

Evaluation of the Implementation of the Safer Social Networking Principles for the EU Part I: General Report

By request of the European Commission
under the Safer Internet Programme

Authored by:
Elisabeth Staksrud, University of Oslo,
& Bojana Lobe, University of Ljubljana



European Commission
Information Society and Media

**THIS IS A REPORT MADE BY REQUEST OF THE EUROPEAN COMMISSION
UNDER THE SAFER INTERNET PROGRAMME**

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.**

January 2010

Please cite as follows:

*Staksrud, E. and Lobe, B. (2010) Evaluation of the implementation of the Safer
Social Networking Principles for the EU Part I: General Report. European
Commission Safer Internet Programme, Luxembourg*

Contents

Executive Summary	5
Methodology	12
What do the SNSs say they do?	14
Have the SNSs done what they say they have done?	15
Overall level of compliance	15
Overall compliance of Principle 1-7 among all signatories	17
Evaluation of Principle 1 – “Raise Awareness”	18
Does the SNS provide targeted guidance and educational material?	18
Is information presented in a prominent and accessible format?	19
Do providers have clear safety information for children and teens?	20
Is it made clear to users what constitutes inappropriate behavior?	21
Is safety information on specific risks provided?	22
Evaluation of Principle 2 – “Age appropriate services”	24
Can 11-year olds have access to a restricted site?	26
Can an 11-year old get access to a restricted site by changing her age?	26
Evaluation of Principle 3 – “Empower users”	27
Are profiles of underage users set to private by default?	27
Are private profiles of users below 18 searchable?	28
Who can post comments on a user’s profile?	28
Can users control who can access their full profile?	30
Can users remove content from their own profile?	31
Evaluation of Principle 4 – “Easy-to-use mechanisms for reporting violations”	32
Are reporting mechanisms easy to understand?	32
Are reports acknowledged?	33
Are reports acted upon expeditiously?	33
Evaluation of Principle 5 – “Respond to notifications of illegal content/conduct” ..	35
Evaluation of Principle 6 – “Encourage a safe use approach to privacy”	36
What personal information is typically asked for when creating a profile?	36
What personal information is automatically inserted into a profile	37
Is it easy to change privacy settings?	37
How easy is it to delete the profile?	38
Evaluation of Principle 7 – “Reviewing illegal or prohibited content/conduct”	40
References:	41
Annex 1. Background and objectives for the testing	i
Annex 2. Safer Social Networking Principles	iii
Annex 3. Testing Questionnaire	viii
Annex 4. Description of participating Social Networking Sites	xxiv

Table of figures:

Figure 1.	Number of SNSs by compliance between Principles and self-declaration report	14
Figure 2.	Categories of SNSs after compliance between Principles and self-declaration.....	15
Figure 3.	How many Principles the social networking services have complied with	15
Figure 4.	How many of the Principles the social networking services have partially complied with	16
Figure 5.	Categories of SNSs after compliance between self-declaration and service	16
Figure 6.	Total testers' assessment of compliance between SNS self-declaration and services by Principle	17
Figure 7.	Existence of types of information on the SNS sites for potential users.....	18
Figure 8.	Format of safety information provided on the SNS sites	19
Figure 9.	Types of information that are easily found for users before signing up	20
Figure 10.	Is information targeted towards children and teens easy to understand?	21
Figure 11.	Information on and consequences of engagement in prohibited behaviors/actions are clearly stated for users	21
Figure 12.	Frequency of safety information found on specific risks by number of SNSs	22
Figure 13.	Overview of minimum age for registration.....	24
Figure 14.	Restrictions aimed at ensuring age appropriate services for users according to self-declarations	25
Figure 15.	Attempts to sign up to age restricted sites	26
Figure 16.	Testing if testers had to change settings for personal information to be visible to other users on SNSs stating in their self-declarations that profiles for under-aged users are set to private by default ...	27
Figure 17.	Testing results when searching for profiles of under-aged users	28
Figure 18.	Who can post comments on user's profile?.....	29
Figure 19.	Who can post comments on profiles of under-aged users by their privacy settings	29
Figure 20.	Visibility of personal information on the service.....	30
Figure 21.	Response time to users asking the social networking services for help	33
Figure 22.	Personal information asked for when creating a profile by number of SNSs.....	36
Figure 23.	Personal information automatically displayed in profile.....	37
Figure 24.	Available information on deleting or deactivating profiles on the SNS services	38
Figure 25.	Reported steps taken by SNSs to "review illegal/prohibited content".....	40

Executive Summary

- This report is a part of the European Commission’s commitment to and support of the self-regulatory initiative from social networks to implement “Safer Social Networking Principles” signed by 20 social networking companies in 2009. The report analyzes the 19 self-declarations¹ submitted by the signatories of the Principles as well as 25 of the services offered among these companies in order to give an overview of the general level of implementation. All services have been tested in their original language version by a team of 13 national and two lead experts.
- The report consists of two parts – the first part gives an overall analysis of findings across the services evaluated. The second part consists of individual testing reports for all SNSs that have signed the agreement.
- Comparing the compliance between the Principles and what is reported in the self-declaration reports *excellent compliance* is found with eight SNSs, eight services have *good compliance*, five services have *fair compliance*, and one service has *poor compliance*.
- On an overall level, the compliance between what is stated in the self-declaration reports against what is found on the services themselves is assessed with the following results:
 - *Excellent compliance* is found with two SNSs, ten services have *good compliance*, ten services have *fair compliance*, while no service is assessed as having *poor compliance* between the self-declaration and what was found on the service during testing.
 - Principle 3 (“empower users”) Principle 6 (“Encourage safe use approach to Privacy”) are the principles best implemented. Also Principle 1 (“Raise awareness”) has a high score on *compliance*.
 - Principle 2 (“Age-appropriate services”) and Principle 4 (“Easy to use mechanisms for reporting violations”) are assessed to be the principles where the compliance between what is stated in the self-declaration and what is observed on the service itself is the lowest, as the majority of services are assessed to be *partially compliant*.
- Comparing the self-declaration reports with the services themselves, there is a general under-reporting on measures and tools available on the site. On the negative side this indicates that the self-declaration reports are incomplete; on the positive side more relevant safety measures are available to the ordinary user than stated by the SNSs.

¹ *Giovani* has not submitted a self-declaration.

Summary Principle 1 – “Raise Awareness”

- Testing reveals that while most services give sufficient information on Terms of use/service, such information cannot be found on three services. Information on privacy/privacy policy cannot be found on four services.
- While 17 services² provide safety tips/information for children and young people before they sign up to the service. This information could only be found easily on nine services.
- Safety information for younger children was assessed as difficult or not possible to understand on one third of all services with such information.
- Information for parents and teachers could be found on 16 services, while safety tips for teachers could be found on only five services.
- All services except one have information on what content and conduct is not allowed, but on five of these services this information is assessed as being difficult to understand for children and young people.
- General textual information is the most common format for safety information (22 services). Least common is general audio/video information (found on six services). External links/referrals to professional safety organizations and authorities are found on 18 of the 25 services.
- Regarding awareness and safety information on specific risks, information on online bullying, risks of divulging personal information, and hate speech is most frequently found by testers, followed by information on the risk of posting sexually provocative photographs.
- Of the 25 tested services, very few have information on the risks of inappropriate contact from adults with a sexual interest in children (seven services), the possibility of seeing or being the subject of images of child abuse (six services) or information on self-harm actions (three services).

² Two additional services were assessed not applicable during the test but actually provide safety tips/information for *teenagers* so the total number of services with information available for users below 18 years is 19.

Summary Principle 2 – “Age appropriate services”

- All services tested used/asked for birthday data at the registration process
- E-mail verification from the user or user’s parent is required on 20 services but the testers were able to sign up without confirming over e-mail on seven of these services.
- For sites that deny signing up as an 11-year old user, another attempt was made, with the same profile, but with a different birth-date pretending to be a 15-year old. On seven services changing the date of birth/age was enough to grant access. On two additional services this could be done after a cookie was removed, while on 12 services the tester could not sign up. All testers were later able to sign up with a new profile as an older user adhering to the age-requirements of the service on the same computer/device.
- Only seven services state in their self-declaration that they promote parental control tools on their service. The testing of these services reveals that the parental control tools can easily be found on three of the services, not easily found on two services and not found at all on two services.

Summary Principle 3 – “Empower users”

- Statements that profiles are set to private by default for users below 18 years are given by 14 SNSs in their self-declarations, but this is only found by testers in seven of the cases. On five services of the some information is publicly available, while in two cases the profile is not found to have any specific restrictions. Of the SNSs that do not make such claims in their self-declaration report, the test reveals that six additional SNSs have such a mechanism on their site.
- On eight services it was possible to search for users/user profiles that are 12 years or younger on the service/SNS itself. In addition 11 services allowed the profiles of underage users to be available through common search engine(s).
- Users can delete/remove *postings* on their own profile on 22 services, while 18 services allows for users to delete/remove *pictures* on their profile

Summary Principle 4 – “Easy to use mechanisms for reporting violations”

- A majority of services (19) are found to have a link/information available at all times on where to report *content* that bothers the user and/or is a violation of terms.
- A majority of services (18) are found to have information available all the time on where to report *other users* that bother them/conduct violations of terms, while on four services such information is only found after considerable searching.
- The reporting mechanism on 15 of the services was considered to be easy to understand for children and young people, while eight were considered not to be.
- Of the services tested for having report mechanisms, 14 of 22 comply with the recommendation of acknowledging reports from users.
- Of a total of 22 services tested for report mechanisms, 13 did not give any reply to a message from an underage user asking for help sent through their reporting mechanism, two replied within a week (3-4 days), while seven replied within 24 hours.

Summary Principle 5 – “Respond to notifications of illegal content/conduct”

- Most SNSs (22 of 24 services with a self-declaration report) state that they share reports of illegal content or conduct with relevant law enforcement bodies and/or hotlines.
- A majority of SNSs (19) explicitly state that they have effective processes for reviewing and removing illegal content or conduct.
- For ethical reasons Principle 5 is not tested.

Summary Principle 6 – “Encourage safe use approach to privacy”

- Users are typically required to submit their e-mail, real name and gender when signing up to a service
- Often other personal information is asked for, but optional for the user to submit

- The most frequently automatically uploaded personal information is gender and real name (both first and last) followed by age. Profile pictures are automatically uploaded on every fourth service. One service automatically displays the user's phone number.
- Four services allow users submitting personal security/identification number and ask for their political sympathies and religious affiliation.
- On 14 services testing found that the user has control over the display of his/her online status (whether other people could see if they are online).
- Information on how the users can delete their profile is found on 18 of 25 services. On five services the profile cannot be deleted, just deactivated.
- Eight of 25 services offer information on how personal information may be used by the service after the profile is deleted.
- How to change privacy settings is easily found on all services except one.
- Eight services provide users with safety tips and/or information about publishing personal information when they are about to publish information on their profile and twelve services do the same for users when trying to upload a photo on ones profile.

Summary Principle 7- "Reviewing illegal or prohibited content/conduct"

- SNSs report having various measures for reviewing illegal or prohibited content/conduct, where human and/or automated forms of moderation are most common (23 services).
- Only five of 24 services report to having taken steps to minimizing the risk of employing moderators that may be unsuited for work which involves real-time contact with children and young people.
- Principle 7 is not tested for ethical and practical reasons.

INTRODUCTION

In 2008, as part of its Safer Internet Plus Programme, the European Commission gathered 18 of the major online social networks active in Europe as well as researchers and child welfare organizations to form a European Social Networking Task Force to discuss guidelines for the use of social networking sites by children and young people. As a result “the Safer Social Networking Principles for the EU” were developed by social networking services providers in consultation with the Task Force. The aim was to “provide good practice recommendations for the providers of social networking and other user interactive sites, to enhance the safety of children and young people using their services” (European Commission, 2009).

The guidelines were adopted voluntarily by the major online social networks active in Europe, and signed on Safer Internet Day, February 10th 2009.

The Principles are meant as a guidance to SNS providers when they seek to minimize potential harm to children and young people ("Safer Social Networking Principles of the EU," 2009: 1). They recommend a wide range of good practice approaches, allowing for the diversity and judgment of the social networks themselves in terms of relevance and implementation. Within the context of the Principles, “Social Networking Services” are defined as services that combine the following features ("Safer Social Networking Principles of the EU," 2009: 3):

- A platform that promotes online social interaction between two or more persons for the purposes of friendship, meeting other persons, or information exchange;
- Functionality that lets users create personal profile pages that contain information of their own choosing, such as the name or nickname of the user, photographs placed on the personal page by the user, other personal information about the user, and links to other personal pages on the service of friends or associates of the user that may be accessed by other users or visitors to the service;
- Mechanisms to communicate with other users, such as a message board, electronic mail, or instant messenger; and
- Tools that allow users to search for other users according to the profile information they choose to make available to other users

The European Commission has, as part of its extensive encouragement and support of the self-regulatory initiative of the SNS providers committed to monitoring the implementation of the Principles within one year of the signature of the agreement. This report is a part of that commitment.

The core purpose of this report is to assess how the signatories of the *Safer Social Networking Principles for the EU* have considered the Principles, by analyzing the *self-declaration reports*³ submitted by the social networks between April 10th and June 17th 2009 and testing the corresponding *SNS Services* (25 services in total).

³All these reports are public and can be downloaded from the European Commission’s website:

http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm#self_decl (link valid as of August 2009).

Of a total of 20 signatories, 19 reports are available (by the date the test was performed this report was written the self-declaration report from *Giovani.it* was not available). Below is a summary of the participating Social Networks, date of their accession to the Principles and date of submission of their self-declarations. Please see Annex 4 of this report for more detailed information on the signatories and the relevant SNS services they offer.

Signatories	Date of accession to the Principles	Date of submission of the self-declarations
Arto	10 February 2009	15 April 2009
Bebo	10 February 2009	17 April 2009
Dailymotion	10 February 2009	10 April 2009
Facebook	10 February 2009	16 April 2009
Giovani.it	10 February 2009	<i>Not Available</i>
Google	10 February 2009	15 May 2009
Hyves.nl	10 February 2009	17 April 2009
Microsoft Europe	10 February 2009	17 April 2009
MySpace	10 February 2009	17 April 2009
Nasza-klasa.pl	10 February 2009	1 May 2009
Netlog	10 February 2009	28 May 2009
One.It	10 February 2009	17 June 2009
Piczo	10 February 2009	16 April 2009
Rate.ee	9 June 2009	9 June 2009
Skyrock.com	10 February 2009	29 April 2009
StudiVZ.de	10 February 2009	17 June 2009
Sulake/Habbo.com	10 February 2009	15 April 2009
Tuenti	12 June 2009	12 June 2009
Yahoo!Europe	10 February 2009	17 April 2009
ZAP.lu	10 February 2009	17 April 2009

This report is meant to give a comprehensive and clear view of:

- Safety measures taken by the signatories
- The extent of implementation of the Principles in terms of compliance between what has been stated in the self-declarations vs. what was found when testing the measures and features on the Social Networking sites.

In this first part of the report this is done by providing an overview of the implementation of the Principles by the group as a whole, by analyzing the coverage of different services under each principle, and what

specific types of measures have been implemented. The second part consists of individual testing reports for each SNS that has signed the Principles.

Methodology

As part of this assessment a test was conducted on a specified set of the measures implemented by the Social Networking Sites that have signed the self-regulatory agreement the “Safer Social Networking Principles for the EU”. The test has been developed by the two lead experts Bojana Lobe, University of Ljubljana, Slovenia and Elisabeth Staksrud, University of Oslo, Norway. In the draft stage, the testing questionnaire was submitted to the Social Networking Task Force for its comments as well as suggestions. The European Commission approved the final version.

A team of 13 national experts, testing the main language version of the signatories’ sites, conducted the testing itself in October/November 2009. The national experts were given detailed instructions on how to perform the testing in order to ensure as much consistency in the testing process as possible.

Of the 20 companies that signed the agreement some offer more than one service that is stated to comply with the Principles. This resulted in a total of 25 different services being tested.

The child safety policies of the signatories were assessed in a two-step process: on the level of assessing self-declaration against Principles, followed by assessment of what has been stated in SNS’s self-declarations against what has been observed on their services.

Therefore, the test questionnaire consists of two parts for each principle. The first part closely resembles the main points of each Principle and introduces them in a question-like format in order to test whether the SNSs have addressed those points in their self-declarations. Following that, each of seven of the Safer Social Networking Principles is operationalized into quantitative indicators measured against various scales in order to perform a test on the sites themselves. The operationalization is mainly based on a coding scheme developed in an analysis of the self-declaration reports. The Social Networking Sites are then evaluated individually against the indicators. This enables us to make a thorough and comprehensive assessment of each SNS separately and yet all the data can be merged into a common data set to conduct an overall analysis and get a broader perspective across the SNSs on specific issues that apply to most of them.

Direct comparisons between SNSs are limited, due to the specificity, purpose and different nature of each service. However, a limited degree of comparability was achieved through a standardized and closed testing questionnaire that experts had to fill in. Such questions are more likely to be understood in the same way, as there is less room for self-interpretation, which increases the validity of the results.

For as much standardized reporting as possible, the instructions to national testers also provided details on how to structure and organize their national reports. For each Principle, they were asked to focus on the extent to which the actions mentioned by SNSs in the self-declarations are in line with the Principles (based on the part of the questionnaire linked to the self-declaration). Further, they focused on whether the measures reported by the signatories in their self-declaration reports have been implemented the site and if so, was the implementation effective and how it worked on the site. Finally, they were asked to provide a global compliance table, for each Principle assessing the compliance between the self-declaration and the implementation of the measures on the site.

The draft national reports have been submitted to the social networking companies for comments. Before finalizing the reports, national experts considered these comments where applicable.

Addressing ethical considerations of testing such sites, the national experts were asked to choose two imaginative nicks/testing names for testing purposes. In this way, the test avoided including any real under-aged children and the potential risks that such actions could have resulted in.

It is important to emphasize that this evaluation also has limitations. The participating Social Networking Sites are a diverse group offering different types of services, directed towards different types of audiences. The test design has therefore allowed for testing various types of services, and an assessment of the quality of implementation of some of these services. The test and subsequent reports are based solely on the self-declaration reports from the SNS, and testing performed by independent, adult expert testers, and does thus not represent a direct analysis of the services as they are used by a regular (minor) user. Please also note the following.

- *Not all safety tools are relevant to all services.* The services included in this report are different in terms of target groups, features, and aims. Hence, not all tools or measures will be relevant for all services. Therefore, if a particular SNS has not implemented a safety tool or policy, this does not necessarily constitute a safety “problem”.
- *Not stating does not imply not doing.* The declaration form used by the services that signed up to the Principles has open ended questions. This means that not all relevant features, tools and policies may have been reported on, or are reported on in such a way that they could be operationalized for direct comparison. For instance, the statement that “we cooperate closely with the authorities” gives no indication whether illegal material found on the SNS is forwarded to the police. Similarly, several SNSs mention the use of “many tools” without further specifying which may result in them not being specifically registered as e.g. having a privacy policy, even if such policy should exist.
- *Safety is not an exact science.* The view of risk, safety and what constitutes efficient protective measures in relation to children, youth and the Internet varies by country, culture, age, beliefs and so forth. This is also reflected in the safety approaches taken as described in the self-declaration reports. For instance, some will encourage the use of real names on their services, some require it, and so do not, or will not, display real names and require a “nick”. All approaches can be validly argued for on the basis of Internet safety, hence can be assessed as “compliant” even if diametrically different in practice.
- *A report represents a moment in time.* All services reported on different times (between April 10th and June 17th2009), while testing was performed during Oct/November 2009. Changes occurring after the self-declaration was submitted and the testing performed have not been taken into account. In addition the testing process has allowed for the industry to submit additional information on the new features of their services that have been developed both since the self-declaration was submitted and since the testing occurred. This information can be found in separate reports published by the European Commission.

RESULTS

What do the SNSs say they do?

On an overall level the testers were asked to assess the compliance between the signed agreement and the self-declaration report submitted, for each Principle separately (for more information on the specifics of the Principles please refer to Annex 2). This could be done for all but one service (Giovani), where a self-declaration report has not been submitted. For two SNSs, services were merged when assessing compliance: Habbo Hotel and IRC Galleria (Sulake) and StudiVZ and meinVZ (VZnet Netzwerke Ltd).

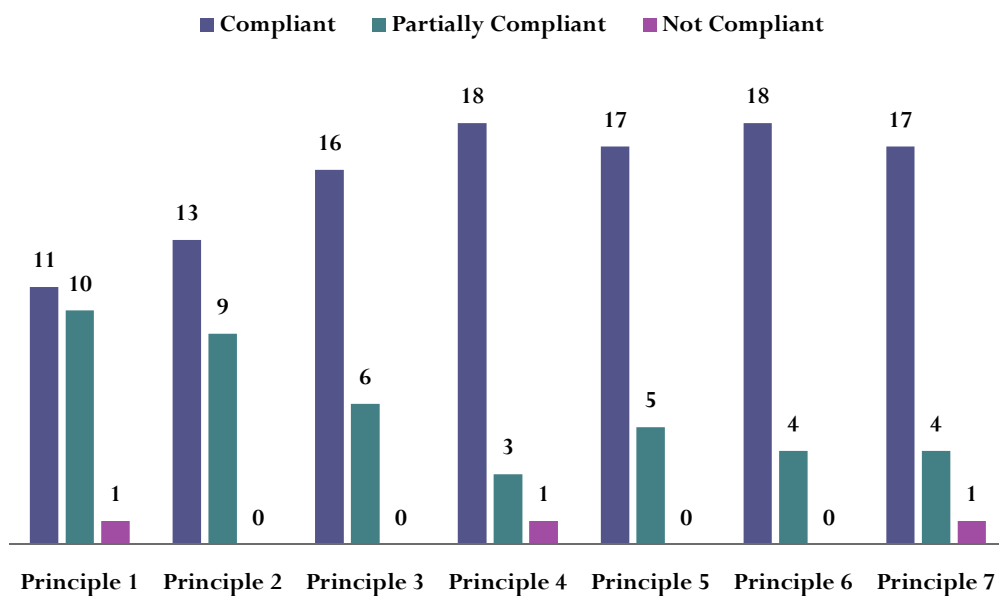


Figure 1. Number of SNSs by compliance between Principles and self-declaration report

Figure 1 above shows that the assessed compliance varies between the Principles. The services are more in compliance with Principles 4-7 and less in compliance with Principles 1, 2 and 3. It can also be noted that very few of the submitted self-declarations are considered to not be in compliance with the Principles at all.

Summarizing the compliance based on what the SNSs stated in their self-declaration versus what is stated in the signed Principles, the services were given a score of “2” for each compliant principle, and a score of “1” for each principle the partially complied with. No points were given for “not compliant”. Figure 2 below shows the distribution of services in terms of compliance.

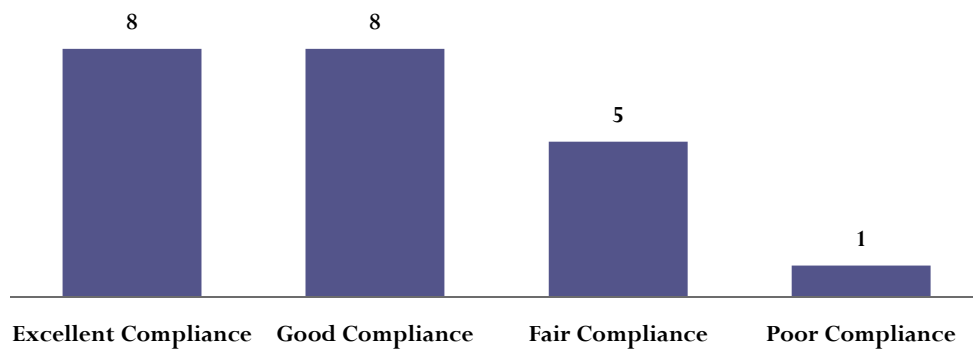


Figure 2. Categories of SNSs after compliance between Principles and self-declaration.

Excellent compliance was found with eight SNSs (full score of 14 points), eight services had good compliance (11-13 points), five services had fair compliance (7-10 points), and one service scored only four points, hence, being assessed as having poor compliance between the signed Principles and what was reported in the self-declaration.

Have the SNSs done what they say they have done?

This section contains an overview of the combined level of compliance between the self-declaration report and the services tested as assessed by the expert testers – in short: How many of the signatories have done what they have said they have done in their self-declarations?

Overall level of compliance

Figure 3 below shows the distribution by level of compliance of the services. Only two services got a fully compliant score on all principles tested, while two services did not get any principles assessed as fully compliant when comparing the self-declaration report with the service itself.

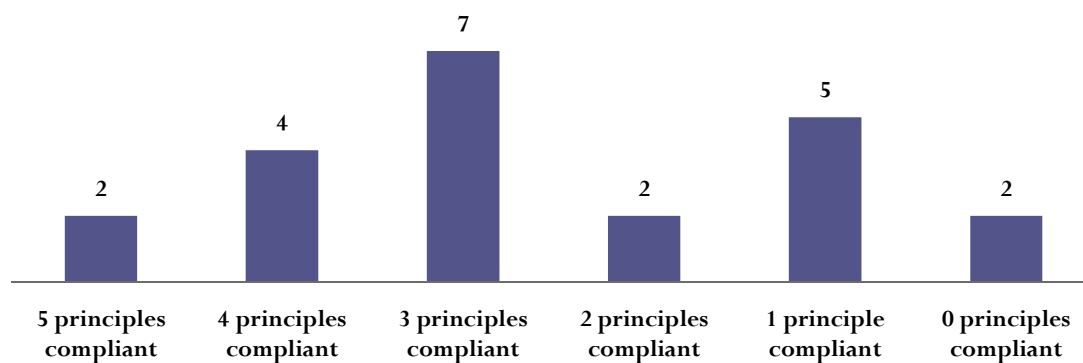


Figure 3. How many Principles the social networking services have complied with

Figure 4 below shows the distribution of services according to how many of the principles they have been assessed as being partially compliant with. Six services were assessed as partially compliant with two principles and two services were assessed as partially compliant with all five tested principles. Finally, when it comes to “not-compliant”, two services have been assessed as not compliant with one principle.

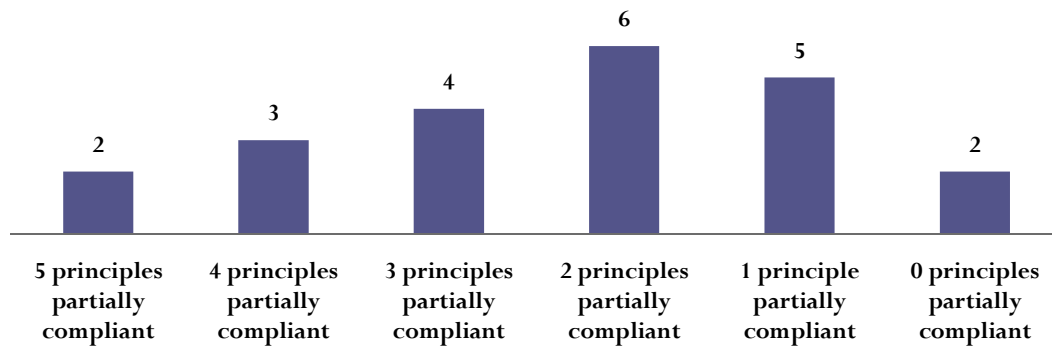


Figure 4. How many of the Principles the social networking services have partially complied with

The assessment in the figures above show that the SNSs are on different stages in terms of implementing the Principles. While very few are compliant with all or most Principles, many are partially compliant, and non-compliance is rare.

Summarizing the compliance among the services based on what they stated in their self-declaration, the services were given a score of “2” for each compliant principle, and a score of “1” for each principle the partially complied with. No points were given for “not compliant”. Figure 5 below shows the distribution of services in terms of compliance.



Figure 5. Categories of SNSs after compliance between self-declaration and service

Excellent compliance was found with two SNSs (full score of 10 points), 10 services had good compliance (8-9 points), 10 services had fair compliance (5-7 points), while no service scored lower than 4 points (equivalent of e.g. 2 complied principles or 4 partially complied principles).

Overall compliance of Principle 1-7 among all signatories

As part of the testing, all experts were asked to assess the compliance between what the signatories had stated in their self-declaration and what was found when testing the specific services. All principles except 5 and 7, both relating to the reporting and handling of illegal content, were tested through a wide range of exercises. Figure 6 below provides an overview of the total result of the testers' assessment of the 22 services tested.⁴

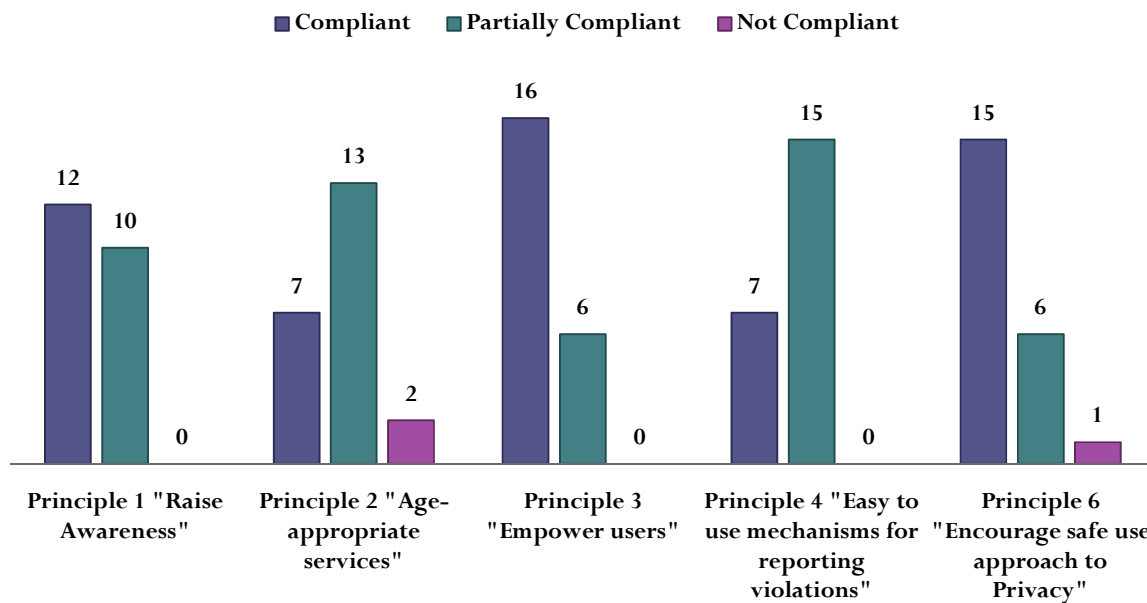


Figure 6. Total testers' assessment of compliance between SNS self-declaration and services by Principle

A majority of services complied with Principle 3 ("empower users") with 16 compliant services and 6 partially compliant, and Principle 6 ("Encourage safe use approach to Privacy") with 15 compliant services and 6 services partially compliant. Also, many services were compliant with Principle 1 ("Raise awareness") (12 compliant vs. 10 partially compliant).

For Principle 2 ("Age-appropriate services") and Principle 4 ("Easy to use mechanisms for reporting violations") the compliance between what is stated in the self-declaration and what is observed on the service itself is the lowest, as more services are assessed as being partially compliant.

Finally, non-compliance can only be found in three cases: two services under Principle 2 and once service under principle 6 were assessed as being not compliant. No service was found to be not compliant with more than one Principle (ref. to "overall level of compliance of SNS services" above).

⁴ Some signatories have included more than one service in their self-declaration report that has been tested and assessed for compliance separately. As there is no self-declaration report from *Giovani*, this service is not included in this table. Please refer to the *Giovani* testing report for more detailed information. For two SNSs, services were merged when assessing compliance: *Habbo Hotel* and *IRC Galleria* (Sulake) and *StudiVZ* and *meinVZ* (VZnet Netzwerke Ltd).

Evaluation of Principle 1 – “Raise Awareness”

The first principle states that Social Networks should “*Raise awareness of safety and education messages and acceptable use policies to users, parents, teachers and carers in prominent, clear and age-appropriate manner*”. The principle is operationalized into five specific recommendations (“Safer Social Networking Principles of the EU,” 2009: 6):

- Providers should create clear, **targeted guidance and educational materials** designed to give children and young people the tools, knowledge and skills to navigate their services safely.
- These **messages should be presented in a prominent, accessible, easy-to-understand and practical format**.
- Service providers should **provide clear information about what constitutes inappropriate behaviour**.
- Providers should **offer parents targeted links, educational materials and other technical controls** as appropriate with the aim of fostering dialogue, trust and involvement between parents and children about responsible and safer internet use.
- SNS providers should ensure that such materials also **empower teachers** to help children use SNSs safely and responsibly.

In order to test Principle 1, the testers were asked a variety of questions aimed at both assessing the location of the information (how easy it was to find) and the quality of the information (e.g. is it understandable for children and young people).

Does the SNS provide targeted guidance and educational material?

The availability of key awareness information, such as terms of use, were tested as a user thinking of signing up to the service, or a parent wanting to learn more about the service their child have signed up to. The availability of such information was therefore tested before user profiles were created on the respective sites.

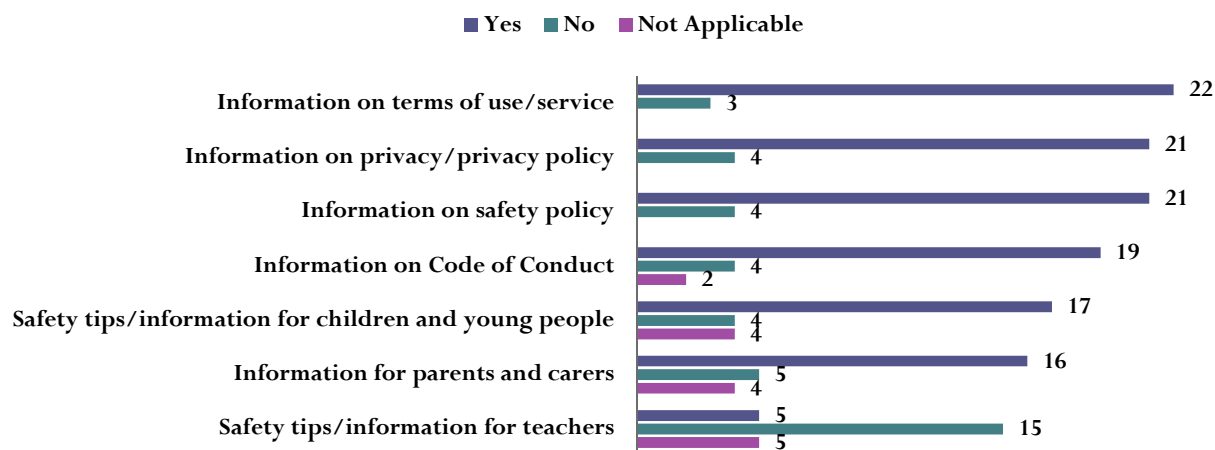


Figure 7. Existence of types of information on the SNS sites for potential users

Figure 7 shows that the majority of services provide key awareness information. Information on terms of use is the most frequently shown information. Safety tips/information for children and young people were stated to be found on 17 services. Two additional services were assessed not applicable during the test but actually provide safety tips/information for *teenagers* so the total number of services with information available for users below 18 years is 19. Information for parents and carers were found on 16 of the services, whilst the least safety tips and information is available for teachers (only five services).

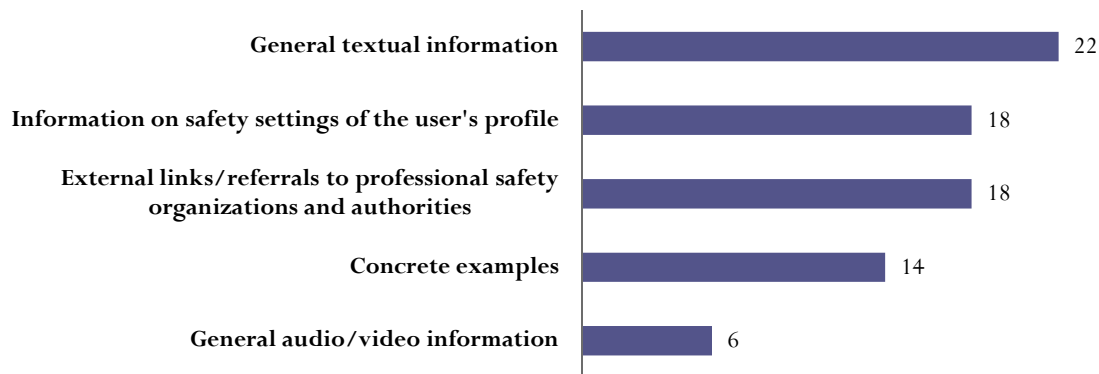


Figure 8. Format of safety information provided on the SNS sites

As shown in the figure above, the format of the information varies, with general textual information being the most common (22 services). The least common is general audio/video information (found on six services). External links/referrals to professional safety organizations and authorities were found on 18 of the 25 services.

Is information presented in a prominent and accessible format?

Looking at those types of information that was very easily or easily found on the services (figure 9 below), it is clear that terms of use/service and information on privacy is the most easily found. However, on one service, the terms of service/use was difficult to find, and on three services, the terms of use could not be found at all.

Even after extensive searching the expert testers were not able to find information on terms of use/services for three services. This is considered a surprising result, as the terms of use/service can be regarded as the core regulatory tool between the service and its customers/users, and its content is vital for the user to understand in order to be able to make informed decisions about their relationship with the site.

Information for parents and carers was easily found on 14 services and safety tips/information of children was easily found on nine services. For teachers information could only be found easily on four services. On five services information directed towards teachers was not seen as applicable to the service, on one service the information was found after considerable searching, whereas on 15 services the information for teachers could not be found at all.

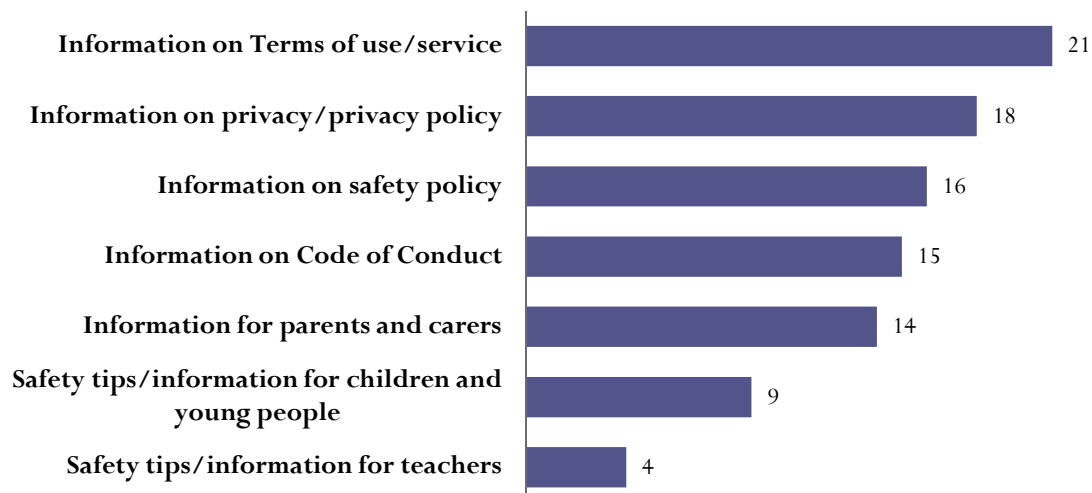


Figure 9. Types of information that are easily found for users before signing up

The final recommendations in the signed agreement are that providers should offer parents targeted links, educational materials and other technical controls as appropriate with the aim of fostering dialogue, trust and involvement between parents and children about responsible and safer internet use and they should also ensure that this material can empower teachers so they can help children use SNSs safely and responsibly. Half of the SNSs (12) stated in their self-declaration that they have such information available. Of these, information could be found very easily or easily on nine services, and could not be found at all on two services. Of the 12 SNSs that did not state that they had such information available, it was still found on seven of the sites (of which two had information very easily accessible).

In addition, 18 signatories were found to have links and/or referrals to external safety organizations and authorities (such as Insafe, national hotlines, police, health authorities etc.).

Do providers have clear safety information for children and teens?

Testing if information that was targeted towards children and teens was easy to understand⁵ revealed that while most services will provide information that is assessed as easy to understand or sufficient, four services with information directed towards children and five services with information directed towards teens had information that was partly difficult to understand. One service was considered as having information that could not be understood by children, and one service was considered as having information that could not be understood by teens.

⁵ It should be noted that the large number of “not applicable services” is due to age restrictions on the sites; hence information for younger children is not relevant for sites where only teens are allowed.

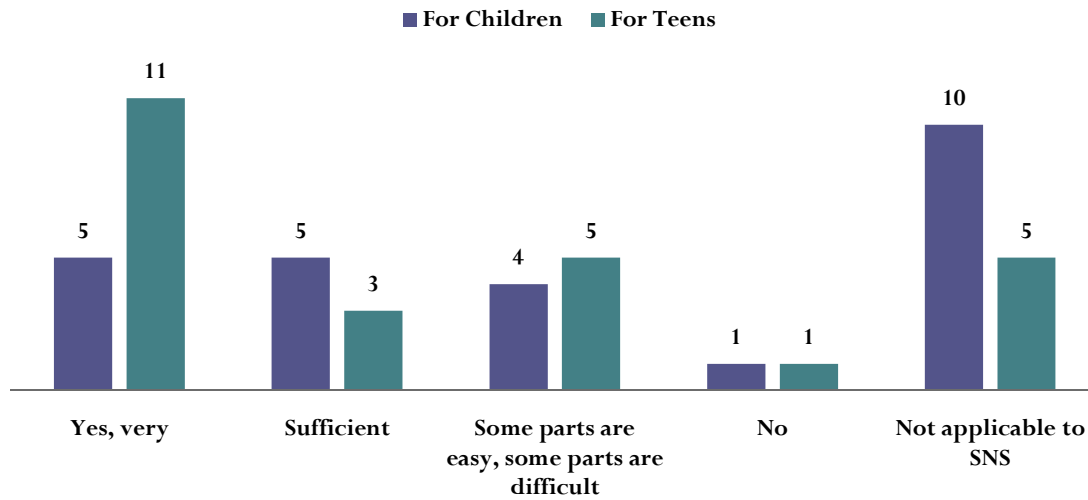


Figure 10. *Is information targeted towards children and teens easy to understand?*

It should also be noted that while almost half of the SNSs (12) in their self-declaration reported having information specifically targeted towards children; only eight of them were assessed as having information that is very easy or sufficiently easy to understand by children. Out of the 15 services who reported in their self-declaration that they had such information for teens, ten were found to have information that is very easy or sufficiently easy to understand.

Is it made clear to users what constitutes inappropriate behavior?

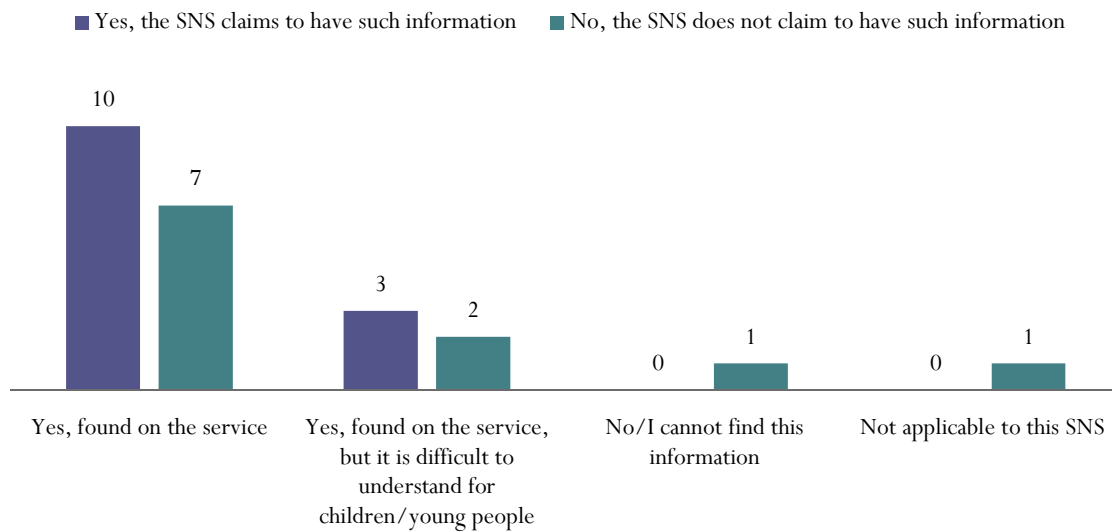


Figure 11. *Information on and consequences of engagement in prohibited behaviors/actions are clearly stated for users*

All but one service⁶ was found to have information on content and conduct that is not allowed on the service. However, on five of these services the information was assessed as being difficult to understand for children and young people.

Is safety information on specific risks provided?

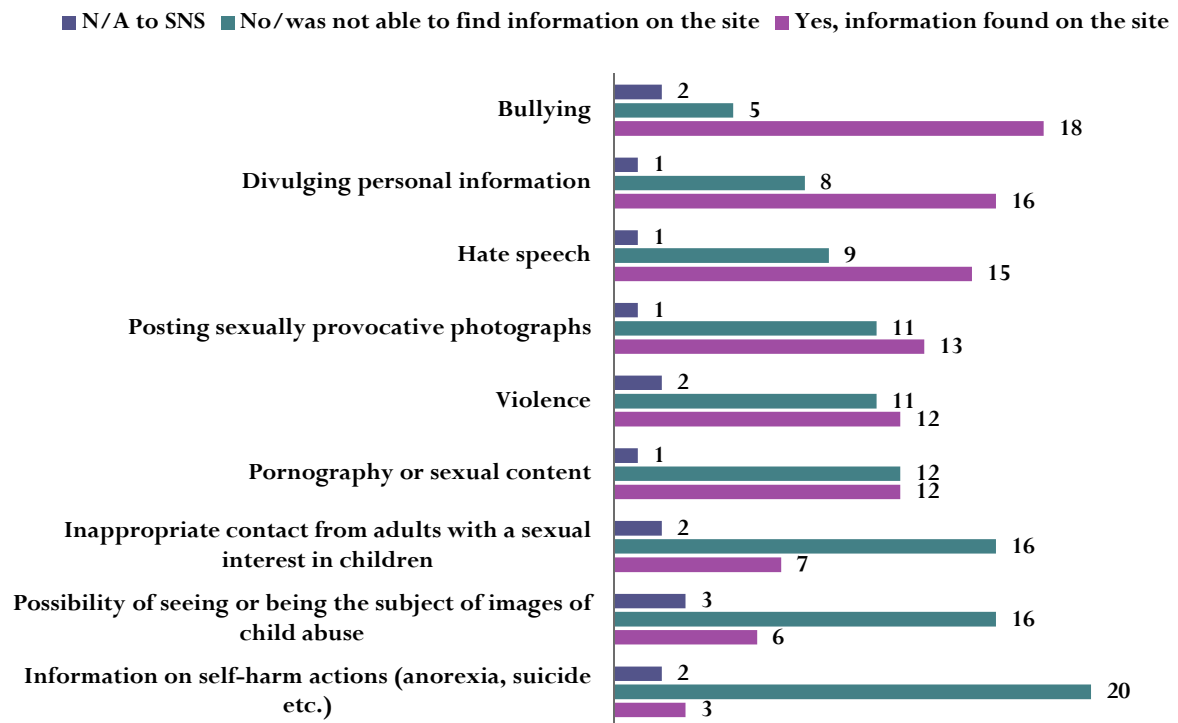


Figure 12. Frequency of safety information found on specific risks by number of SNSs

The information on specific risk that is most often found on services includes information on online bullying, hate speech, and risks of divulging personal information, followed by information on the risk of posting sexually provocative photographs.

Out of all the 25 tested services, very few had information on the risks of inappropriate contact from adults with a sexual interest in children (seven services), the possibility of seeing or being the subject of images of child abuse (six services) or information on self-harm actions (three services).

⁶ Excluded here is one service where such information was assessed to be not-applicable to the type of service.

Example of best practice under Principle 1:

A best practice example of providing easy access to all the different types of information (terms of use, privacy policy, safety policy, etc.) is Youtube.

Safety tips and information for children and/or young people that are both easily accessed and is easy to understand was found at Habbo Hotel, Hyves, MySpace, nasza-klasa, netlog, one.It, rate.ee, SchulerVZ, Skyrock, IRC galleria, , Yahoo! Answers, Yahoo! Flickr, YouTube and Zap.

Evaluation of Principle 2 – “Age appropriate services”

Principle 2 states that Social Networks should “*work towards ensuring that services are age-appropriate for the intended audience*”. In order to assess the implementation of such services, a differentiation has been made between 1) restrictions meant to ensure that those below the intended minimum age of the service cannot register (sign-up restrictions), and 2) restrictions aimed at ensuring age appropriate services when the user is already registered and a member of a social networking site.

For the services included in this evaluation, the figure below shows the distribution of age-requirements for users that want to sign up to the services.⁷



Figure 13. Overview of minimum age for registration

A positive result is that most services have clear and transparent age requirements for users. Three services were found to have age requirements that were difficult to understand for children. On one site the information could not be found at all.

A variety of techniques are used, often in combination, to prevent younger users from participating in the social network, or to ensure that the functionality available in the service (ref. principle 3) will be set up according to their age.

⁷ Please note that these requirements are on the basis of the information found on the sites and in the self-declaration of the services, and do not necessarily reflect the actual ability to sign up. Also, parental approval must be given for users under a certain age on some services that do not have a specific age limit.

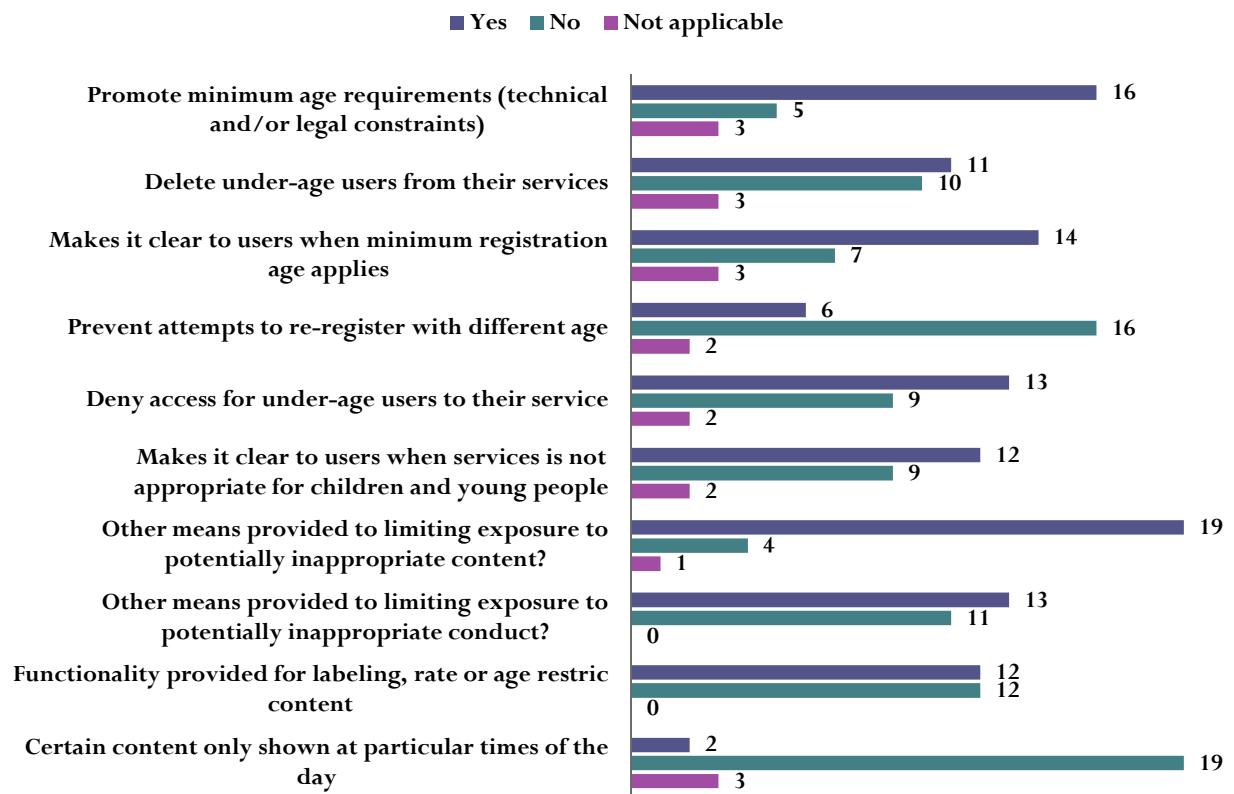


Figure 14. *Restrictions aimed at ensuring age appropriate services for users according to self-declarations*

Among restrictions aimed at ensuring age appropriate services for users, providing various means to limit exposure to potentially innappropriate content is the most often implemented (18 services use it), followed by promoting technical and legal constraints to assure minimum age requirement.

Only seven services stated in their self-declaration that they promote parental control tools on their service. The testing of these services revealed that the parental control tools could easily be found on three of the services, not easily found on two services and not found at all on two services. Out of the three services where the information was found easily, it was also considered to be efficient.

Can 11-year olds have access to a restricted site?

When testing this principle several profiles were used or attempted to be used: an 11-year old girl, and 15-year old girl as well as an adult.

All services tested used/asked for birthday data at the registration process. On four services the user had to state that they were above a certain age (e.g. by ticking a box), while e-mail verification/address for e-mail verification was required by 20 services. Out of those 20 services, the testers were able to sign up without verifying over e-mail on seven of them.

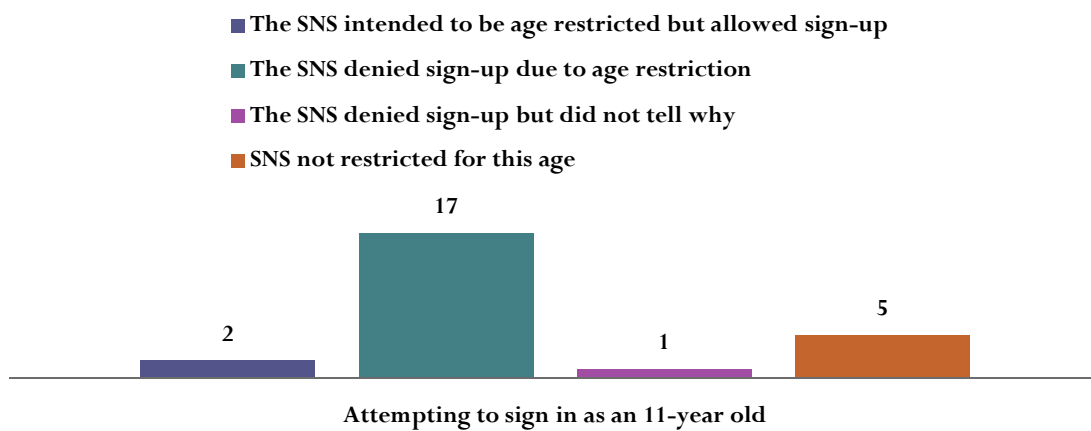


Figure 15. Attempts to sign up to age restricted sites

On three services intended to be age-restricted for 11 year olds, sign-up was not allowed. 17 services denied sign-up explicitly referring to the age restrictions on the site.

Can an 11-year old get access to a restricted site by changing her age?

For services that restricted signing up, another attempt was made, with the same profile, but with a different birth-date pretending to be a 15-year old girl. On seven services the changing the date of birth/age was enough to grant access. On two additional services this could be done after a cookie was removed. All testers were later able to sign up with a new profile as an older user adhering to the age-requirements of the service on the same computer/device.

Example of best practice for Principle 2:

Best practice examples of SNS who state that they take steps to deny access for under-ages users and are actually denying the access to those under-aged on the site are ARTO, Bebo, Facebook, Microsoft XBOX Live, MySpace, SchulerVZ, SkyRock, Tuenti, Yahoo! Answers and Yahoo! Flickr.

Evaluation of Principle 3 – “Empower users”

The third principle “*Empower users through tools and technology*” covers the tools and technologies employed to assist users – children and young people – in managing their experience of the service. Recommendations for such tools according to the “Safer Internet Principles for the EU” (2009: 7-8) are:

- Make private profiles for users below 18 not searchable
- Set private profiles for users below 18 to private by default
- Make private profiles viewable only to “friends”/people on the user’s contact list
- Give users control over who can access their full profile
- Give users control over who can post comments and content on their profile and the possibility to delete messages and other content
- Give users the option to pre-moderate comments from other users before they are published on their profile
- Provide easy-to-use tools for reporting inappropriate contact or content from other users⁸
- Educate parents about available tools.

Are profiles of underage users set to private by default?

Statements that profiles were set to private by default for users below 18 years were given by 14 SNSs in their self-declarations. After testing, this was found to be true in only seven of the cases. It is also interesting to note that of the SNSs that did not give such claim in their self-declaration report, the test revealed that six additional SNSs had such a mechanism on their site.

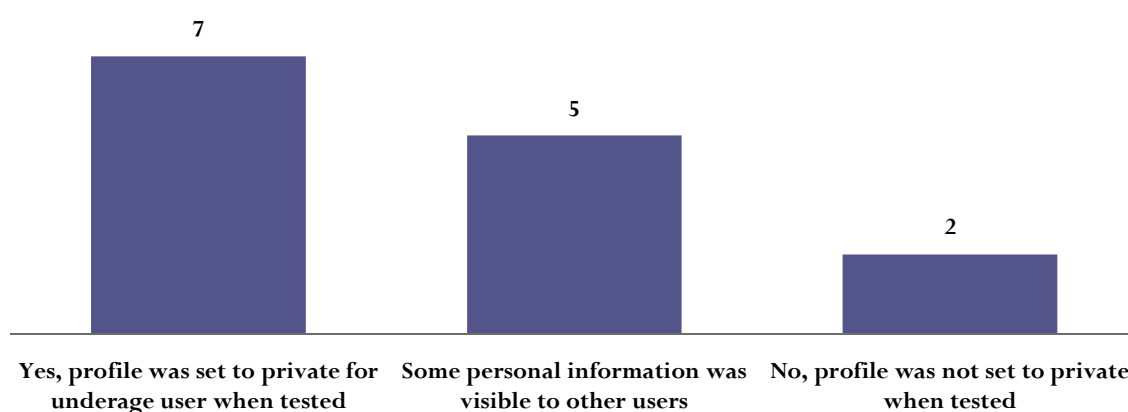


Figure 16. *Testing if users have to change settings for personal information to be visible to other users on SNSs stating in their self-declarations that profiles for under-aged users are set to private by default*

⁸ For elaboration on the implementation of this point, please refer to Principle no.4 and Principle no.5.

Are private profiles of users below 18 searchable?

As part of the testing, all testers created several profiles on the service, both as underage users, and as adults. To test if private profiles of users were searchable, the testers used their adult testing profile to search for (one of their) child profiles.

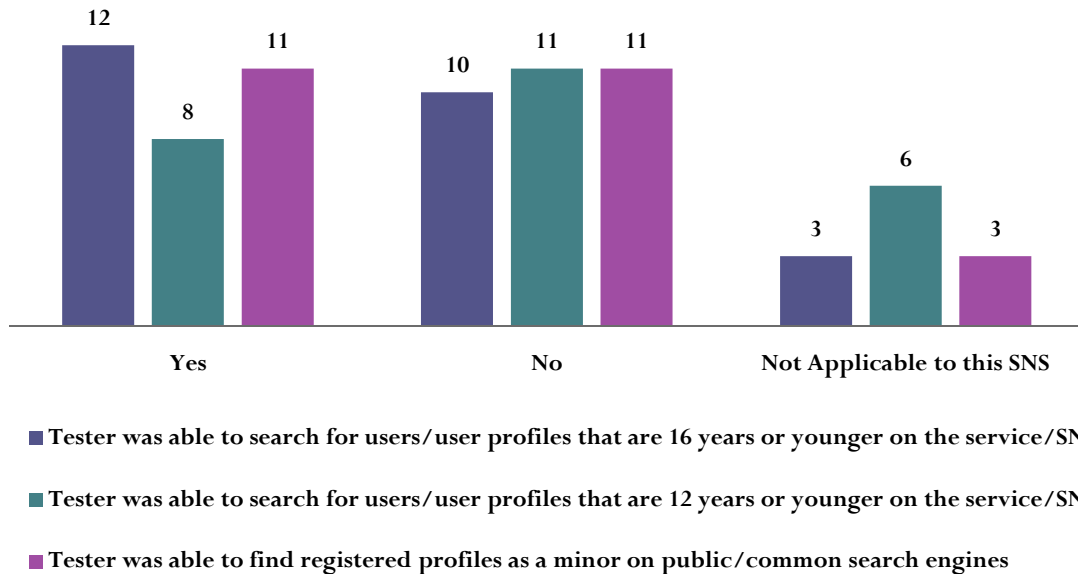


Figure 17. Testing results when searching for profiles of under-aged users

Profiles of the youngest children (12 years or younger) were found on eight services, while profiles for users 16 years or younger were found on 12 services. In addition 11 services allowed the profiles of underage users (11 and/or 15 year olds) to be available through common search engine(s).

Who can post comments on a user's profile?

The figure below shows that on 11 services only the user's friends can post comments on their profiles while in 12 cases all users can post comments. Further, only one service requires the approval of comments by friends before being published and two services enable that for the comments from all users.

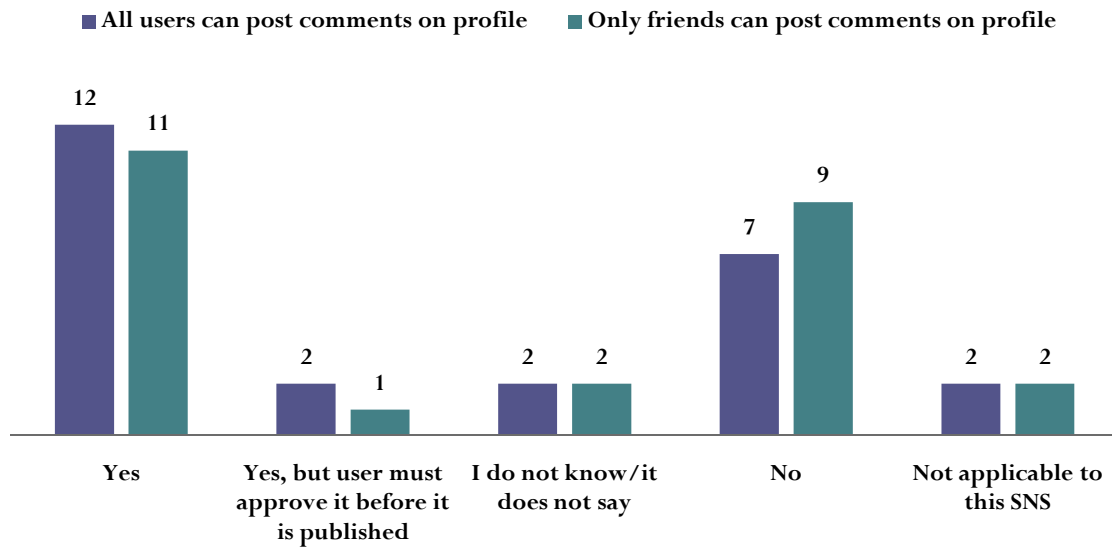


Figure 18. Who can post comments on user's profile?

If we compare the ability to post comments with the visibility of information (below) we see that the ability for other users to post comments on the profiles of underage users are linked to the profile status of the latter. Users whose profiles are set to strictly private are more likely to have only friends being able to post comments (7 of 10 services).

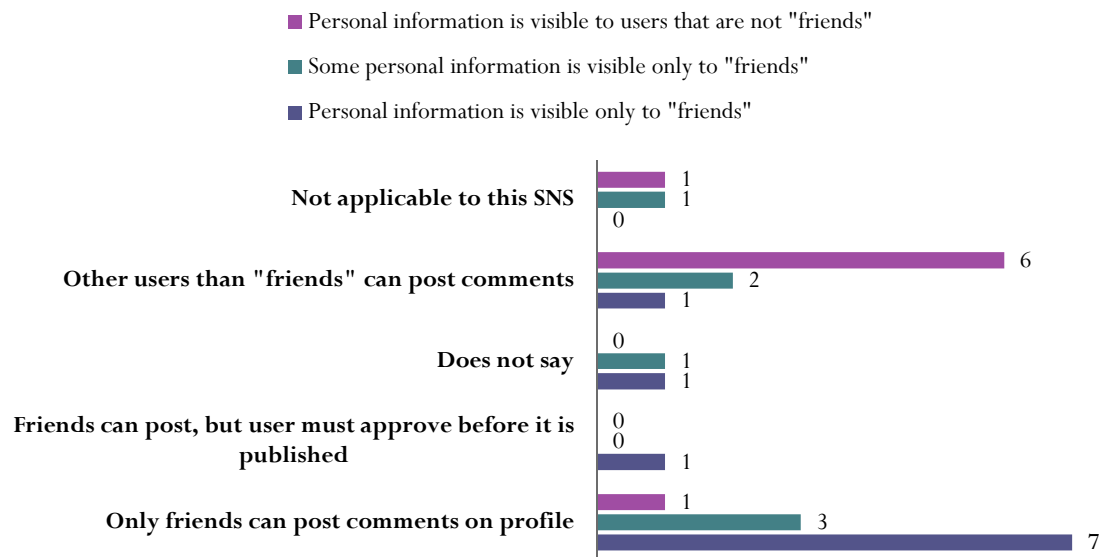


Figure 19. Who can post comments on profiles of under-aged users by their privacy settings

For one service other users can post comments on your profile, even if only your friends can see your personal information. Vice-versa, on one service only friends can post comments, but personal information is visible to all users.

Can users control who can access their full profile?

On 24 services the testers were able to block a friend and on 21 services a friend request could be rejected, while on two services (both stating in their self-declaration that the user would have control over who could access their full profile) this could not be confirmed.

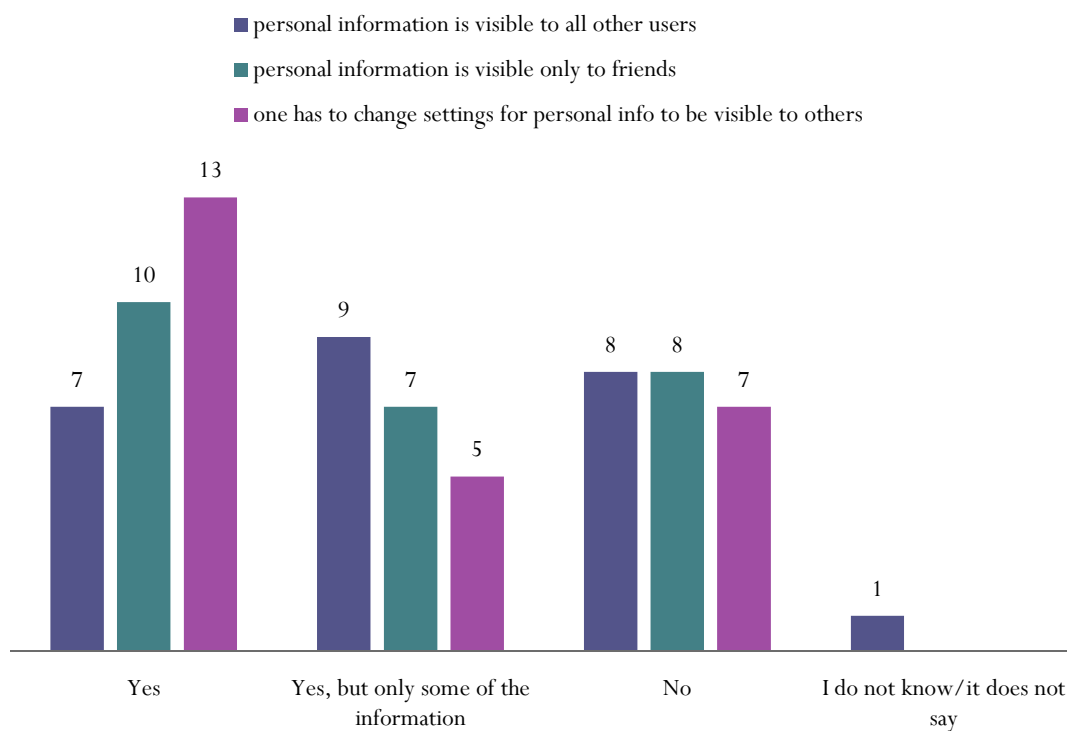


Figure 20. *Visibility of personal information on the service*

The above figure shows that on a total of 17 services the user's personal information (some or all) is visible only to their friends. Ten out of these 17 services enable the user's full information to be private and only visible to their friends.

Can users remove content from their own profile?

Users can delete/remove *postings* on their own profile on 22 services, while 18 services allows for users to delete/remove *pictures* on their profile.

In addition, nine services notify the user when they are identified (tagged) in pictures posted on other people's profiles, but no one has the option of allowing the user to approve the photo before it is published. On eight services, information about tagging could not be found.

Example of best practice for Principle 3:

Best practice examples of SNS where users' personal information is visible only to their friends are Facebook, Giovanni, MySpace, One.It, SchulerVZ, Habbo, Tuenti, Windows Live, Yahoo! Answers and Yahoo! Flickr.

Evaluation of Principle 4 – “Easy-to-use mechanisms for reporting violations”

In order to comply with principle 4 “Provide easy-to-use mechanisms to report conduct or content that violates the terms of service”:

- Providers should provide a mechanism for reporting inappropriate content, contact or behavior as outlined in their Terms of Service, acceptable use policy and/or community guidelines. These mechanisms should be easily accessible to users at all times and the procedure should be easily understandable and age-appropriate.
- Reports should be acknowledged and acted upon expeditiously.
- Users should be provided with the information they need to make an effective report and, where appropriate, an indication of how reports are typically handled.

In order to test principle 4, the social networking sites were sent the following message from the expert testers on their service(s) if at all possible⁹:

**“I am writing to you because someone is sending me scary messages.
What should I do about this? Please help me.”**

This message was carefully designed and worded to be a general request, and would in most cases be sent from the profile of a registered, underage user of the site (in most cases an 11 year old, in a few cases a 15 year old, pending on the overall age restriction of the SNS site). In this message, the SNS is asked to give specific advice on how the user themselves should handle this. The message does not mention the SNS in particular. It is also a general cry for help. On a few services it was not possible to send a general request, asking for help, but rather requests pre-defined by the SNS. In these cases the tester was asked to send the pre-defined report that resembled the original message the most.

As the signatories are very diverse in the services they provide, this message might not be fully relevant to all the 20 social networking sites that have committed to the principles. However, it is deemed that an underage user asking for advice and help from a professional party should receive some sort of feedback, preferably with information relevant to the request sent. The way the message is worded should also prompt a personal response.

Are reporting mechanisms easy to understand?

All services had some type of reporting mechanism available. A majority of them (19 services) were found to have a link/information available all the time on where to report content that bothered the user and/or was a violation of terms. Similarly, 18 services were found to have information available all the time on

⁹ Two services (Microsoft Xbox Live and Yahoo Flickr) could not be tested for technical as well as ethical reasons. Please refer to the individual testing reports of these services for more information. In addition the testing of StudiVZ/MeinzVZ was tested and reported as one service.

where to report other users that bothered them/violated the terms, while on four services such information was found only after considerable searching.

The reporting mechanism on 15 of the services were considered to be easy to understand for children and young people, while eight were considered not to be.

Are reports acknowledged?

Of a total of 24 services with a self-declaration report, less than half (10) stated that reports from users were acknowledged to the user. During the testing, such acknowledgement could only be confirmed among seven of these signatories, while three did not give any feedback to the tester. Among the 13 services that did not give information on acknowledgement of reports from users, six did send such information. In sum 14 services complied with the recommendation, including one service originally assessed as “not applicable” to the recommendation.

Are reports acted upon expeditiously?

Figure 21 below gives an overview of the response time of the SNSs. Only relevant feedback is listed as a response, hence automatic responses only stating that the message has been received and will be reviewed are not deemed sufficient to be listed as a full “reply”.

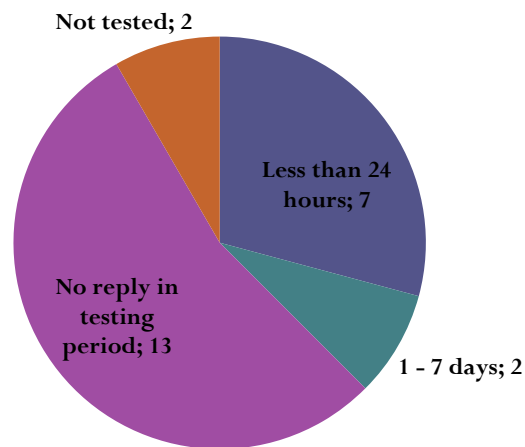


Figure 21. *Response time to users asking the social networking services for help*

Of a total of 22¹⁰ services tested, 13 did not give any reply to the message asking for help in the testing period, two replied within a week (3-4 days), while seven¹¹ replied within 24 hours.

¹⁰ Two services (Microsoft Xbox and Yahoo Flickr) were not tested for both practical and ethical reasons. Two services (StudiVZ and MeinzVZ) were tested together and reported as one, bringing the total number of services to 25.

¹¹ In one of these cases the reply did not reach the tester, but after consulting with the SNS it is clear that a reply was sent.

Example of best practice under Principle 4:

Best practice of SNSs that provide easy to understand report mechanisms and send acknowledgement after reports are ARTO, Bebo, Dailymotion, Facebook, Giovani.it, Hyves, MySpace, Nasza-Klasa.pl, Netlog, Piczo, Rate, SkyRock and Yahoo! Answers.

Best practice examples of SNSs that replied to the request from an underage user asking for help are Arto, Dailymotion, Hyves, Microsoft Windows Live, Myspace, rate.ee, Sulake (Habbo and IRC- Galleria), and Google (YouTube).

Evaluation of Principle 5 – “Respond to notifications of illegal content/conduct”

Principle 5 states that Social Networking Services should “*Respond to notifications of illegal content or conduct*”. While efficient processes for handling such notifications should be in place, it is clear that as the nature of the services, national legislation and often unclear jurisdiction varies, only a very overall picture can be presented.

Reviewing *the self-declarations* it is clear that most services (22 of 24 services with a self-declaration report) state that they share reports of illegal content or conduct with relevant law enforcement bodies and/or hotlines. In addition, 19 explicitly state that they have effective processes for reviewing and removing illegal content or conduct. Finally, 16 of them state that they feature links to relevant local agencies or organizations. The SNSs RATE, ARTO, Facebook, MySpace, SchulerVZ, StudiVZ, MeniVZ, Habbo, IRC Galleria, Piczo, One.lt, Hyves, Netlog, Yahoo! Flickr and Youtube all state to have implemented all these measures.

For ethical and practical reasons responses to reports of *illegal* content and conduct could not be directly tested in this evaluation.

Evaluation of Principle 6 – “Encourage a safe use approach to privacy”

Principle 6 requires that the Social Networks “Enable and encourage users to employ a safe approach to personal information and privacy”. Specifically providers should

- provide a range of privacy setting options and information easily accessible for the user
- consider the implications of automatically mapping information provided during registration onto profiles, make users aware when this happens, and should consider allowing them to edit and make public/private that information where appropriate.
- give users the ability to view their privacy status or settings at any given time

On more than half of the services (14) the testing found that the user had control over the display of their online status (if other people could see if they were online), while five services did not provide this option to the user. On five additional services the testing could not assess if this feature existed, while one was deemed “not applicable”.

What personal information is typically asked for when creating a profile?

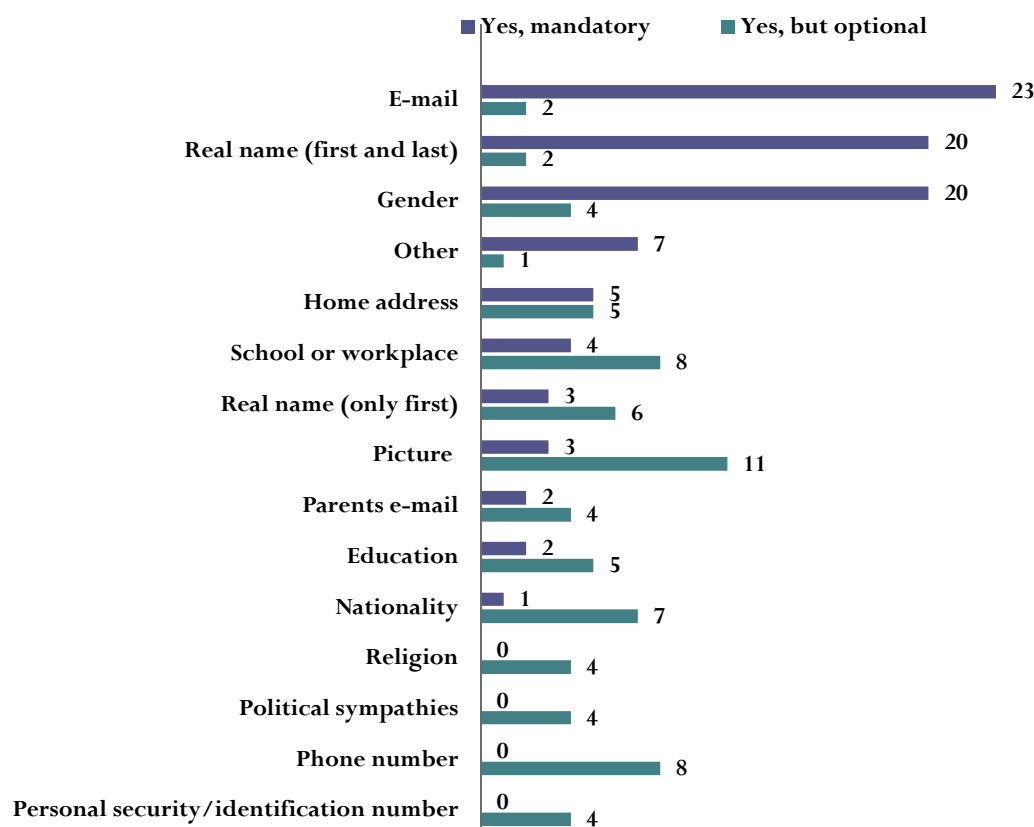


Figure 22. Personal information asked for when creating a profile by number of SNSs

As indicated in the above figure, the most frequently asked for personal information during the creation of a new account are email address, real name and gender.

Four services allow users to submit their personal security/identification number and ask for their political sympathies and religious affiliation

What personal information is automatically inserted into a profile

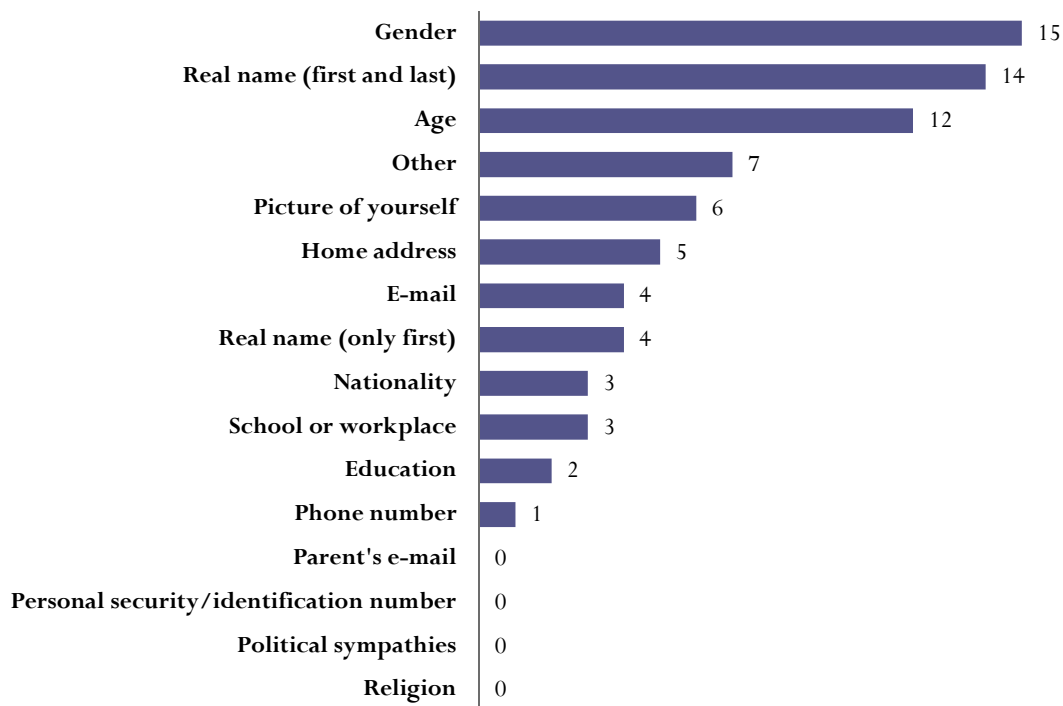


Figure 23. Personal information automatically displayed in profile

The most frequently automatically inserted personal information is gender and real name (both first and last) followed by age. Profile pictures are automatically uploaded on every fourth service. One service automatically displays the user's phone number.

Is it easy to change privacy settings?

Testers found that privacy settings could be easily changed on all services except one.

Further, assessing whether providers had privacy options supported by information that encourage users to make informed decisions about the information they post online, the testers checked if they got safety

tips/and or information about publishing personal information when they were about to publish information on their profile. In the self-declarations, 11 providers stated having such information, while this could only be confirmed for six of the services when it come to textual information and confirmed for seven services when trying to upload a photo on ones profile. In addition such information was found on two services for textual information and five services for photo – that had not mentioned this in their self-declaration report.

How easy is it to delete the profile?

In addition to the privacy settings recommended in the Principles, a special test was done to assess how easy it was to find information on how to delete one’s profile and what would happen to your personal information should you do so.

It should be emphasized that as this is not a specific situation addressed by the industry in the Principles, none of the signatories had elaborated on such practices in their self-declaration.

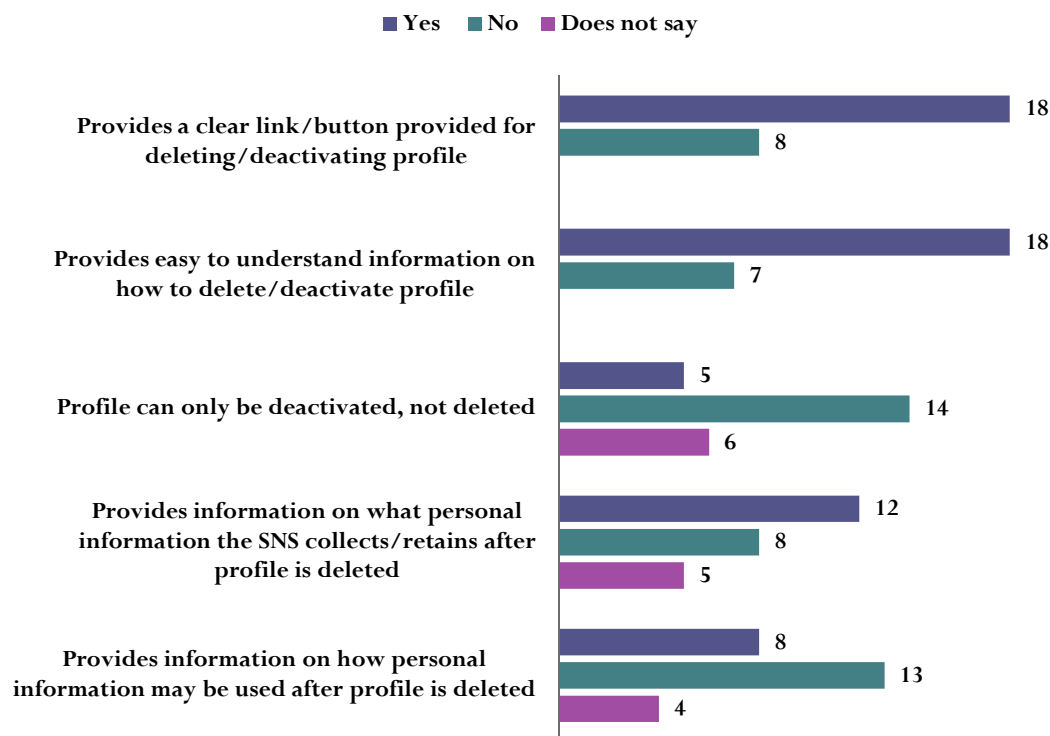


Figure 24. Available information on deleting or deactivating profiles on the SNS services

The above figure shows that a majority of services provided a clear link/button for deleting/deactivating the account as well as easy to understand information on how to delete/deactivate one’s profile.

At the same time five services do not allow for profiles to be completely deleted and on six services this information could not be found. There is also a lack of information on what personal information the SNS collects and/or retains after a profile is deleted (could not be found on 13 services) and how this personal information may be used (could not be found on 17 services).

Best practice example for Principle 6:

Best practice examples of SNS that provide safety tips and/or guidance to users before they publishing personal information and when they are about to upload a photo on their profile are Bebo, MySpace, Habbo and IRC Galleria.

Evaluation of Principle 7 – “Reviewing illegal or prohibited content/conduct”

The last principle pertains to the reviewing of illegal or prohibited material on the sites. According to the signed principles the SNS providers should “during the normal course of developing and managing SNSs, assess their service to identify potential risks to children and young people in order to determine appropriate procedures for reviewing reports of images, videos and text that may contain illegal and inappropriate/unacceptable/prohibited content and/or conduct”. Listed examples of such procedures are (“Safer Social Networking Principles of the EU,” 2009: 9):

- human and/or automated forms of moderation
- technical tools (e.g. filters) to flag potentially illegal or prohibited content
- community alerts
- user-generated reports

In addition attention and warning is given to the risk of employing or using human moderators who are unsuitable for working with children or young people.

As with Principle 5, for ethical and practical reasons Principle 7 could not be tested in this evaluation. However, analyses were made of the self-declarations submitted, giving indication to the various approaches taken by the different SNSs that have signed up to the principles.

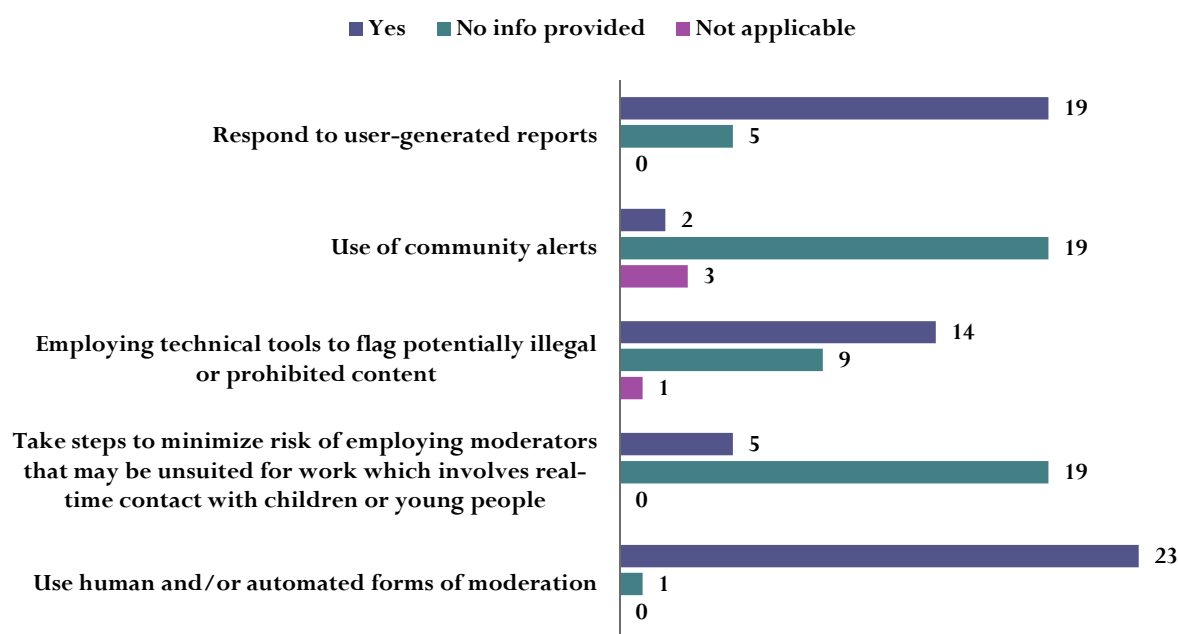


Figure 25. Reported steps taken by SNSs to “review illegal/prohibited content”

The figure above shows that according to the SNS’s own self-declarations the most frequently employed step in reviewing illegal/prohibited content is the use of human and/or automated forms of moderation.

References:

European Commission. (2009). Safer social networking: the choice of self-regulation. Retrieved 20.08.09, 2009, from

http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm#self_decl

Safer Social Networking Principles of the EU. (2009, February 10th). Retrieved 20.08, 2009, from

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

Annex 1. Background and objectives for the testing



EUROPEAN COMMISSION
Information Society and Media Directorate-General
Digital Content and Cognitive Systems
eContent and Safer Internet

Luxembourg, 08-10-2009
INFSO/E6/AR/sp D(2009) 142813

Note to the experts

Subject: Assessment of the implementation of the Safer Social Networking Principles for the EU

(1) Background

In 2008, the European Commission convened a Social Networking Task Force, bringing together major SNS providers on the European market for under 18s, as well as organizations involved in child welfare and researchers. The objective was to consider the signature of a charter of guidelines by SNS providers, meant to ensure children's and young people online safety. The Commission acted as a facilitator and contributed to gather input from a wider range of organisations through a public consultation run in summer 2008.

In February 2009, after several meetings of the Social Networking Task Force, the Commission brokered an agreement, the "Safer Social Networking Principles for the EU", which has been signed by 20 of the most popular social networking companies on the European market.

This is a self-regulatory document, which outlines the principles by which SNS providers should be guided as they seek to help minimise potential harm to children and young people, and recommends a range of good practice approaches, which can help achieve these principles

The full text of the "Safer Social Networking Principles for the EU" is available online at http://ec.europa.eu/information_society/activities/social_networking/index_en.htm

As part of their commitment to implement the Principles, the signatories to the "Safer Social Networking Principles for the EU" undertook to provide to the European Commission a self-declaration on how they have considered the Principles in relation to the social networking services they offer, using a template that is annexed to the final version of the Principles.

Self-declarations are available online at:

http://ec.europa.eu/information_society/activities/social_networking/index_en.htm

Monitoring is important for the credibility of the exercise and for the common goal of child safety online. At the signature of the SNS Principles on 10 February 2009, Mrs Reding, the European Commissioner for Information Society and Media, said:

"The European Commission intends to monitor what we hope and expect will be continuing progress in the development of safety measures, as well as efforts to implement these measures effectively and in a transparent way. We will come back to this agreement and evaluate the progress made in a year's time."

The results of this assessment of the progress will be presented on Safer Internet Day, 9 February 2010.

(2) Objectives of the assessment

The objectives of this process are:

- To assess the compliance of the companies' policies with the Principles, checking the extent to which actions mentioned in the self-declaration are in line with the Principles, and to what extent they are implemented;
- To assess the effectiveness of the self-regulatory agreement in ensuring that SNS can be used safely by minors.

(3) Process

In order to assess the implementation of the agreement, the Commission services have decided to draw up a report with the assistance of independent experts. Two lead experts were hired to draw up a methodology, and a final report. 13 other experts assisted them. All experts have previous experience in the field of Internet/new technologies usage by children and young people.

The European Commission requested the lead experts to draw up a methodology based on 2 steps: first, the analysis of the self-declarations provided by the signatories and second, testing from the users' perspective in the main language of each service. Signatories to the Principles provide different types of services to their users (e.g. video sharing platforms, virtual worlds, online gaming). Therefore, the experts have been requested to ensure that the testing methodology takes account of the type of service, in the light of information provided in the self-declarations.

This methodology has been submitted to the Social Networking Task Force for its comments and approved by the European Commission.



Richard Swetenham
Head of Unit

Annex 2. Safer Social Networking Principles¹²

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

Providers should create clear, targeted guidance and educational materials designed to give children and young people the tools, knowledge and skills to navigate their services safely.

These messages should be presented in a prominent, accessible, easy-to-understand and practical format (e.g. on a help pages and/or in locations where the user makes a decision about how to use the service).

Service providers should provide clear information about what constitutes inappropriate behaviour. This information should be easily accessible and include information about the consequences of breaching these terms. Providers should explore other ways to communicate this information outside of the Terms and Conditions.

Parents play a crucial role in their child's internet safety and this role is often best fulfilled when a parent is able to discuss safety issues with their child in an open and informed way. As such, providers should offer parents targeted links, educational materials and other technical controls as appropriate with the aim of fostering dialogue, trust and involvement between parents and children about responsible and safer internet use.

Teachers and other carers also play a crucial role in promoting the safe use of SNSs by children and SNS providers should ensure that such materials also empower teachers to help children use SNSs safely and responsibly.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience¹³

Providers should, in the normal course of developing and managing SNSs, consider how their service may be associated with potential risks to children and young people, where it is intended for them to use the service^{14 15}. Service providers should seek to limit exposure to potentially inappropriate content and

¹² This Annex lists the Principles. For the full text of the agreement, including background information, please refer to http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf.

¹³ The intended audience as outlined in each providers' Terms of Service

¹⁴ The intended audience as outlined in each providers' Terms of Service

contact. Measures that are available or appropriate to each service will vary in each case¹⁶, but may include for example:

- making clear when services are not appropriate for children and young people or where a minimum registration age applies;
- taking steps to identify and delete under-age users from their services;
- taking steps to prevent users from attempting to re-register with a different age if they have previously been rejected for being below the minimum age (if their terms require a minimum age), such as employing cookies;
- working within technical and legal constraints to promote compliance with minimum age requirements;
- promoting the uptake of parental controls which allow parents to manage their children's use of the service;
- providing means for content providers, partners or users to label, rate or age restrict content where appropriate¹⁷;
- only showing certain professionally produced content certain times of the day.

Principle 3: Empower users through tools and technology

Providers should employ tools and technologies to assist children and young people in managing their experience on their service, particularly with regards to inappropriate or unwanted (but not illegal) content or conduct. Service providers should make an assessment of what measures to implement based on the services being offered and the intended audience.

The measures that can help minimise the risk of unwanted or inappropriate contact between children and young people and adults may include for example:

- taking steps to ensure that private profiles of users registered as under the age of 18¹⁸ are not searchable (unless the user actively consents for their profile to be searchable), either on the service or via search engines;

¹⁵Each SNS is different in terms of target audience, the range of activities users can engage in, the platforms on which they can be consumed and the countries in which they are available. These factors will affect the range and extent of the risks that may affect children and young people when using the site. Assessments of what constitutes inappropriate content for children and young people also varies.

¹⁶The same combination of factors as listed in the previous footnote will determine what measures are appropriate to address the unique set of challenges and potential risks to users on a particular service. In addition, service providers may also be required to comply with specific local legal requirements pertaining to children's privacy, which may affect how the service is operated in any given jurisdiction. For example, it is common for US-based service providers to adopt a minimum age of 13 years for their services. This reflects the requirements of the Children's Online Privacy Protection Act (COPPA), which only allows providers to collect data without parental consent from users over 13 years old. In the absence of specific local legal requirements, however, service providers will adopt a default specification for their product which is determined by a range of factors such as company policy, adherence to industry good practice or the prevailing law in their principle market.

¹⁷ For example, the Broadband Stakeholder Group's good practice principles on audiovisual content information. See <http://www.audiovisualcontent.org/>

- setting the default for full profiles to 'private' or to the user's approved contact list for those registering under the age of 18¹⁹ (some service providers set the profile default as 'private' for all users);
- 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 (users may actively choose to change their settings to public or equivalent);
- giving users control over who can access their full profile by, for example, being able to block a user from viewing their profile and 'reject' friend requests;
- giving users the option to allow only direct friends to post comments and content to their profile or to delete unwanted comments;
- giving users the option to pre-moderate comments of other users before being published on their profile;
- providing easy-to-use tools for users to report inappropriate contact from or conduct by another user;
- educating parents about available tools, both for wider internet access (for example, the benefits of using filtering tools and/or parental controls²⁰) and the tools, information and advice provided to parents by social networking sites to help them protect young people.

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

Providers should provide a mechanism for reporting inappropriate content, contact or behaviour as outlined in their Terms of Service, acceptable use policy and/or community guidelines. These mechanisms should be easily accessible to users at all times and the procedure should be easily understandable and age-appropriate.

Reports should be acknowledged and acted upon expeditiously.

Users should be provided with the information they need to make an effective report and, where appropriate, an indication of how reports are typically handled.

¹⁸ The 18+ age requirements may be difficult for services that have already been developed around the legal age of consent, e.g. 16 years. However, future services should consider using 18 years.

¹⁹ The 18+ age requirements may be difficult for services that have already been developed around the legal age of consent, e.g. 16 years. However, future services should consider using 18 years

²⁰ See some of the solutions at "Study on Safer Internet Programme BENCHMARKING of Filtering software and services" at <http://www.sip-bench.eu/index.html>

Principle 5: Respond to notifications of Illegal content or conduct

Upon receipt of notification of alleged illegal content or conduct²¹ providers should have effective processes in place to expeditiously review and remove offending content.

Service providers should have in place arrangements to share reports of illegal content or conduct with the relevant law enforcement bodies and/or hotlines. These arrangements will depend on local jurisdiction and applicable law, as well as the existence of effective reporting frameworks.

Providers may consider including links to other local agencies or organisations, for example the relevant InHope services and law enforcement agencies. Where there is an immediate threat to safety or life, users should be advised to contact the emergency services by, for example, phoning 999 (UK) or 112 (EU).

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

Providers should provide a range of privacy setting options with supporting information that encourages users to make informed decisions about the information they post online. These options should be prominent in the user experience and accessible at all times²².

Providers should consider the implications of automatically mapping information provided during registration onto profiles, make users aware when this happens, and should consider allowing them to edit and make public/private that information where appropriate.

Users should be able to view their privacy status or settings at any given time. Where possible, the user's privacy settings should be visible at all times.

²¹ In the context of child protection, illegal content and conduct in this context refers to child abuse images and grooming respectively.

²² Social networks are used for myriad purposes and by a wide range of users. Different services have different profile formats which allow users to share different information about themselves, for example some providers encourage users to create nicknames and post avatars and create a novel online identity. These formats vary between sites.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct²³

SNS providers should, during the normal course of developing and managing SNSs, assess their service to identify potential risks to children and young people in order to determine appropriate procedures for reviewing reports that images, video and text may contain illegal and inappropriate/unacceptable/forbidden content and/or conduct.

There is a range of procedures which can be used to promote compliance with the Terms of Use, Acceptable Use Policy and/or House Rules. These may include for example:

- human and/or automated forms of moderation;
- technical tools (e.g. filters) to flag potentially illegal or prohibited content;
- community alerts;
- user-generated reports.

Some providers employ human moderators who interact in real-time with children or young people. Such providers should take reasonable steps (working within good practice frameworks²⁴ where possible or legal frameworks as applicable), to minimise the risk of employing candidates who may be unsuitable for work which involves real-time contact with children or young people.

²³ Prohibited content/conduct as defined by Terms of Use, Acceptable Use Policy and/or House Rules

²⁴ Home Office Internet Task Force Good Practice Guidance for the Moderation of Interactive Services for Children
<http://police.homeoffice.gov.uk/publications/operational-policing/moderation-document-final.pdf>

Annex 3. Testing Questionnaire

Name of SNS being reviewed						
URL of SNS						
Date of testing						
Name of tester						
Nicknames to be used for testing (please list all)						
Contact e-mail for tester						
Contact phone for tester						
Other contact info for tester						
Browser used for testing	Chrome	Firefox	Internet Explorer (7/8)	Opera	Safari	Other, Please specify

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

According to its self-declaration:

	<i>Yes (relevant quote from the self-declaration)</i>	<i>No info provided in the self-declaration</i>	<i>Not applicable²⁵ to this SNS (relevant quote from the self-declaration)</i>
Does the provider include information on terms of use in their self- declaration?			
Does the provider include information on safety in their self-declaration?			
Does the provider include information on privacy in their self-declaration?			
Does the provider state that the safety information is targeted (info specifically targeted at children)?			
Does the provider state that the safety information is presented in a prominent way?			
Does the provider state that the safety information is accessible?			
Does the provider state that the safety information is easy to understand?			
Does the provider state that the safety information is			

²⁵ If the provider has indicated in the self-declaration an explanation why this optional recommendation is not part of the service, please note that explanation in the 'not applicable' column

presented in a practical format?			
Does the provider state that the safety information provides guidance regarding inappropriate content and conduct and information on the consequences of breaching the Terms of Service?			
Does the provider state that the service includes information on links to educational material and technical controls for parents?			
Does the provider state that the service provides advice/link to advice for teachers?			

WITHOUT REGISTERING AS A USER, PLEASE ANSWER THE FOLLOWING QUESTIONS:

I can find the following information about the SNS on the site itself:	Yes, very easily	Easily	Partly easily/partly difficult	Difficult	Very difficult	I could not find it	N/A to this SNS	Comment?
Terms of use/service								
Safety policy								
Privacy policy/information								
Code of conduct ²⁶								
Safety tips/information for children								
Safety tips/information for parents and carers								
Safety tips/information for teachers								
Links to educational material or organizations active in child safety								
Other (according to self-declaration)								

²⁶ A code of conduct is a set of rules outlining the responsibilities of or proper practices for an individual.

PLEASE LOOK AT HOW THE SAFE USE INFORMATION TO THE DIFFERENT TARGET GROUPS IS PRESENTED ON THE SITE. CONSIDERING THE TARGET GROUP THE INFORMATION IS INTENDED FOR - DO YOU BELIEVE THE INFORMATION TO BE:

	Yes, very	Sufficiently	Some parts are easy, some parts are difficult	No	Not applicable to this SNS	Comment?
FOR TEACHERS						
Easy to understand?						
Easy to access (less than 15 seconds ²⁷)?						
Exhaustive?						
All material is available in (insert language)						
FOR PARENTS	Yes, very	Sufficiently	Some parts are easy, some parts are difficult	No	Not applicable to this SNS	Comment ?
Easy to understand?						
Easy to access (less than 15 seconds)?						
Exhaustive?						
All material is available in (insert language)						
FOR CHILDREN (<13)	Yes, very	Sufficiently	Some parts are easy, some parts are difficult	No	Not applicable to this SNS	Comment?
Easy to understand?						
Easy to access (less than 15 seconds)?						
Exhaustive?						
All material is available in (insert language)						
FOR TEENAGERS	Yes, very	Sufficiently	Some parts are easy, some parts are difficult	No	Not applicable to this SNS	Comment?
Easy to understand?						
Easy to access (less than 15 seconds)?						
Exhaustive?						
All material is available in (insert language)						

²⁷ Research shows that one second is the limit for the user's flow of thought to remain uninterrupted, while 10 seconds is about the limit for keeping the users attention focused on the dialog online. 15 seconds is therefore quite long. (Ref. Jakob Nielsen's "Designing web usability").

	Yes	No	Comment?
What kind of safety information is provided at this SNS (please choose all that apply)?			
General textual info			
General audio/video info			
Concrete examples (e.g. anecdotes, information on concrete consequences of safety threats etc)			
Information/tips for children and young people			
Information on safety settings of the user's profile			
External links/referrals to professional safety organizations and authorities (e.g. Insafe, national hotline, police, health authorities etc.)			

	Yes	Yes, but it is difficult to understand for children/young people	No/I cannot find this info	N/A to this SNS	Comment?
In their terms of service/use and/or codes of conduct does the SNS clearly list the following:					
Content that is not allowed on the social network (e.g. pornographic or racist content)					
Conduct (behavior/actions) that is not allowed (e.g. bullying, harassment, racist comments)					
Consequences of engagement in prohibited behaviour/actions (e.g. your user profile/messages/photos might be deleted, or police contacted)					
Age requirements					

	Yes, I can find it on the site	No/I cannot find this info	N/A to this SNS	Comment?
Is there any information provided on specific risks regarding using online services?				
The possibility of seeing or being the subject of images of child abuse				
Hate speech				
Pornography or sexual content				
Violence				
Inappropriate contact from adults with a sexual interest in children				
Bullying				

Divulging personal information				
Posting sexually provocative photographs				
Information on self-harm actions (anorexia, suicide etc)				
Other, please list:				

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

According to its self-declaration:

Recommendation: Limit exposure to potentially inappropriate content and contact. For example:	Yes (relevant quote from the self-declaration)	No info provided in the self-declaration	Not applicable to this SNS (relevant quote from the self-declaration)
Does the provider outline in the self-declaration how it is made clear to users when services are not appropriate for children and young people?			
Does the provider outline in the self-declaration how it is made clear to users where a minimum registration age applies?			
Does the provider in their self-declarations outline the steps taken to deny access under-age users from their services?			
Does the provider in their self-declarations outline the steps taken to deleting under-age users from their services?			
Does the provider in their self-declarations outline the steps taken to prevent users from attempting to re-register with a different age if they have previously been rejected for being below the minimum age (if their terms require a minimum age)?			
Does the provider in the self-declaration indicate how compliance with minimum age requirements is promoted (within technical and legal constraints)?			
Does the provider in the self-declaration outline how uptake of parental controls is promoted on the service?			
Does the provider in the self-declaration outline what functionality is provided for content providers, partners or users to label, rate or age restrict content that is provided?			
Does the provider in the self-declaration outline that certain professionally produced content is only shown at particular times of the day?			
Does the provider in the self-declaration outline other means they have employed to limiting exposure to potentially inappropriate <i>content</i> ?			

Does the provider in the self-declaration outline other means they have employed to limit exposure to potentially inappropriate contact?

--	--	--

PLEASE ATTEMPT TO SIGN UP AS AN ADULT USER. WHEN SIGNING UP, PLEASE STOP AT EACH STAGE MAKING SURE THAT YOU ARE ABLE TO RESPOND TO THE NEXT SECTION OF QUESTIONS. DEPENDING ON THE SNS THE INFORMATION PROVIDED BY THE SNS MIGHT NOT COME IN THE SAME ORDER AS THE QUESTIONS IN THE FOLLOWING SECTION.

	Yes	No	No/I cannot find this info	N/A to this SNS	Comment?
When signing up to the SNS it requires you to submit the following information:					
Birthday data at the registration process					
Statement that I am above a certain age (e.g. by ticking a box)					
E-mail verification*/address for e-mail verification					
<i>*If e-mail verification DO NOT verify over e-mail yet:</i>					
I am able to sign in even without verifying my e-mail address first (e.g. without clicking on a verification link sent over the e-mail)					

Now please make new attempts to sign up as specified below, using the SAME COMPUTER:

	The SNS allows me to sign up because the service is not age restricted	The SNS is intended to be age restricted but it allows me to sign up anyway	The SNS denies the signing up due to age restrictions	The SNS denies the signing up, but I am not told why	N/A to this SNS	Comment?
Sign up as a 11 year old child using 06.06.98 as date of birth						
Sign up again as a 15 year old child using 06.06.94 as date of birth						
IF PREVIOUS ATTEMPTS ARE REFUTED: Sign up again as a 15 year old child using 07.07.94 as date of birth						

PLEASE SIGN IN AGAIN TO THE SNS, USING THE YOUNGEST IDENTITY THAT IS WITHIN THE RULES OF THE SNS YOU ARE TESTING (IF THE SNS IS FOR ALL USERS/YOUNGER USERS, USE THE 11-YEAR OLD, IF THE SNS IS FOR OLDER USERS, USE YOUR 15 YEAR OLD IDENTITY). IF YOUR ATTEMPTS TO SIGN UP ARE REFUTED PLEASE REMOVE THE COOKIE FROM YOUR COMPUTER.²⁸ IF THIS DOES NOT WORK, PLEASE CHANGE COMPUTER AND LOG IN AGAIN.

I have successfully signed in as	Yes	Yes, but I had to remove cookies first	Yes, but I had to change computer	No, I had to move on to the next user profile	N/A to this service	Comment?
An 11-year old user						
A 15 year old user						
No need to sign in, access open						

Parental control tools	Yes, I can find it on the site ²⁹	No/I cannot find this info	N/A to this SNS	Comment?
Does the SNS provide any parental control tools?				

As a parent:	Yes	No/I cannot find this info	N/A to this SNS	Comment?
I can easily find the information on how to use parental control tools on the site				
I can easily understand how to use the available parental control tools.				
I can monitor my child's activities on the SNS.				
I have to verify my child's profile over the email before it can be used.				
I consider available parental control tools efficient.				

²⁸ Find information on how to do this on <http://www.aboutcookies.org/Default.aspx?page=2> for the browser you are using.

²⁹ If yes, please answer the following set of questions about parental control tools

Principle 3: Empower users through tools and technology

According to its self-declaration:

Recommendation: Employ tools and technologies to assist children and young people in managing their experience on their service. For example:	Yes (relevant quote from the self-declaration)	<i>No info provided</i>	<i>Not applicable to this SNS (relevant quote from the self-declaration)</i>
Does the provider indicate in the self-declaration that the private profiles of users registered as under the age of 18 are not searchable on the service or via search engines?			
Does the provider indicate in the self-declaration that full profiles are set to 'private' by default or to the user's approved contact list for those registering under the age of 18?			
Does the provider indicate in the self-declaration that users have control over who can access their full profile by, for eg, being able to block friends or 'reject' friend requests?			
Does the provider indicate in the self-declaration that users have the option to allow only direct friends to post comments and content to their profiles?			
Does the provider indicate in the self-declaration that users have the option to delete unwanted comments of other users?			
Does the provider indicate in the self-declaration that users have the option to pre-moderate comments from other users?			
Does the provider indicate in the self-declaration that it provides easy-to-use tools for users to report inappropriate <i>contact</i> from another user?			
Does the provider indicate in the self-declaration that it provides easy-to-use tools for users to report inappropriate <i>conduct</i> by another user?			
Does the provider give information in the self-declaration on how it educates parents about available tools, both for wider internet access and the tools, information and advice provided to parents by SNS to help them protect young people ?			
Does the provider address in the self-declaration how to delete profiles?			

On the Social Networking Site, I can find information on:

	Yes, I can find it on the site	No/I cannot find this info	N/A to this SNS	Comment?
How to report abuse or bullying;				
The possibility to block other users from contacting me (or reject friendship requests);				
The possibility to specify who or which groups of users can contact me (defined by age, gender, etc.);				
Restrictions on search options for profiles (e.g. not able to search for minors);				

PLEASE CONSIDER ALL THE INFORMATION YOU HAVE INSERTED INTO YOUR PROFILE PERSONAL INFORMATION AND ANSWER THE QUESTIONS BELOW (NB, BY "FRIENDS" WE MEAN ALL THE CONTACTS YOU CONFIRM WHEN RECEIVING THEIR FRIENDS REQUEST OR YOU HAVE ADDED YOURSELF):

When signed in to my user profile I am able to:	Yes	Yes, but the person who posted/own the profile must approve it first	No	I do not know/it does not say	N/A	Comment?
I am able to delete/remove postings on my profile						
I am able to delete/remove pictures on my profile						
I am able to delete/remove postings I have put on other peoples profile						
I am able to delete/remove pictures I have put on other peoples profile						

On my user profile:	Yes	Yes, but I must approve it before it is published	No	I do not know/it does not say	N/A	Comment?
All users can post comments on my profile						
Only my friends can post comments on my profile						

When signed in to my user profile:	Yes	Yes, but only some of the information	No	I do not know/it does not say	N/A	Comment?
My personal information is visible to all other users						
My personal information is visible only to my friends						
I have to change settings for my personal information to be visible to other users						
I have control over the display of my online status (if other people can see if I am online)						

When I am about to upload a photo/publish information on my profile I get:	Yes	No	I do not know/it does not say	N/A	Comment?
Safety tips and/or guidance about publishing personal information on the profile					
Safety tips and/or guidance about uploading the photo onto my profile					

When signed in to my user profile:	Yes, and I can approve it before the photo is published	Yes, but I do not have a chance to approve the photo before being published	No	I do not know/it does not say	N/A	Comment?
I am notified when I am identified (tagged) in pictures posted on other people's profiles						

If I wish to delete my profile:	Yes	No	I do not know/it does not say	N/A	Comment?

I can find easy-to-understand information on how to delete/deactivate my profile.					
There is a clear link/button provided for deleting/deactivate my profile.					
I can only deactivate my profile but not completely delete it.					
The provider provides information about what personal information the SNS collects/retains after deleting/deactivating my profile.					
The provider provides information about how the personal information is/may be used once I delete/deactivate my profile.					

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

According to the self-declaration:

	<i>Yes (relevant quote)</i>	<i>Yes (relevant quote)</i>
Does the provider indicate in the self-declaration that a mechanism for reporting inappropriate content, contact or behavior is provided?		
Does the provider indicate in the self-declaration that reporting mechanisms are easily accessible to users at all times?		
Does the provider indicate in the self-declaration that the reporting procedure is easily understandable?		
Does the provider indicate in the self-declaration that the reporting procedure is age-appropriate?		
Does the provider indicate in the self-declaration that reports are acknowledged?		
Does the provider indicate in the self-declaration that reports are acted upon expeditiously?		
Does the provider indicate in the self-declaration that users are provided with the information they need to make an effective report and, where appropriate, an indication of how reports are typically handled?		

Principle 5: Respond to notifications of illegal content or conduct

According to the self-declaration:

	<i>Yes (relevant quote)</i>	<i>No info provided</i>	<i>Not applicable (relevant quote)</i>
Does the provider indicate in the self-declaration that effective processes are in place to expeditiously review and remove offending content upon receipt of notification of alleged illegal content or conduct?			
Does the provider indicate in the self-declaration that arrangements are in place to share reports of illegal content or conduct with the relevant law enforcement bodies and/or hotlines?			
Does the provider indicate in the self-declaration that links to other local agencies or organizations, for example that relevant Inhope services and law enforcement agencies are featured?			

On the Social Networking Site

When signed into my user profile I can find:	Yes, (available all the time)	Difficult (more than 15 seconds)	No, I cannot find it	N/A to this SNS	Comment ?
a link/information on where to report other users that bothers me /violations of terms					
a link/information on where to report content that bothers me/violations of terms					
Information on how to block a friend/contact request					
A link/tool where I can report abuse/violation of terms is visible at all times when I am signed into the SNS					

When signed in to my user profile:	Yes	No	I do not know/it does not say	N/A	Comment?
I can block a friend					
I can decline a contact request					

BEFORE YOU START ANSWERING THE FOLLOWING QUESTIONS, PLEASE REVIEW THE SELF-DECLARATION REPORT IN REGARD TO HOW USERS CAN REPORT ABUSE ONLINE. PLEASE ALSO LOCATE THE REPORT MECANISM ON THE SNS SITE AND SEND THE REPORT THAT HAS BEEN PROVIDED FOR YOU IN ANNEX II TO THE SNS.

	Yes	No	N/A to this SNS	Comment?
The report mechanism				
Is easy to understand (for children/young people)				
Is difficult to find (more than 15 seconds)				
Sends a notification/receipt to the user when a report has been sent				
Sends information to the user on how a report will be handled				
Gives feedback to the user about the report/result? If so, how long did it take:				

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

According to the self-declaration:

<i>Recommendation</i>	<i>Yes (relevant quote from self-declaration)</i>	<i>No info provided</i>	<i>Not applicable (relevant quote)</i>
Does the provider indicate in the self-declaration that a range of privacy setting options are provided for users?			
Does the provider indicate in the self-declaration that privacy options are supported by information that encourage users to make informed decisions about the information they post online?			
Does the provider indicate in the self-declaration that privacy options are prominent in the user experience?			
Does the provider indicate in the self-declaration that privacy options are accessible at all times?			
Does the provider indicate in the self-declaration that the implications of automatically uploaded information provided during registration onto profiles have been considered?			
Does the provider state in their self-declaration that users are notified when the information used to register is automatically uploaded onto their profile?			

Does the provider indicate in the self-declaration that when information is automatically uploaded to profile users are able to edit and make public/private that information where appropriate?

Does the provider indicate in the self-declaration that users are able to view their privacy status or settings at any given time?

Does the provider address in the self-declaration the issue of third party applications?

	Yes	No	I do not know/it does not say	N/A	Comment?
When signed in to my user profile:					
I can easily change my privacy settings.					
Applications (3rd party, external or additional programs and/or services) need permission from the user to be installed and/or pull info from user's profile.					

	Yes	Yes, but optional	No	I do not know/it does not say	N/A	Comment?
When registering ³⁰ to the SNS I am asked to provide the following personal information						
Age						
Education						
e-mail						
Gender						
Home address						
Nationality						
School or workplace						
Parents' e-mail						
Personal security/identification number						
Phone number						

³⁰ In order to be able to create a profile on a social networking site, most of these services require that the user is registered with them. In order to register, the user needs to fill out a form with certain personal information (such as age, name, email address, etc)

Picture of yourself						
Political sympathies						
Real name (first and last)						
Real name (only first)						
Religion						
Other, please specify...						

Please list which personal information that you used for registration was automatically inserted into your profile ³¹	Information was inserted into profile	Information was not inserted into profile	I am not sure/It does not say (please also add comment)	Comment?
Age				
Education				
e-mail				
Gender				
Home address				
Nationality				
Parents' e-mail				
Personal security/identification number				
Phone number				
Picture of yourself				
Political sympathies				
Real name (first and last)				
Real name (only first)				
Religion				
School or workplace				
Other, please specify..				

PLEASE SIGN OUT AS A CHILD AND THEN SIGN IN AGAIN AS AN ADULT.

³¹ With most social networking services, creating a profile is possible only after registration with the respective service. In some cases, the information provided for registration is also automatically used for building a profile for the new user. The objective of the testing is to check to what extent this happens and whether the user has any control on the information that is included in his/her profile.

	Yes	No	N/A	Comment?
When signed in as an adult user:				
I am able to search for my other profile(s) where I test as an 11/15 year old				
I am able to search for users /user profiles that are 16 years old or younger				
I am able to search for users /user profiles that are 12 years or younger				
When I use search engine and search my nick names I am able to find the profiles I have registered as a minor in the SNS				

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

According to the self-declaration:

Recommendation: Promote compliance with the Terms of Use, Acceptable Use Policy and/or House Rules. For example, by employing:	<i>Yes (relevant quote from the self-declaration)</i>	<i>No info provided</i>	<i>Not applicable (relevant quote from the self-decl)</i>
Does the provider in the self-declaration indicate that it employs human and/or automated forms of moderation?			
Does the provider in the self-declaration indicate that it employs technical tools (e.g. filters) to flag potentially illegal or prohibited content?			
Does the provider in the self-declaration indicate that it provider employs community alerts?			
Does the provider in the self-declaration indicate that it responds to user-generated reports?			
Does the provider in the self declaration indicate that where human moderators are employed, reasonable steps are taken to minimize the risk of employing candidates who may be unsuited for work which involves real-time contact with children or young people?			

Annex 4. Description of participating Social Networking Sites



The following is a description of the Social Networking Sites (SNSs) that have signed the “Safer Social Networking Principles for the EU” and been included in the analysis provided in this report. The descriptions of the services are compiled verbatim from their self-assessment reports, and can also be found under “Point 1. About the Social Networking Services” of each submitted report.

Arto.com

Arto.com is a social networking site, who's core user base is made up by teenagers. We have a minimum age requirement of 12 years old, but we have no upper age limit. Users create a profile where they can choose how to inform visitors about themselves. The design process of this is decided solely by the user, and he or she may decide how much information is given to visitors. Through several features on the site the users keep in touch with friends from the real world and new friends made on the site. This includes a guestbook, which is the main tool for communication, a hidden mail system, a public chat with private rooms, a chat tool for talking with friends which also offers microphone and webcam support. We also offer the users a forum divided into different categories where they may discuss certain topics with other users. We have a club-section where our users may create fan clubs on any given topic (a soccer team, cartoons, school, games, idols etc) and these clubs all feature a secluded club profile, forum, gallery, calendar and file sharing system for the members of the club. The users may create and manage blogs, galleries with pictures and video, post messages on a bulletin board, share high resolution photos from events and travels, and play games with and against other users. We also offer features that allow users to create quizzes for their friends and new relations to answer, and we have an Idol section that allow the creative user to upload videos of them and their friends singing, dancing, juggling or other talents they may wish to share and the community may rate and comment the videos they upload.

Bebo

Bebo (www.bebo.com) is a popular social networking site that connects users to everyone and everything they care about. It was founded in 2005 and since May 2008, has been part of AOL's People Networks division. Bebo combines community, self-expression and entertainment, enabling users to consume, create, discover, curate and share digital content. Bebo allows users to find and communicate with friends as well as discover, experience and share user generated content. Users can create profiles and interact with friends' profiles, send messages to other users, join groups, become fans of bands, use third party applications, and using third party services, upload and share photos and videos. Bebo has a membership of more than 45 million individuals worldwide with experiences optimized for the US, UK, Ireland, Australia, New Zealand, Canada, Poland, France, Germany, Italy, Spain, India and the Netherlands. Bebo recently launched a series of new products including, Social Inbox, which allows you to organize your messages in one easy-to-use inbox, Lifestream Platform which delivers real-time, chronological updates from all of your friends from Delicious, Facebook, Flickr, Myspace, YouTube and Twitter, and Lifestory, an interactive display of life events in chronological order. Users can also access the Bebo experience through their mobile phone, enabling them to send and receive SMS updates and alerts, update their Bebo profile, add photos to their gallery, send virtual gifts and access mobile content. Bebo, and its parent company AOL, takes the safety and wellbeing of its users very seriously, as reflected in the range of safety and education features and tools on its service as outlined below. We also engage heavily in a range of multi-stakeholder dialogues on internet safety across the world including: the EU social networking task force; the UK Council for Child Internet Safety and its predecessor the Home Office Internet TaskForce; the UK cyberbullying taskforce; the Technology for Wellbeing group in Ireland; and the US Internet Safety Technical Task Force.

Dailymotion

Dailymotion is a video hosting service website attracting over 47,9 million unique monthly viewers worldwide. Every day, over 15,000 new videos are uploaded into Dailymotion's global suite of 18 localized video entertainment sites. In January 2009, Dailymotion streamed over 914 million videos to users, including curated content from premium and "Motionmaker" creative contributors. Offering the most advanced technology to both users and content creators, Dailymotion provides high quality and HD video in a fast, easy-to-use website that automatically filters copyright-infringing material when notified by content owners. Dailymotion is more of a video platform than a "social networking service", but it does deploy a number of social features. Users may communicate by leaving comments on each other's

videos, sharing videos with their contacts, and messaging their contacts through an internal inbox system. The contact model is reciprocal: you are only considered a contact when the second party has confirmed and approved the relationship.

Facebook

Facebook gives people the power to share, making the world more open and connected. Worldwide, we have more than 200 million active users keeping their friends and families up to date with the happenings in their lives. Facebook's authenticity-based, real name culture, as well as its innovative privacy controls and safety features are designed to build a safer and more trusted online experience.

Google

Google fully supports the creation of these principles and the approach with which they have been drafted. In such a fast moving environment as online services it is crucial for stakeholders to work in a collaborative and flexible approach. We commend the European Commission for bringing together the task-force and for encouraging this self-regulatory approach. Google is deeply committed to protecting children on the Internet and providing all of our users with a safe experience online through empowerment, education, and protective measures. That's why we empower parents with tools to help them choose what content their children see online; educate children on how to stay safe online; and protect children through partnerships with law enforcement and industry. We build these key 3 principles through all Google products and services. Google's family safety centre is a great resource for any user looking for safety tools and resources. The tools we offer are varied depending on the services. Firstly to help prevent access to unwanted content Google Search has implemented 'safe search' which can be easily chosen through the preferences tab on the Google home page. Many users prefer not to have adult sites included in their search results (especially if their kids use the same computer). Google's SafeSearch screens for sites that contain inappropriate content and eliminates them from search results. While no filter is 100% accurate, Google's filter uses advanced technology to check keywords, phrases, and URLs. Users can modify their computer's SafeSearch settings by clicking on the Preferences link to the right of the Google search box. On balance we empower users with tools to combat abuse with report mechanisms in YouTube or Blogger for example. This will be explored more in relation to Principle 4. Google also actively supports law enforcement efforts to keep kids safe online. Google also provides training and technical assistance to law enforcement officials investigating online crimes against children through forums such as the Internet Crimes Against Children (ICAC) National Conference and the Virtual Global Taskforce (VGT). Google has a specialized legal team dedicated to working with law enforcement officials, available 24 hours a day, 7 days a week. We're also leveraging Google tools to combat online child exploitation. Throughout 2007, engineers used some of their 20% time to create innovative software tools. The keys here were organization, scalability, and search. In particular, the tools we provided will aid in organizing and indexing NCMEC's information so that analysts can both deal with new images and videos more efficiently and also reference historical material more effectively. This task has been time-consuming, and NCMEC analysts were simply getting overwhelmed by all of the data they had to sift through to help NCMEC track down child predators through video and image search. With these tools, analysts will be able to more quickly and easily search NCMEC's large information systems to sort and identify files that contain images of child pornography. In addition, a new video tool we built streamlines analysts' review of video snippets. Google has also donated Google Search Appliances and hundreds of thousands of dollars of in-kind advertising each year through our Google Grants program to national clearinghouses for child exploitation cases in the U.S. (National Center for Missing and Exploited Children) and the U.K. (Child Exploitation and Online Protection (CEOP) Center). Google is a member of both NCMEC's Financial Coalition Against Child Pornography and Technology Coalitions. The Financial Coalition includes leading banks, credit card companies, third party payment companies and Internet services companies, and is dedicated to fighting child pornography over the Internet. The goal of the Financial Coalition Against Child Pornography is to eradicate commercial child pornography. NCMEC's Technology Coalition's mission is to develop and deploy technology solutions that disrupt the ability of predators to use the Internet to exploit

children or traffic in child pornography. In an outshoot of that industry initiative we discovered some other areas where I thought Google could help the staff at NCMEC. In relation to these principles, Google is not a social networking service however there are social elements to our video sharing platform YouTube. YouTube is a user generated video sharing platform around which communities form, have discussion and interact. Bearing this in mind, Google provides below how it maintains these principles on the YouTube platform, where the relevant principles can be applied.

Hyves

Hyves is Holland's most popular social network and the most visited Dutch website.

Microsoft

Founded in 1975, Microsoft (NASDAQ:MSFT) is the worldwide leader in providing software, services and solutions that help people and businesses realize their full potential. We have been operating in Europe for over 20 years and employ more than 13,000 people in the region. We have subsidiary offices in all EU member states. Microsoft understands that the guidance provided by the EU Safer Social Networking Principles is not intended as a "one size fits all" solution. Accordingly, while providers should support all seven Principles, each provider should judge for itself where and how to apply the document's specific recommendations. Given that the Principles are not prescriptive or legally binding, we believe that the question of whether any of Microsoft's services are or should be classified as "social networking" as a matter of any national law is outside the scope of this document. However, we do offer a number of services that combine the following features: promoting online social interaction between two or more persons; allowing users to create online personal profiles; engaging in communication and sharing information, files and gaming experiences. Such Microsoft services include:

***Xbox LIVE**, an online gaming and entertainment service that connects more than 17 million members across 26 countries. Details about this service can be found at www.xbox.com/live.*

***Windows Live**, a service that keeps users in sync with a range of services and applications that work together across the PC, phone and Web and allows individuals to decide how, when and where to use the services. More than 460 million customers around the world use Windows Live to share e-mail, messaging, photos and files within their networks of friends, family members, colleagues and others. Windows Live is available at www.windowslive.com.*

In this declaration, we will outline our efforts to increase trust and safety online with a special emphasis on the two services described above.

MySpace

MySpace.com (“MySpace”), a unit of Fox Interactive Media Inc. (“FIM”), is the world’s premier social portal for connecting people, content, and culture. MySpace empowers its global community to experience the Internet through a social lens by integrating personal profiles, photo sharing, professional and viral videos, blogs, mobile, instant messaging, and the world’s largest music community. MySpace is the highest trafficked website in the United States and includes an international network of more than 30 local community sites throughout North America, Latin America, Europe, Asia, and Australia.

Nasza-klasa.pl

Nasza-klasa.pl is a social networking site gathering Internet users who want to find classmates. Thanks to *nasza-klasa.pl* it is possible to rebuild relations with colleagues from kindergarden, primary school, high school or college. *Nasza-klasa.pl* was created by four students: Maciej Popowicz, Paweł Olchawa, Michał Bartoszkiewicz and Łukasz Adziński and has been operating since 11th of November 2006. Today there are over 20 million profiles on this website. Every month *nasza-klasa.pl* users generate 15 billion pageviews (22.62 page/visit; 00:11:20 avg. time on site/visit). *Nasza-klasa.pl* offers many social features which help people 'stay in touch'. Users can create their own profiles, join school and class profiles, gather their friends, send internal messages, upload photos, leave comments on profiles and under photos and chat with friends via the forum. Almost 80% of *nasza-klasa.pl* users are adults, but this number doesn't change the fact that we try to protect our younger visitors.

Netlog

Netlog is a pan-European social networking website with its headquarters in Belgium. On *Netlog*, youngsters can connect with and extend their social network. Young people between 13-24 years of age form *Netlog*’s target group, however people of all ages are welcome to subscribe. *Netlog* gathers over 45 million individual users worldwide and is available in nearly 30 language versions.

ONE.LT

ONE.LT is a social networking site serving over one million internet users in Lithuania as well as a sizeable Lithuanian-speaking internet user audience in other countries. *ONE.LT* offers a variety of social features helping people express themselves and stay in touch with their real-life and virtual friends. *ONE.LT* enables users to create and accessorize online profiles, establish friend connections with other users on the site, exchange private in-site messages, upload and showcase photos, post notes to forums attached to individual user profiles and user groups, rate user photos join public online clubs dedicated to specific themes or topics, send virtual gifts to friends and participate in other online communication activities of similar nature. AS of Q1 2009, *ONE.LT* is accessed by over 900 thousand unique users a month generating nearly 1 billion pageviews a month. While the significant majority of *ONE.LT* users are above 18 years of age, *ONE.LT* does provide services to younger users and considers its responsibility to work toward ensuring their safety, providing protection against abuse and inappropriate content.

Piczo

Piczo.com (“Piczo”), a unit of the Stardoll Network (“Stardoll”), empowers teens worldwide to creatively express themselves, build personal communities, and share ideas and experiences with their friends in a safe online environment. Since its launch, *Piczo* has roughly 6.5 million monthly unique visitors and over a 150 million monthly page views solely through the viral efforts of loyal members. Rave reviews from these members claim that *Piczo* is unmatched in the control, ease-of-use, and flexibility it offers them when building their websites. *Piczo*’s customizable content, colorful graphics, glitter text, video, and photo tools spotlight member creativity without requiring technical skills. Members share their life stories with friends by designing their sites with multiple pages featuring photos, graphics, videos, music,

comment boards, games, and more. Each site can be linked to other friends' sites and members can interact with them and their friends, and meet new people online. And, the "first of its kind" Piczo Zone allows members to share their customizable content with the rest of the Piczo Community. The end result is a vibrant, creative community where members are given the complete freedom to make a site, make friends, or make whatever. Piczo recently merged with Stardoll.com and PaperDollHeaven.com to form the Stardoll Network, with a combined reach of more than 20 million people a month, a majority of which are girls aged 5 to 20. Piczo, along with the Stardoll Network are based in Stockholm, Sweden with offices in London and Los Angeles.

Rate.ee

Rate.ee is the largest social networking site in Estonia. Launched in 2002 offering a simple picture rating service it has since grown to a fully fledged online community featuring friends lists, blogs, albums, and many other services. It has now over 300,000 active users comprising a one fifth of the population. EMT, the largest telecom company in the country, acquired a majority stake in Rate.ee in 2006.

Skyrock

Skyrock.com is a global social networking site dedicated to the New Generation offering its members a free, personal web space where they can create a blog, add a personal profile, share photos and videos, and exchange messages with other registered members. The platform registers 35 million accounts¹, and is frequented by over 14.508 million of Unique Visitors in Europe (reach: 4.7%)². Fifty percent of those visitors are under eighteen years old¹. 1 : Internal data – April 13th 2009 2 : Mymetrix Comscore – Europe – Skyrock.com – February 2009

StudiVZ

studiVZ Ltd. provides three Social Networks for the German market.

schülerVZ, www.schuelervz.net SNS for pupils in the age of 12 to 21, 5 Million users (April 2009)

studiVZ, www.studivz.net SNS for students with full legal capacity, 5,5 Million users (April 2009)

meinVZ, www.meinvz.net SNS for employees and alumni with full legal capacity, 3 Million users (April 2009)

75% of all Germans between 14 and 29 years own an account at one of the three VZ-Networks. schülerVZ is a stand-alone platform, it is not possible for those users to interact with persons who are registered at studiVZ or meiVZ e.g. by sending messages or friend requests studiVZ and meinVZ are completely interconnected, users can contact each other but they are not able to contact users of schuelerVZ. All three platforms are real name based, authentic networks.

Sophisticated privacy settings enable every user to choose, which information of him can be seen by friends and other users. Users of a VZ-Network can create a personal profile, upload images, find discussion groups, organize friend lists, use an platform based instant messaging service, send private messages and have also a mobile access to the network.

Sulake

Sulake is an online entertainment company focused on virtual worlds and social networking. Sulake's main product Habbo is one of the world's largest and fastest growing virtual worlds and online communities for teenagers. Currently there are localized Habbo communities in 31 countries on six continents and to date over 129 million Habbo characters have been created. On a monthly basis the service is visited by over 11,7 million unique browsers worldwide. Habbo is a richly colorful, multi-dimensional virtual world and community for teens. Users join by creating a fully customized online character called a Habbo. From there, they can explore many public hang-outs, participate in a variety of activities, connect with friends, decorate their own rooms, and have fun through creativity and self expression. The majority of Habbo users globally are between 13 and 16, equally boys and girls. The age limit to Habbo is 13 in most of

the countries. Virtual world Habbo is not a typical “social networking service”, which means that certain best practices in the principles don’t apply to it. In Habbo users can’t e.g. post any real-life photos, videos or share any personal information. However, the users have their own Habbo profiles, they meet and chat with friends, like in other social networking sites. Teens are attracted to Habbo because of the camaraderie of the community and the opportunity for self-expression. The animated nature of the site itself fosters a spirit of non-violence and nonaggression; fun and creativity are encouraged and openly displayed. Online safety is a high priority for Sulake Corporation and the company is committed to keep Habbo a safe haven for its teens. Sulake uses a variety of vehicles that work together to help ensure a safe online experience for Habbos: (i) Empowering its users (both teens and their parents) through education and participation

(ii) Active moderation by real people in Habbo

(iii) Using advanced technology in Habbo for content monitoring

(iv) Using payment limits with different payment methods

(v) Working with law enforcement around the world

(vi) Working with external partners and governmental organizations (like Safer Internet Day) on player safety issues

Tuenti

TUENTI is a private social network that allows users to create a space where they can post and share information, as well as communicate with people they already know. TUENTI allows users to stay in touch with their friends and acquaintances and to stay informed of events and developments concerning their social circles. TUENTI is a ‘private’ network and people can only join our platform if they have been previously invited to do so by a current TUENTI member. By only allowing users to join if they are invited by a pre-existing member, we have developed a platform built on confidence that allows users to interact with people they already know.

Yahoo!

Yahoo! is a leading global internet brand and one of the most trafficked internet destinations worldwide. Headquartered in Sunnyvale, California, and with its European HQ in Switzerland, Yahoo!'s global network includes 25 world properties and is available in 13 languages. Yahoo! provides online products and services, offering a variety of services essential to users’ life with ‘social networking’ features. These comprise Flickr (photo sharing), Yahoo! Video (commercial and user generated video sharing) and Yahoo! Answers (knowledge sharing).

ZAP

ZAP is a free-access social networking website for people aged 13 and over with a valid e-mail address. The main features on our website are events schedules, nightlife reports, profiles, homepages and photos. ZAP is the most visited community platform in Luxemburg integrating individual and business profiles. Individual profiles enable users to present and describe themselves in order to meet friends or become get to know other people. Public messages can be exchanged in the “Shoutboxes” which are to be found on every profile, unless this function has been deactivated by the user. Other features are the friends list, the clickers list, the mail system... Of course pictures and videos can be uploaded on the homepages.

**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>