to identify potential risks to children and young people by... Employed educationists are evaluating entire communication and safety education" and "Every application is reviewed for legal and technical aspects in an approval process."

According to the self-declaration, the procedures employed by schuelerVZ to promote compliance with the Terms of Service are based on the user-generated report mechanism by means of which objectionable conduct or content can be identified. Users who breach the code of conduct can either be temporarily reprimanded, locked or deleted, while content which is found to breach the internal code of conduct is deleted.

Regarding the measures steps taken by schuelerVZ to minimize the risk of employing candidates who may be unsuited for work which involves real-time contact with children or young people, the self-declaration stresses that "Trained employees with different skills for special topics are working in teams 365 days a year to screen reports and act promptly". Finally, it is not clear from the self-declaration how the service provider assesses the effectiveness of their services to identify potential safety threats.

Principle 7 was not tested in the website.

Summary of Results and Conclusions

According to its self-declaration, schuelerVZ has implemented Principles 1, 2, 3 and 6 very satisfactorily and Principle 4 rather satisfactorily on its website. The testing on the website revealed some areas of attention, for instance:

- Apart from providing general e-safety information and guidance for parents (see Principle1), no specific tools to promote the uptake of parental controls (e.g. filtering software) or specific information about them were found on the site.

- Even though the reporting button mechanism provided by SchuelerVZ is user-friendly, it is also ineffective. Users get neither an acknowledgement that their message would be handled nor any reply from the provider. Besides, the offending content was not removed from the site and the "bullies" did not get any warning nor were they "reprimanded" in any way.

Assessment of all the Principles in the Self-declaration

Principle	*Very satisfactory*	*Rather Satisfactory*	*Unsatisfactory*
1		x	
2		x	
3	x		
4		x	
5		x	
6		x	
7		x	

Implementation of the Self-declaration on the SNS

Principle	*Very satisfactory*	*Rather satisfactory*	*Unsatisfactory*
1	x		
2	x		
3	x		
4		x	
6	x		

TUENTI

Charo Sádaba, School of Communication, University of Navarra, Spain
Verónica Donoso, Appointed Research Coordinator by the EC

Introduction

Tuenti is a Spanish-based Social Networking Site, the most popular amongst teenagers and young adults (14-25) in the country. It has only one language version in Spanish. It started in January 2006. It is the second largest SNS in Spain after Facebook, with 8 million users[56].

Tuenti features many tools common to social networking sites. It allows users to set up a profile, upload photos, link videos and connect with friends; it also offers a chat application and some other utilities, such as the ability to create events. A mobile version of the SNS is offered to users, with some specific features (users' mobile phone number only appear on the mobile version.

The following is a report of findings of the analysis of the self-declaration provided by Tuenti and the testing of its website. The test was conducted in December, 2010 – January, 2011.

Summary of main findings

In spite of the fact that the minimum age requirement is 14 visitors younger than 14 can easily register on the site[57]. Even though Tuenti does not index profiles of minors in external search engines like Google or Yahoo!, inside the service, profiles of minors (set to the maximum privacy level) are not only open to "friends" but also to other "non-friends" registered users of the platform including adults) who can contact minors via private messages, ask for their friendship and even have access to a thumbnail of the profile picture, the full name, the name of the school and the city where the minor lives. The rest of the information included in the minors` profile is only accessible to friends. In other words, minors' profiles are not set to "private by default" as understood by the Safer Social Networking Principles.

Regarding the appropriateness of advertising content available on the site for minors, Tuenti does not display conventional ad formats (like banners), however brands can create an "event", that will be presented to users as reminders or offers they can decide to attend to or not. No inappropriate content for minors was found on Tuenti during testing.

Tuenti has developed an easy to use reporting mechanism to report any piece of content. However, during testing, this mechanism did not work fully efficiently. Indeed, the " bullying report" (made up for this test) was only replied to four days after submitting the complaint and the bullying content (offensive pictures of a minor) remained on the site even after the "victim" explicitly asked for the pictures to be removed.

Finally, Tuenti provides its users (and non-users) with plenty of information and practical tips on safety and privacy issues. Besides that, a concise summary of the *Terms of Use* has been developed and is presented to non-users and users in a direct and simple language.

[56] http://www.elpais.com/articulo/economia/presidente/Tuenti/abandona/cargo/compra/Telefonica/red/social/elpepieco/20100805elpepieco_4/Tes

[57] According to the provider, TUENTI has signed an agreement with the Spanish Data Protection Agency, whereby our public commitment to prevent minors from creating and maintaining accounts in our network is formally laid out. As a consequence of this collaboration TUENTI runs an enquiry and deletion protocol applicable to users under the age of 14.

Analysis of Results by Principle

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner

Main findings in relation to the self-declaration

According to its self-declaration Tuenti provides *clear* guidance and safety information specifically targeted at 14-18 children on how to navigate their website safely including concrete tips and information on privacy, data protection, image rights, etc. Tuenti also claims to provide useful information and links for parents and teachers (e.g. links to the Spanish Data protection Agency). The self-declaration indicates that the Terms & Conditions and the Privacy Policy are clearly summarized and are easy to understand even for 14 year old children (the youngest allowed Tuenti users).

The self-declaration neither specifies what constitutes inappropriate behaviour on the site nor where this information can be found. Besides, no explicit information on the consequences of inappropriate behaviour on the website is found in the self-declaration. The self-declaration does not mention if the website offers parents and/or teachers any types of technical controls to support the safety of their children online apart from the general safety and privacy information aforementioned.

Main findings in relation to the website

Tuenti offers relevant information related to safety and privacy issues in an open area of the site, under the "Help" button (two steps from the homepage). The SNS offers the Privacy principles of the SNS, plus a concise summary of the Terms of Use in the form of a Decalogue, as well as a short, but relevant selection of external links to institutions working for a safer Internet. This information is targeted at a general public and is not directly addressed to parents and/or educators.

When the user opens a profile in Tuenti the same information relating to safety and privacy is also available on the Privacy section, under the "My account" link. Once in the Privacy section, the Q&A covers a wide variety of issues on privacy and safety in a direct and simple manner, just as stated in the self-declaration.

The information about the "Terms of Use" is only textual, and some pieces of it, such as forbidden content and the consequences of misuse, are present both in the short (Decalogue) and long versions of the Terms. As opposed to the Q&A section which is written in a more concise and direct tone, the Terms of Use and the Decalogue are written with a legal tone, not so easy to understand for minors.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience

Main findings in relation to the self-declaration

Tuenti states that the minimum age requirement to create an account on this SNS is 14. According to its self-declaration, the provider continuously verifies suspicious profiles ("enquiry and deletion protocol") so as to prevent users from attempting to re-register with a different age if they have previously been rejected for being below the minimum age required. If someone is found to have "lied" about their age (e.g. after verification of their ID), their e-mail address is blocked to avoid that they re-register in the system with the same e-mail address. Still, Tuenti admits that "there is no reliable mechanism to verify the age of users at the time of registration" because it relies on users` self-declaration of age.

In its self-declaration Tuenti refers to one main mechanism to limit the exposure of children to potentially inappropriate contact, namely the fact that Tuenti is an "invitation-only system" which would ensure that only users who get an invitation from another existing user can register on the site. Apart from stating that inappropriate content can always be reported to Tuenti support team, the mechanisms through which the service provider ensures limited exposure to potentially inappropriate content are not clearly specified in the self-declaration.

Tuenti does not refer to the ways in which it promotes the uptake of parental controls in its self-declaration; although it does claim that they provide parents with general safety and privacy information (see Principle 1).

Main findings in relation to the website

The SNS makes clear to users and potential users that 14 years old is the minimum age required to use the service. Reading the Privacy page, and the Terms of Use, Tuenti mentions that their support team is always looking for dissonances on profiles in order to avoid users under 14 to have a profile. SNS could ask a suspicious user for an official ID to check if they are as old as they claim to be. Tuenti publicly states that thousands of profiles are erased every day. Users are also invited to report a profile of an under aged. Besides this information and a registration form that prevents users from selecting an inappropriate age, no other mechanisms, e.g. cookies, are implemented to ensure that users are above the minimum age required. When an under 14 user wants to open a profile the only possible way to do that is by lying about their birth date, so breaching the terms of use of the SNS and risking termination. As the SNS relies too much on the user's self declaration of age, it is really easy for an under 14 years old, to open an account on the service, as was demonstrated by the test on the website.

The SNS does not rate content or services by age and all content is available to all users. Regarding the advertising content, Tuenti does not display conventional ad formats (like banners). Brands can create an event, that will be presented to users as reminders or offers they can decide to attend to or not. Besides that, brands can also create pages (non-personal profiles) where advertising (banners, video ads) could be part of the content. In searching results pages, the logos and links of the "official pages" (sponsors of the SNS) are presented to users. No inappropriate advertising content for minors was found during testing.

Tuenti does not offer parents any possibility for active parental control such as filtering software or other similar mechanisms.

As Tuenti is a closed network, and an invitation of an existing member is required to open a profile, a previous fake account created two years ago was used to send invitations to the testing profiles. To open this account, with research purposes, a university student and real Tuenti user, invited the tester to join the SNS.

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

Tuenti claims that by default the profiles of users under 18 are set to "maximum privacy level" (= 'friends only') so that access to unknown users or even to "friends of friends" is not allowed. The default privacy setting described by Tuenti in its self-declaration is, thus, in line with the concept of "private by default"[58] as defined in the Safer Social Networking Principles[59].

The self-declaration refers to a few mechanisms employed by Tuenti to assist children and young people in managing their experience on their service, particularly with regards to inappropriate or unwanted content or conduct, among others: privacy settings are very easy to control, users have the option not to receive messages from unknown users and to prevent others from downloading their pictures and the Help page includes relevant safety and privacy tips so that users (and non-users) can make informed decisions regarding the personal information they post online.

[58] "Ensuring that setting a profile to private means that the full profile cannot be viewed or the user contacted except by 'friends' on their contact list".

[59] http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

The self-declaration does not provide any further information on how Tuenti supports parents be aware of the existence of other available safety tools/information (such as filtering tools or parental controls) to help them protect young people online.

Main findings in relation to the website

As demonstrated by the test and, as opposed to what is stated in the self-declaration, even though the full profiles of minors in Tuenti are set to the maximum privacy level (= "friends only"), this privacy setting does not exactly correspond with the definition of "private by default"[60] suggested by the Safer Social Networking Principles. According to the latter, "setting a profile to private means that the full profile *cannot be viewed* or the user *contacted* except by 'friends' on their contact list". In the case of Tuenti, even though, the test confirmed that Tuenti does not index profiles of minors in external search engines like Google or Yahoo!, inside the service, profiles of minors (set to the maximum privacy level) are not only open to "friends" but also to other "non friends" registered users of the platform (including adults) who can contact them via private messages, ask for their friendship and even have access to a thumbnail of the profile picture, the full name, the name of the school and the city where the minor lives. Users, however, can easily reject a friendship request and also block other users. After registering, it is also possible to limit who can send private messages to "only friends", but this is not a default privacy setting for minors.

Users can block friends and non-friends, and then unblock them easily and they can delete unwanted comments in an easy way.

Tuenti does not offer any tool or information specifically addressed to parents/educators to help them protect minors online or to enable parental control.

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service

Main findings in relation to the self-declaration

Tuenti self-declaration refers to only one basic mechanism to report inappropriate content, contact or behaviour, namely, sending an e-mail to the Tuenti support team (soporte@tuenti.com). Tuenti claims that not only the reports, but also other user`s queries and requests are analysed and acted upon expeditiously and that users are always provided with a confidential, "personal and individual reply". According to the self-declaration users can contact Tuenti in case of "breaches involving users, photographs and any other content". It is not clear from the self-declaration if any other reporting mechanisms are in place.

The self-declaration does not explicitly state if the procedure to report inappropriate content, contact or behaviour is *age-appropriate, easily understandable* for children and young people, or if it is *easily accessible* to users.

Main findings in relation to the website

As observed during the test and as opposed to the analysis of the self-declaration, Tuenti provides its users with more than one reporting mechanisms, namely a report button placed next to every picture and contacting the support team via e-mail. The reporting button mechanism is functional and user-friendly. Every time a user is tagged in a picture, the user can either remove the tag, or report it. When users initiate a report, they are advised about the consequences of fake reporting, and a link to the "Terms of Use" is offered to check the accuracy of the report.

[60] "Ensuring that setting a profile to private means that the full profile cannot be viewed or the user contacted except by 'friends' on their contact list".

As part of this study, a (fake) minor user reported that she had been bullied on this SNS. A realistic bullying situation was set up between the (fictitious) owners of profiles that were created for this assessment. The scenario consisted of one minor being bullied by two other minor users who posted a nasty comment on the wall of the "victim" and who uploaded and/or sent hurtful pictures. As the "victim" could not cope with the nasty comment put on her profile and the embarrassing pictures, she contacted the provider via a form that was filled in and sent to Tuenti explaining the situation and asking for help and advice. Four days after the message was sent the "victim" received a reply advising her to talk to their friends and solve the uncomfortable situation. The user asked to erase the nasty pictures, but Tuenti did not agree with the reasons provided by user and so, the bullying pictures remained on the site.

Reading the Terms of Use link, Tuenti offers an email address (soporte@tuenti.com) as a way of asking for help or contacting their support team. This information is hard to find for minors, and the user is advised to read carefully the Q&A to find the answer before sending a message. The Q&A clearly refers to all the available mechanism for users to control who can access the information they post online. It provides users with ideas and solutions for a wide range of safety and privacy issues, including when and how to send report or how to react to eventual inappropriate contacts or content. By doing this, Tuenti is consistent with its own philosophy of giving the user the control but also the responsibility of what they post online.

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

In the self-declaration Tuenti claims that whenever "a user may be at risk involving a purportedly criminal offence" the issue at stake is dealt with "diligently" by the Legal and Privacy Department in charge of studying the case. If confronted with a criminal offence, Tuenti claims to file a complaint with the Police within 24 hours. Tuenti also claims to provide its users with expert legal support. The self-declaration does not provide specific information regarding how Tuenti deals with potentially offending content so it is not clear if it is immediately deleted from the site, if it is saved for further investigations or if any other measures apply.

Because of ethical reasons, Principle 5 was not tested in the website.

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

Main findings in relation to the self-declaration

According to its self-declaration, users of Tuenti are provided with supporting information to help them make informed decisions about the information they post online. For instance, the Help Page and Privacy Centre provide clear and relevant information for 14-18 year olds (but also for their parents, teachers and non-users) on how to ensure online safety in general and on specific privacy issues, in particular. Tuenti also claims to raise awareness of privacy and safety issues by cooperation with local safety and governmental centres.

Apart from the plenty of information regarding privacy, the self-declaration does not provide detailed information regarding the actual privacy mechanisms and functionalities provided to users of Tuenti. It does mention, though, that the default settings for profiles of users under 18 are set to strict "private" settings by default and that users can always adapt their privacy settings via the user- friendly "privacy panel". Regarding the exchange of content, Tuenti claims that users have the option not to receive messages from unknown users and to prevent others from downloading their pictures. Further, no other specific functionalities are mentioned in the self-declaration. The self-declaration does not refer to if the service provider automatically maps information provided by users (during registration) onto their profiles or if users are made aware when this happens.

In sum, the self-declaration focuses on the privacy information made available on the site, but not on the functionalities that would actually *enable* a safe approach to privacy.

Main findings in relation to the website

As previously mentioned, the default profiles of users under 18 years old are set to the "maximum level of privacy" possible in Tuenti, but they are not "private by default". The following mandatory information is required of minors to open an account on the service: real first and last names, birth of date, name of school they attend, expected graduation year and place of residence. This information is displayed in the user profile page, although only friends have access to the whole profile. The rest of registered users, including adults, can only have access to a thumbnail of the profile picture, the minors` full name, name of school and place of residence. Profile editing is possible after registration, but mandatory information cannot be left blank.

Privacy settings are accessible at two steps from the profile page, which may make them a bit difficult to find especially for the youngest minor users. Users can control who (*only friends, friends of friends or everyone*) can see their profile, who can download their pictures, who can send them private messages, see their wall, or their phone numbers. Controls to block users, pictures, applications or games are also offered. The "Help" button is also always present in the page and is accessible at all times. Recommendations for a safer use of the SNS are presented to non-users and registered users in the Privacy page. Users 14-18 are advised, for instance, to "ask your parents if you have any doubts about a message or situation", or "before publishing a picture, ask for permission of anyone included in it". A specific email address is offered to solve questions about privacy on Tuenti: privacidad@tuenti.com.

Finally, when a user wants to delete their account the first option Tuenti offers is to deactivate it. It clearly states that in this case, the information would only be "hidden" and that it would be possible to recover it at a later time if the user wished so. On the same page, Tuenti explains that the account could also be deleted. In this case the information would be permanently eliminated. In both cases, the user is asked about the reasons to quit the service.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

Main findings in relation to the self-declaration

According to the self-declaration, the procedures employed by Tuenti to promote compliance with the Terms of Service are based on the user-generated reporting mechanism by means of which objectionable conduct or content can be identified. This process implies that all requests, queries and complaints submitted by users are reviewed by Tuenti user support. As stated in Principle 5, whenever criminal offences are spotted the Legal and Privacy Department studies the case and, if necessary, files a complaint with the Police.

It is not clear from the self-declaration how the service provider assesses the effectiveness of their services to identify potential safety threats in particular in relation to removing inappropriate and/or illegal content found on the site.

Principle 7 was not tested in the website.

Summary of Results and Conclusions

Considering the self-declaration submitted by Tuenti we can conclude that the service provider has implemented all the Principles rather satisfactorily on its website. The testing on the website revealed some areas of attention, for instance:

- Even though the minimum age requirement is 14, visitors younger than 14 can easily register on the site.
- Although the privacy settings are set to "maximum privacy level" (= 'friends only'), still all registered users can contact minors via private messages. In other words, minors' profiles are not set to "private by default" as defined by the Safer Social Networking Principles.

- Even though Tuenti does not index profiles on search engines outside Tuenti, inside the service, all profiles are searchable by other "non friends" registered users of the platform with no limit of age.
- Even though the reporting mechanisms proved to be user-friendly, during the testing they did not work completely efficiently. Indeed, the " bullying victim" (created for this test) only got a reply four days after submitting her complaint and the bullying content (offensive pictures of the minor) remained on the site even after the "victim" asked explicitly for the pictures to be removed.

Assessment of all the Principles in the Self-declaration

Principle	*Very satisfactory*	*Rather Satisfactory*	*Unsatisfactory*
1		x	
2			x
3		x	
4		x	
5		x	
6		x	
7		x	

Implementation of the Self-declaration on the SNS

Principle	*Very satisfactory*	*Rather satisfactory*	*Unsatisfactory*
1		x	
2		x	
3		x	
4		x	
6		x	

ZAP

Dr. André Melzer, Université du Luxembourg, Luxembourg
Verónica Donoso, Appointed Research Coordinator by the EC

Introduction

ZAP is a free-access social networking website ("community platform") in Luxembourg for people aged 12 and above. Due to the three main languages that are spoken in the country, *ZAP* offers Luxembourgish, German, and French versions of the site. It provides information on event schedules, nightlife reports, user profiles, homepages, and photos that may be used on mobile devices or web browsers. Users of *ZAP* may present and describe themselves for social purposes using public messages, friend lists, a mailing system, and picture and video upload functions. Although exact numbers are missing, *ZAP* claims to have a penetration of 65% in its target audience in Luxembourg (http://www.zap.lu/lu/p10458/index.html, accessed 10-12-2010). In 2010, the company launched the international version of its services under ZAPOn.com.

The following is a report of findings of the analysis of the self-declaration provided by ZAP and the testing of its website. The test was conducted in December, 2010 – January, 2011.

Summary of main findings

Testing of the ZAP website showed that the *ZAP* provides users with a comprehensive, age-appropriate and easy-to-find safety tips and information for adolescents and their parents. The SNS provider treated a report on bullying timely and adequately; the offensive material in question was deleted and a warning was sent to the initiators of bullying. Other areas, however, are less successfully implemented on the *ZAP* website. For example, simply changing the year of birth was sufficient to outmanoeuvre the age registration barrier. In contrast to the self-declaration, profiles of users under 16 are searchable within *ZAP* and via Google. In addition, the SNS website currently lacks additional educational material for children and carers, although links are provided to organisations concerned with online safety.

In contrast to the self-declaration, default settings for new user profiles render all personal information visible to everyone, rather than keeping the information private by default. Finally, deleting a user account is easy. It is possible to do it via a dedicated web link and users receive a warning that all data will be lost. In sum, testing revealed that not all safety measures mentioned in the self-declaration have been implemented in the *ZAP* website, yet.

Analysis of Results by Principle

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner

Main findings in relation to the self-declaration

According to its self-declaration ZAP provides clear guidance for children and young people on how to navigate their website safely, for instance the site includes safety Guidelines for children and their parents and some specific sections of the Terms of Service have been written keeping both parents and children in mind. ZAP continually reminds its young users to consult the Guidelines (downloadable PDF) so that they can learn to be safe online.

Zap`s Terms of Service is dedicated to adolescents and their parents. They inform users that they have to adhere to Zap`s guidelines and specify what Zap considers as inappropriate behaviour and the consequences thereof. Zap is currently working on a school guide for teachers and school personnel focused on the potential risks associated to the use of SNS use and how to prevent them.

The self-declaration does not specify if any technical controls (e.g. parental filters) are currently offered to parents and/or teachers.

Main findings in relation to the website

In accordance with the self-declaration, the ZAP website provides guidelines on Internet safety, online risks, and information on privacy. In addition, there is explicit information on both content and conduct that is not allowed on the SNS. Likewise, the consequences of engaging in prohibited behaviour and/or actions are clearly stated. Detailed, yet not easy for children to understand, information is found in Terms of use ("Konditiounen"). Surprisingly, and in contrast to Protection of minors, Terms of use are not available in Luxembourgish, but in German and French only, which Luxembourgish minors may not read or understand.

In contrast, Protection of minors ("Jugendschutz") contains clear and targeted information for minors and parents (e.g. "What can I do as a parent to protect my child?" ("Wat kënnen d'Elteren maachen?"). Links to these webpages are located at the very bottom of the website. Once clicked, information is clearly visible. The text-based information itself is presented using plain and succinct language. Additional PDF files containing safety-relevant tips that were mentioned in the self-declaration were not found during testing, though.

For more information on Protection of minors, the website provides users with links to the EC, to youth services (Service national de la jeunesse - snj), and to organisations that are committed to online safety, including the National Commission for Data protection (CASES), Luxembourg Safer Internet (Lusi), and Luxembourg Internet Safety Alert (LISA Stop Line). General information for parents and caregivers is not available separately, but presented as the final paragraph in the Protection of minors section.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience

Main findings in relation to the self-declaration

In its self-declaration ZAP refers to diverse mechanisms through which the service provider ensures limited exposure to potentially inappropriate content and contact for children, for example by rejecting and hashing inappropriate pictures, by deleting accounts for uploading inappropriate content (e.g. Pornographic, racist, violent content.). Furthermore, ZAP claims it retraces inappropriate content by collecting IP addresses and Buzz words filters, installed to identify inappropriate behaviour or abusive users. The types of services that are considered as not appropriate for children and young people are specified in the Terms of Service (e.g. racist, violent, pornographic content, etc.). The minimum age requirement is 13. However, Zap stresses that no extra steps are taken to ensure that children younger than 12 do not re-register on their site.

In order to guarantee users` privacy, ZAP claims it employs cookies to make sure that advertising is age-related and suitable for minors. Besides, "foreign applications" are not allowed to be embedded on ZAP`s website. Moreover, user profiles can be evaluated by other users. Profiles of users who get systematic bad evaluations are checked up promptly.

The self-declaration does not refer to how this service provider promotes the uptake of parental controls to allow parents to manage their children's safe use of the service.

Main findings in relation to the website

As opposed to what is stated in the self-declaration, ZAP Terms of use indicate that people aged 12 (and not 13) and above are allowed to use most, but not all services of *ZAP,* for which additional age restrictions apply (i.e., "Disco", "Café", "DeeJay"). With regard to these age-restricted services, some inconsistencies were observed in the different language versions of the Terms of use. According to the French version, some of *ZAP's* functions require a minimum age of 16, and others are for people aged 18 and above. According to the German version, however, additional functions always require a minimum age of 18. Testing also revealed another inconsistency in terms of age requirements. In contrast to both the German and the French version of the Terms of use, it was not possible to sign up as a 12-year old child (i.e., by selecting 1998 as year of birth) on *ZAP.* Rather, only users aged 13 and above are allowed to sign up.

Signing up to the SNS website requires ticking a box that indicates that the Terms of use are accepted. Next, the date of birth and other information (e.g., name, nickname, sex) have to be entered. Entering the birth data of a 9-year old child leads to a rejection of the user during registration. However, simply changing the year of birth from 2001 to 1997 (but not to 1998, see above) led to successful signing up, confirming the fact that ZAP does not take any extra steps to ensure that children younger than 12 do not re-register on their site. However, the SNS provider ensures limited exposure to potentially inappropriate material and contact for minors, for example, by removing content or deleting accounts of users that posted inappropriate content.

During testing the "Buzz words filter" functionality was tested. To test for automatic identification of inappropriate behaviour and abusive users, a (fake) female minor was "bullied" by two other (fake) minors who explicitly used offensive Luxembourgish derogatory terms. A bullying picture was also uploaded to a new photo album entitled "dirty X" on the personal page of one of the "bullies" and a comment was posted on the wall of the "bully victim". However, no actions were taken by ZAP, the offensive content was not removed and none of the "bullies" received any warnings indicating that the "Buzz words filter" functionality is ineffective.

In relation to advertising, when signed up as the 15-year old girl, banner advertising was present on the top and on the right side of the minor's personal page. One banner announced the availability of a mobile version of *ZAP*. The second banner automatically switched between an announcement of a so-called "flirt party" (with only date and venue shown) and an e-commerce ad for tires. No other advertisement was present.

Confirming the analysis of the self-declaration, parental control tools are missing on the SNS. However, the Protection of minors document includes a "what parents can do" section.

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

According to its self-declaration several tools and technologies are employed by ZAP to assist children and young people in managing their experience on their service, particularly with regards to inappropriate or unwanted content or conduct, for instance profiles and homepages of users under 16 are not searchable and users under 16 cannot be browsed. By default profiles of users aged 13-16 are "not public", i.e. "they are unsearchable by age on search engines". But this does not necessarily mean that their profiles are "private by default"[61] as defined in the Safer Social Networking Principles[62]. Besides, nothing is mentioned about the default privacy settings of 17-18 year olds.

According to the self-declaration, however, users can manage the access to their profiles, for instance by "opening" their profile to friends, by reject friendship requests or by putting users to the "ignore list". Ignored

[61] "Ensuring that setting a profile to private means that the full profi le cannot be viewed or the user contacted except by 'friends' on their contact list".

[62] http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

users cannot post further messages, ratings or comments on the "protected" profile. Users can, thus, restrict access to the different sections on their profile and they can always report inappropriate behaviour on the site.

Main findings in relation to the website

As opposed to what is stated in the self-declaration, testing on the site revealed that registered adults of ZAP can search for personal profiles of 13- and 15-year old minors by using *ZAP*'s searching function. Also, using Google's search function returned the full profile (e.g., age, personal preferences, sexual orientation, private messages, pictures) of the 15-year old minor, but not that of the 13-year old created for this test. However, because the two minors were friends on *ZAP,* postings of the 13-year old on his profile were also displayed on the profile of the 15-year old. Testing revealed that these postings (e.g., a picture) serve as a link and that simply clicking on his postings was sufficient to gain access to the full profile of the younger user. Adults may also add minors to their contact list without restriction. Likewise, minors may accept the adult's invitation and add them to their contact lists without any restrictions, either. During testing, no tool was found to enable the user to restrict the search options of others (e.g., in order to prevent adults from contacting minors). In sum, these observations are in sharp contrast to the self-declaration of the SNS provider.

In line with the self-declaration, testing revealed that the *ZAP* website offers various tools that empower users. These include specifying user groups that may or may not contact the user (i.e., blocking function), as well as specifying actions with regard to the availability or accessibility of individual profiles (i.e., restricting access to certain sections of the personal profile). Users may also delete unwanted comments, prevent posting of public messages on their profile, and report unsuitable behaviour.

Finally, apart from the safety information provided to parents via the Protection of minors section (see Principle 1), parents are not provided with any (parental control) tools to help them protect their children.

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service

Main findings in relation to the self-declaration

In its self-declaration ZAP refers to the available mechanisms to report inappropriate content, contact or behaviour that violates the Terms of Service, namely a Report button on the top of every page and a Report abuse email available from the contact info. No information is provided in the self-declaration regarding if or how the reports are acknowledged or if the reports are acted upon expeditiously. The self-declaration does not mention if users are provided with an indication of how their reports are typically handled, either.

Main findings in relation to the website

Confirming the analysis of the self-declaration, a list of e-mail addresses may be found in the Contact and Support document ("Kontakt und Support"), which is located on the bottom of each page of the *ZAP* website. Inappropriate pictures and behaviour may be reported via different e-mail addresses (e.g. pictures@zap.lu; abuse@zap.lu). In addition, a "Report" button serves as an alternative to report inappropriate conducts or content. The "Report" mechanism is found easily and quickly. Clicking on the "report webpage" button opens a window that provides the user with a text box, in which observations may be entered. In addition, the user is presented with a (non-exhaustive) selection of topics (e.g., violation of Terms of use, pornographic content). In some cases, for instance in the case of bullying, it may be difficult to decide which label to use because no explicit "report person" option is provided.

As part of this study, a (fake) minor user reported that she had been bullied on this SNS. A realistic bullying situation was set up between the (fictitious) owners of profiles that were created for this assessment. The scenario consisted of one minor being bullied by two other minor users who posted a nasty comment on the wall of the "victim" and who uploaded and/or sent hurtful pictures. As the "victim" could not cope with the nasty comment put on her profile and the embarrassing pictures, she contacted the provider. Given the aforementioned fact that the “Report” button on the *ZAP* website has no explicit “report person” option, it was decided to contact the provider via “abuse@zap.lu“. However, the e-mail returned twice with a “message delivery failure”. Finally, the message was sent using the e-mail address “contact@zap.lu“. This time, the report message was acted upon expeditiously (approx. 22 minutes). Using a succinct language, the e-mail explained that the offensive pictures had been removed and that both users who had sent the bullying messages had been sent warnings. Indeed, this was the case. In sum, the test demonstrates that reporting mechanisms are not very user-friendly and that ZAP replies expeditiously to user reports.

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

The self-declaration indicates that users` uploads are daily checked by ZAP administrators. Content that breaches Zap`s Terms of Service is immediately removed. “Minor infractions may lead to a warning” while repeated ones may lead to being removed from the service. Illegal contents and conducts are always reported to the law enforcement.

Because of ethical reasons, Principle 5 was not tested in the website.

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

Main findings in relation to the self-declaration

According to its self-declaration ZAP provides its users with a range of privacy setting options: During registration only the name and the age of minors is shown by default and no other personal information. Users can, then, manage how many details they want to publish about themselves. Furthermore, advice to adapt users’ privacy level is provided. In the Guidelines ZAP encourages users not to reveal any private information, such as phone number or address. ZAP users are encouraged, however, to register using their real names, and their real pictures, to remind them that they are accountable for their actions. This also allows ZAP to more easily identify potential abusers.

The self-declaration does not mention if the privacy settings options are prominent and accessible at all times or if users are allowed to view their privacy status or settings *at any given time.*

Main findings in relation to the website

In accordance with the self-declaration, testing revealed that changing privacy settings is always possible by clicking on the button “account configuration” (“säit administréiren”), which is visible at any time. Changing settings is easy, even for minors. Also, third-party applications will be installed only after previous permission of the user. For the initial step of the first-time registration process, entering e-mail address and individual password is sufficient. Next, a so-called “profile configuration” window appears, which also includes checkboxes on adult-relevant information like, for example, user’s sexual orientation and marital status (although both may be set to “secret”), name of the partner, and main interests of using the SNS. Having to provide this information is surprising, because the self-declaration indicated that users are encouraged not to reveal any private information. Following registration, real name or nickname is automatically inserted into the user profile, depending on the user’s previous decision, together with information on age, gender, and user’s hometown. E-mail is not visible, though. Sexual orientation and marital status (if not set to “secret”) as well as main interests are also displayed on the profile page.

Default settings render minor’s personal information visible to all other users (“Jiddereen”). Restricting the visibility therefore depends on the account owner’s additional activity. This is in contrast to the self-declaration of the SNS that only the name and the age would be shown by default. Also, this is not in line with the information presented in the Protection of minors, which encourages the user not to reveal private information or photos. Apart from this general information on online privacy, there is no additional information on the personal profile that would remind users not to reveal private information.

Finally, deleting a user account is easy. It is possible to do it via a dedicated web link and users receive a warning that all data will be lost.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

Main findings in relation to the self-declaration

ZAP`s self declaration indicates that all uploads on their website are daily checked by ZAP administrators and that content that breaches Zap`s Terms of Service is immediately removed from the site. In the background, the frequency with which adults contact minors is counted. "Great age differences between corresponding users as well as suspicious behaviour are leading to an investigation of the profiles in question". It is not explicitly mentioned, though, how the mechanisms to determine the most appropriate procedures for reviewing reports of illegal or inappropriate content or conduct are assessed.

Principle 7 was not tested in the website.

Summary of Results and Conclusions

Principles 1, 2, 4 and 6 are rather satisfactorily implemented and Principle 3 is unsatisfactorily implemented on ZAP`s website. The testing on the website revealed some problematic areas, for instance:

- Profiles of minors are not set to "private by default" as defined by the Safer Social Networking Principles. As a matter of fact, both registered and non-registered users can have access to the profile data of minor users either via the internal ZAP search engine or via external ones.
- Lack of effective age control systems to register on the site.
- Reports are handled very expeditiously, but they are not particularly user-friendly.
- The "Buzz words filter" functionality is ineffective.
- Lack of additional educational material for parents and caregivers in the Luxembourgish version of the Terms of use.
- Lack of consistency in the different language versions of the Terms of use.

Assessment of all the Principles in the Self-declaration

Principle	*Very satisfactory*	*Rather Satisfactory*	*Unsatisfactory*
1	x		
2		x	
3		x	
4		x	
5	x		
6		x	
7		x	

Implementation of the Self-declaration on the SNS

Principle	*Very satisfactory*	*Rather satisfactory*	*Unsatisfactory*
1		x	
2		x	
3			x
4		x	
6		x	

This is a report made by request of the European Commission under the Safer Internet Program

The Copyright of this report belongs to the European Commission.

Opinions expressed in the report are those of authors

and do not necessarily reflect the views of the EC.

FOR FURTHER INFORMATION:
DIRECTORATE-GENERAL
INFORMATION SOCIETY AND
MEDIA
EUROPEAN COMMISSION
SAFER INTERNET PROGRAMME
E-MAIL:
SAFERINTERNET@EC.EUROPA.EU
FAX: + 4301 34079
OFFICE: EUFO 1194
EUROPEAN COMMISSION
L-2920 LUXEMBOURG

http://ec.europa.eu/saferinternet