

HYVES

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

Introduction

Hyves is one of the most popular social network sites in The Netherlands and counts more than 10,6 million members¹. This social network platform started in 2004 and is available in two languages (Dutch and English). The founders refer with the name of their social network site to a *beehive*, full of activity. Members can keep contact with friends and meet new people. Next to their profile, users can develop and consult blogs, post comments on profile pages, upload and browse through users' pictures and videos. Also 'gadgets' can be added to one's own profile (embedded third party applications). Next, classifieds can be published and games can be played online. Moreover, users can create groups ('Hyves') that gather persons sharing, for instance, the same interests. The social network site has also created a mobile application, giving the opportunity to be connected everywhere. Persons younger than 16 years old need parental permission to subscribe. According to a study, three quarters of the Dutch 8 till 17-year-olds has a profile on Hyves².

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

Summary of main findings

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

Users of Hyves are offered a broad range of privacy settings that are easy to find. However, tests concluded that profiles of minors are not set to "private by default"³ as defined in the Safer Social Networking Principles⁴. As a matter of fact, not only friends, but also other registered users have access to some profile data of minor users including their name, likes/dislikes, hobbies, relationship status, pictures and comments posted by others). By default, other users (including friends) do not have access to contact details such as the home address, mobile phone number and location on Google maps. Only the (minor) user's e-mail is, by default, displayed to friends. The test also revealed that minors' profiles can be found by (adult) users through the social network site's search engine, although not via external ones such as Google.

¹ Including 9 million members in The Netherlands. Source: *Hyves in numbers* webpage (<http://www.hyves.nl/about/facts/>), information retrieved on the 16th of December 2010

² *Krabbels & Respect plz? Hyves en Kinderen*, September 2009, <http://www.mijnkindonline.nl>

³ "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".

⁴ http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

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

Finally, information and hints on safety and security issues are easily accessible from the “Hyve safely” webpage. Also the FAQ-page is well organized, including a special section dedicated to *privacy, bullying and spam*. Moreover, links are included to several websites that offer more practical advice. Next to hints for young users, a webpage is dedicated to parents, including some tips and a hyperlink to more educational material. By contrast, the length, formal phrasing and the inclusion of legal jargon in the Terms of Use may prevent (young) users to read this essential information.

Analysis of Results by Principle

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

Main findings in relation to the self-declaration

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

The self-declaration does not include explicit information on what constitutes inappropriate behaviour on the site or the consequences thereof. It does mention, however, that “pornographic or nude content with visible genitals is forbidden” on the site, but no other types of inappropriate content are mentioned. The self-declaration states that Hyves “will provide a parallel document to the Terms of Use, which will explain the rules and regulations in a clear and simplified matter.”⁵

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

Main findings in relation to the website

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

The Hyve safely (“Veilig hyven”) webpage provides an overview of important safety and security issues. Concrete hints are formulated in short paragraphs that address several

⁵ This document is live as of the first week of January 2011 and can be found on

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

important topics, for instance, how to choose a ‘strong’ password, how to protect sensitive information (like phone number, e-mail, location). As this information is easy to understand, it is adapted to, amongst others, young social network site users.

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

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

However, a simpler version⁶ of these Terms of Use is available⁷. The Privacy Policy (« Je privacy ») informs users about the uses of disclosed personal information, automatically generated data, that advertisement is adapted to the user’s profile, etc. Again, this text is quite long.

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

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

Main findings in relation to the self-declaration

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

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

Main findings in relation to the website

⁶ According to the provider, this simpler version of the Terms of Use is the shortest version they could provide due to Dutch jurisdiction.

⁷ A simpler version of the Terms of Use can be consulted on <http://www.hyves.nl/useragreement/short/>

Hyves does not state explicit minimum age requirements. Yet, according to the Terms of Use and the Privacy Policy, users younger than 16 need parental permission to subscribe on the site. However, subscribers are only informed that «If you are not yet sixteen (16) you may only create an account subject to the prior consent of your parents or guardian»⁸, still no parental consent is required to be able register on the site as a minor. As a matter of fact, when registering, users are asked to select their year of birth from a drop-down menu (reaching from 1900 till 2010). It was possible to subscribe as a 9 year-old without further questions or remarks. No parental consent was asked by using a parental consent form or any other procedure.

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

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

⁸ «By accepting these Terms of Use you guarantee that you are aged sixteen (16) or over or have the consent of your parents or guardian to create an account », see: <http://www.hyves.nl/useragreement/>

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

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

Main findings in relation to the website

Concerning the default privacy settings of minors, the test demonstrated that profiles of minors are not set to “private by default”⁹ as defined in the Safer Social Networking Principles¹⁰. As a matter of fact, not only friends, but also other registered users have access to some profile data of minor users (e.g. name, likes/dislikes, hobbies, relationship status, pictures and comments posted by others). By default, other users (including friends) do not have access to contact details such as the home address, mobile phone number and location on Google maps. Only the (minor) user’s e-mail is, by default, displayed to friends. However, if the minor selects his/her school and adds a link to the schools profile page, the location of the minor could, eventually, be available by default.

The test also revealed that minors’ profiles can be found by (adult) users through the social network site’s search engine, although not via external ones such as Google. The adult user (created for this test) was, indeed, able to access the profile page and send a friendship request. Furthermore, the (adult) user could add a personal message to the friendship request. Yet, the minor had to confirm this request. These observations are not in line with the self-declaration stating that « New profiles for under 16s are automatically defaulted to private » and « no user can search for under 16s». In sum, profiles of users younger than 16 are not defaulted to private as defined in the Safer Social Networking Principles¹¹.

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

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

If the user is confronted with inappropriate content or conduct, easy-to-use procedures are in place to erase this content and report abuse (see Principle 4). A subscriber can also restrict posting comments and also the access to comments to specific groups. Users can also choose

⁹ “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”.

¹⁰ http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

¹¹ http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

which images (photo albums) will be visible for friends, their friends or everybody. Finally, users can conceal their online status.

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

Main findings in relation to the self-declaration

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

Main findings in relation to the website

When assessing the report mechanism in the social network site, it was observed that users can easily report inappropriate content and conduct in two ways. First, via an online contact form reachable from the Terms of Use, the FAQ-page and the Hyves Safety pages; and second, via the abuse button found near user-generated content. This easily accessible and recognizable button leads to a pop-up form offering the user the opportunity to select a category of abuse (bullying/stalking, spam, discrimination/racism, porn, etc.) and to add a few comments¹². Users are also made aware about the consequences of their report and are clearly asked not to make reports on innocent users. No information is added on how reports are typically handled.

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

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

The analysis of the self-declaration shows that Hyves has effective processes in place to expeditiously review and remove offending content. Hyves claims that their “dedicated” security team identifies potential problems and reacts personally and promptly (within 24 hours) whenever confronted with (sensitive) security issues. Hyves also states that they cooperate with the Dutch Police (KLPD) as well as with other individual law enforcement

¹² If the user needs more space, the provider refers to the contact form. A hyperlink is provided, but does not directly lead to the form.

units to provide them with “information and knowledge on how to use social networks for citizen safety”.

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

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

Main findings in relation to the self-declaration

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

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

Main findings in relation to the website

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

New subscribers are asked to check a box near a sentence stating that they agree with the Privacy Policy and Terms of Use. Therefore, users that are filling in the online form are invited to check this important information. Furthermore, an opt-in check-box is used to ask members if they wish to receive commercial e-mails from partners. Besides, a CAPTCHA¹³ (to prevent the use of automated systems to subscribe and engage in spam) was also included in the subscription form. Moreover, an e-mail verification system is used to prevent unwanted subscriptions.

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

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

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

¹³ *Completely Automated Public Turing Test to tell Computers and Humans Apart* is a challenge-response system test designed to differentiate humans from automated programs (searchsecurity.com).

Main findings in relation to the self-declaration

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

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

Principle 7 was not tested in the website.

Summary of Results and Conclusions

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

- Profiles of users younger than 18 are not set to "private by default" as defined by the Safer Social Networking Principles. As a matter of fact, not only friends, but also other registered users have access to some profile data of minor users (e.g. name, likes/dislikes, hobbies, relationship status, pictures and comments posted by others).
- As far as minimum age requirements are concerned, the provider states that users younger than 16 need parental consent to subscribe to the site. However, in order to register on the site no proof of parental permission was required.

Assessment of all the Principles in the Self-declaration

<i>Principle</i>	<i>Very satisfactory</i>	<i>Rather Satisfactory</i>	<i>Unsatisfactory</i>
1		x	
2		x	
3		x	
4		x	
5		x	
6		x	
7		x	

Implementation of the Self-declaration on the Social Network Site

<i>Principle</i>	<i>Very satisfactory</i>	<i>Rather satisfactory</i>	<i>Unsatisfactory</i>
1	x		
2		x	
3		x	
4	x		
6		x	

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