# Safer Social Networking Principles for the EU

10 February 2009

# Supporters

Arto

bebo

Dailymotion
www.dailymotion.com

facebook

Studenti.it
GIOVANI

Google

Hyves
always in touch with your friends

Microsoft

myspace.com
a place for friends

nasza-klasa.pl
PORTAL DLA LUDZI Z KLASĄ

NETLOG

one
extremely friendly

PICZO

schülerVZ studiVZ meinVZ

SKYROCK.COM
Free People Network

sulake

YAHOO!
EUROPE

zap.lu

rate.ee

tuenti

# Contributors

ADICONSUM
associazione difesa
consumatori e ambiente

Childnet
International

CHIS

e-enfance
Le net qui laisse
toutes ses chances
à l'enfance

Red Barnet
Save the Children Denmark

Save the Children
Italia ONLUS

vodafone

# Supporters

**Chair** – Dr Rachel O'Connell, VP AOL and Chief Security Officer, Bebo
**Secretary** – Victoria Read, Head of Government and Regulatory Affairs, Bebo

Dan A. Poulsen, Editor and Head of Administration, Arto.com
Giuseppe Demartino, SVP and General Counsel, Dailymotion
Karima Ben Adelmalek, Juriste d'Affaires, Dailymotion
Chris Kelly, Chief Privacy Office and Head of Global Policy, Facebook
Luc Delany, European Policy Associate, Google
Nine Ludwig, Redacti, Hyves
Verena A. Gioia, Chief Editor, Gruppo SMB
Jan Muehlfeit, Chairman Europe, Microsoft
Thomas Myrup Kristensen, EU Internet Policy Director, Microsoft
Rita Balogh, Policy Advisor, Microsoft
David Fares, Vice President, Government Relations, News Corporation (on behalf of MySpace)
Shereen Meharg, Director of Safety and Security, Fox Interactive Media UK Ltd
Arkadiusz Pernal, Chief Executive Officer, nasza-klasa.pl
Cedric De Vleeschauwer, Netlog
Aldas Kirvaitis, ONE.LT
Keith Crowell, Director, Product Evangelist, Piczo
Jérôme Aguesse, Directeur de Production, Délégué à la prévention et la sécurité, Skyrock
Philippe Gröschel, Jugendschutzbeauftragter, Studivz
Juhani Lassila, Director, PR & Communications, Sulake Corporation Oy
Emma Ascroft, Head of Public and Social Policy, Yahoo! UK and Ireland
Fraenz Schintgen, Zap.lu

Viktor Ostsepkov, CEO, Rate.ee
Natalia Martos Díaz, General Counsel and Chief Privacy Officer, Tuenti

# Contributors

Nicola Fabiano, Consultant, Adiconsum
Julian Coles, Senior Advisor, Editorial Policy, BBC
Lucinda Fell, Policy & Communications Manager, Childnet International
Peter Davies
Christine du Fretay – Présidente, e-enfance
Hon Mozelle W Thompson, Thompson Strategic Consulting, Facebook
Catherine Borrel, IAB Europe
Michele Ybarra, Internet Solutions for Kids
Dieter Carstensen, Project Manager, Save the Children Denmark
John Carr, UK's Children's Charities' Coalition on Internet Safety
Professor Dr Herbert Burkert, University of St Gallen
Professor Dr Urs Gasser, University of St Gallen
Annie Mullins, Global Head of Content Standards, Vodafone

# Table of Contents

# I. About these Principles

The providers of Social Networking Services (SNS) listed at the end of this document share a common goal to maximise the benefits of the internet while managing the potential risks to children and young people. In order to protect children and young people[1], individual companies have developed and continue to evolve safety strategies. In addition, many providers have been heavily involved in multi-stakeholder and cross industry dialogues within the EU aimed at establishing and sharing good practice. These include the *UK Home Office Task Force on Child Protection on the Internet*[2], the *Human Rights Guidelines for Internet Service Providers*[3] developed by the Council of Europe in co-operation with the European Internet Service Providers Association (EuroISPA) and educational projects such as *Teach Today*[4]. Similar activity is also underway in countries outside the EU[5].

These Principles have been developed by SNS providers in consultation with the European Commission, as part of its *Safer Internet Plus Programme*, and a number of NGOs, 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. SNS providers often operate in multiple territories across Europe and the rest of the world and welcome the opportunity to establish pan-EU principles in this area.

The document 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 those principles. The guidance is not intended as a 'one size fits all' solution. It is recognized that the communications and internet industry is very diverse and ranges from large global providers to smaller locally run services. SNSs vary greatly in terms of the type of service, the platforms on which they can be consumed, their user demographics, the markets in which they operate and the jurisdictions in which they are based. All of these factors affect the levels and types of risks that are attendant to those services and the strategies that may be appropriate and reasonable to address such risks.

Accordingly, in determining their own safety strategies, providers supporting these principles take into account the particular nature of their services in order to apply the relevant recommendations of these Principles. Therefore, while providers will support all seven Principles, it is for each provider to judge where and how far to apply the document's specific recommendations. These Principles are aspirational and not prescriptive or legally binding, but are offered to service providers with a strong recommendation for their use.

---

[1] For the purposes of this document, the term "children and young people" refers to legal minors. Depending on the jurisdiction in which the service is offered and the applicable law, this refers to users under 18 years old or under 16 years old.

[2] http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance?view=Binary. The Home Office Task Force's good practice has now been integrated in to the work of the UK Council for Child Internet Safety.

[3] http://www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf(2008)009_en.pdf

[4] www.teachtoday.eu.

[5] For example, a number of social networking providers worked with the US Internet Safety Technical Task Force to investigate the role technology could play in the protection of children and young people on the internet. See http://cyber.law.harvard.edu/research/isttf/documents

These Principles sit alongside ongoing multi-stakeholder dialogues, in the EU and elsewhere, which collectively aim to shape a consistent and complementary framework on which providers can build and develop strategies to protect children and young people. Providers' application of the Principles, the relevance of this document and the good practices it engenders will be evaluated as outlined below, in consultation with the European Commission and other stakeholders.

These Principles are intended to provide guidance to 'Social Networking Services' which are available to children and young people[6]. In the context of these Principles, the term refers to online services that combine the following features:

- 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.

Social Networking Services can be accessed using a range of platforms. The capabilities of individual platforms may vary and a provider may not be able to make available the same features on all platforms. Services can also be available as downloadable applications. Where practicable, providers will endeavour to work within the limitations of these platforms and delivery mechanisms to consider these Principles when their services are distributed in this way.

Increasingly, Application Programming Interfaces (APIs) are a feature of SNSs, harnessing the open, distributed and collaborative nature of the internet. APIs allow third party developer companies to create 'applications' and, in some cases, users can add such applications to their SNS profile, providing them with added utility and functionality. Because applications are a new and evolving feature of SNSs and because the nature of the relationship between application developers and the SNS varies from case to case, SNSs can offer differing levels of assurances to their users in terms of these Principles. These levels of assurances will be outlined in a guidance note in Annex 1.

---

[6]  Subject to age restrictions defined by the service provider.

# II. Background

*Understanding potential risks to children and young people on Social Networking Services*

The internet, along with other new technologies, has brought citizens and consumers enormous benefits over the past fifteen years, in terms of communication, information, e-commerce and entertainment. The latest wave of technologies, grouped as 'web 2.0 technologies', which includes SNSs, has triggered further evolution in the way people, especially young people, communicate with friends, access entertainment and engage with communities of interest.

As with many products and services, the misuse of these technologies can present an element of potential risk to children and young people. SNS providers must assess if and how these potential risks apply to their own services. Potential online risks to children and young people fall into four categories:

- 'Illegal content', such as images of child abuse and unlawful hate speech

- 'Age-inappropriate content', such as pornography or sexual content, violence, or other content with adult themes which may be inappropriate for young people.

- 'Contact', which relates to inappropriate contact from adults with a sexual interest in children or by young people who solicit other young people.

- 'Conduct', which relates to how young people behave online. This includes bullying or victimisation (behaviours such as spreading rumours, excluding peers from one's social group, and withdrawing friendship or acceptance) and potentially risky behaviours (which may include for example, divulging personal information, posting sexually provocative photographs, lying about real age or arranging to meet face-to-face with people only ever previously met online).

With the interactivity that web 2.0 technologies enable, it is also important to remember that in addition to being victims young people can also initiate or participate in anti-social or criminal activities.

*Safer Social Networking: a multi-stakeholder collaboration*

There are a wide range of stakeholders with a role to play in managing potential risks to children and young people, including online service providers, governments, parents, teachers, users and non-governmental organisations. To date, the experience of managing potential risks from the misuse of various aspects of the internet has shown that the most effective approach is for stakeholders to consult and collaborate with other stakeholders, in addition to performing their own roles. These Principles promote this multi-stakeholder collaboration as the most effective way to manage potential risks on SNSs.

SNS providers that allow either children or both young people and adults to subscribe to their service, have a responsibility to ensure that they have assessed their site for potential risks and put in place appropriate measures and tools designed to mitigate those risks. This document is intended to outline the principles that providers should consider in order to fulfil this responsibility.

In order to set the context for these guidelines, it is useful to briefly outline the roles that other stakeholders play in promoting online safety and how SNS providers can work collaboratively with them.

- **Parents, teachers and other carers:** have an important role to play in both educating and fostering an ongoing dialogue with children and young people in their care about safe and responsible online behaviour. Service providers should provide targeted, easily-accessible and up-to-date information and tools to assist them in doing so. Providers should also explore ways to work with educators, governments and other stakeholders to create resources and other educational vehicles.

- **Governments and public bodies:** should provide children and young people with the knowledge and skills to navigate the internet safely. Governments should ensure that e-safety curricula that accurately reflect current internet services and behaviours are delivered in schools. Governments should also ensure that law enforcement agents and those working in the criminal justice system are equipped with the appropriate training, tools and resources necessary to effectively combat criminal activity conducted online. Governments should work together to ensure that the frameworks for cross-border coordination are effective and efficient[7].

  It is important that all stakeholders, including governments and public bodies, understand new challenges and opportunities as they emerge from the rapidly evolving online space. Service providers can assist governments in maintaining this understanding, and should explore ways to work with governments.

- **Police and other law enforcement bodies:** should ensure that officers have appropriate and relevant training and resources for investigating and prosecuting the illegal use of online services. SNS providers and law enforcement bodies should work collaboratively to share their knowledge of social networking and to support investigations in line with applicable laws.

- **Civil society:** as a whole, and through bodies such as child protection agencies, youth organisations and, counselling services, should collaborate with SNS providers and governments through consultation, dialogue or working groups that address their mutual target groups and challenges online. Increasingly, social networking platforms are being harnessed by mental health, social care and support organisations to raise awareness, educate and to deliver counselling and support to young people online, a development which potentially has many positive outcomes[8]. However, it is important that support

---

[7] For example, Mutual Legal Assistance Treaties (MLATs), which exist between countries and allow for information and other assistance from private and public sources to be shared across borders for the purposes of official investigations and prosecutions.

[8] Providers will pay due regard to good practice recommendations for support service provision within SNS environments being developed in other forums such as www.technologyforwellbeing.ie

organisations conduct a thorough review of a range of issues including how best to uphold essential ethical and professional practices concerning client welfare, confidentiality, competence, responsibility, and integrity when they are considering delivering services from within a social networking environment.

- **Users themselves:** adults, young people and children should at all times respect a service's terms of use and/or community guidelines. They should also make good use of the education, tools, settings and reporting mechanisms designed to encourage them to play their own role in managing the community to which they belong.

# III. Safer Social Networking Principles

***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 of Service.

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 audience[9]***

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[10-11]. Service providers should seek to limit exposure to potentially inappropriate content and contact. Measures that are available or appropriate to each service will vary in each case[12], but may include for example:

- making clear when services are not appropriate for children and young people or where a minimum registration age applies;

---

[9]  The intended audience as outlined in each  providers' Terms of Service

[10] The intended audience as outlined in each  providers' Terms of Service

[11] Each 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.

[12] The 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 principal market.

- 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 the means for content providers, partners or users to label, rate or age restrict content where appropriate[13];

- 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 18[14] are not searchable;

- setting the default for full profiles to 'private' or to the user's approved contact list for those registering under the age of 18[15] (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;

---

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

[14] 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.

[15] 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

- 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 controls[16]) 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.

### Principle 5: Respond to notifications of Illegal content or conduct

Upon receipt of notification of alleged illegal content or conduct[17] 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).

---

[16] 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

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

### 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 times[18].

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.

### Principle 7: Assess the means for reviewing illegal or prohibited[19] content/conduct

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.

There is a range of procedures which can be used to promote compliance with the Terms of Service, 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 frameworks[20] 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.

---

[18] 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.

[19] Prohibited content/conduct as defined by Terms of Service, Acceptable Use Policy and/or House Rules

[20] 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

# IV. Evaluating the Safer Social Networking Principles

Providers supporting these Principles are committed to implementing safety practices and support all seven Principles outlined in this document. These providers will assess the risk of potential for harm to children and young people on their service, and will consider the application of the specific recommendations outlined in this document accordingly.

- In the interests of transparency, these providers will self-declare[21] how they have considered the Principles which are relevant to their services. These providers will provide the European Commission with this self-declaration.

- Providers will make available for publication non-confidential information from their declaration about their consideration of these Principles.

- Providers supporting these Principles will reconvene after eighteen months with other stakeholders to:

    - Review trends in safety policies and practices.

    - Update stakeholders on the evolution of communication technologies.

    - Review user behaviour and associated risks to users.

    - Review and revise the document where appropriate to ensure that it remains relevant and up-to-date and that it reflects developments in online safety practice.

    - Assess the effectiveness of the document.

- Providers supporting these Principles and other stakeholders will work together to encourage other social networking service providers to add their support to this document and its objectives. They will also endeavour to raise awareness of these goals more widely to interested stakeholders, including users.

---

[21] A common self-declaration format will be developed and used by all providers.

# V. Annex I

*Explanatory note on how these Principles may apply to applications*

As outlined in the introduction, applications are increasingly a feature of SNSs. There are three categories of applications, which are broadly defined by the relationship that exists between the application and the SNS. This relationship determines how a provider can apply these Principles, as follows:

1. Applications which are pre-installed, integral to or hosted and sponsored by a SNS and made available by the SNS provider. In these instances, there may be a relationship between the SNS and the application developer. In the context of this category of applications, providers should consider the following:

   - undertake a risk assessment of the potential for harm to children and young people, the goal being compliance with the site's policies and safety and security good practice guidelines;

   - include relevant advice for children and young people in educational material (e.g. 'Help pages');

   - respond appropriately upon receipt of reports regarding an application's non-compliance with the site's policies.

2. Applications which have been created by third party developers and which are displayed on the SNS's Open API platform. The SNS's users can choose to install these applications on their profiles. There is generally a limited relationship between the SNS and the application developer in this instance. In the context of this category of applications, providers should consider the following:

   - make reasonable efforts to raise awareness among third party developers of industry good practice (which includes these Principles and similar initiatives);

   - include relevant advice for children and young people in educational material (e.g. 'Help pages') and make users aware that a third party application may not afford the same protections as users expect on the SNS in question;

   - upon receipt of notification that an application available to children and young people is in breach of the provider's policies, SNS providers will, where appropriate, notify the developer of the situation, and at all times reserve the right to take down applications which break the provider's policies.

3. Applications which are available from a gallery of third party applications on a platform other than the SNS provider's platform. Users can choose to install these applications on their SNS profile. There is typically no relationship between the SNS and the application developer in this instance. In the context of this category of applications signatory companies should consider the following:

- include relevant advice for children and young people in educational material (e.g. 'Help pages') and make users aware that a third party developer may not afford the same protections as the SNS in question;

- upon receipt of notification that an application available to children and young people is in breach of the provider's policies, SNS providers will, where appropriate and possible remove the link to the application.

# VI. Annex II Self-declaration Form

## EU SNS Safer Social Networking Principles
## Self-declaration Form

*In the interests of transparency, providers supporting the EU Safer Social Networking Principles agree to self-declare how they have considered the Principles in relation to the Social Networking Services they offer, using the form below.*

**1. About the Social Networking Service(s)**

The following is a brief outline of [the company making the] declaration, including a short description of the services it offers that fall into the category of "social networking" as outlined in the Principles.

**2. How has the company considered these services in relation to the Principles?**

The following is an outline of how [company] has considered the EU Safer Social Networking Principles in relation to its Social Networking Service(s). This section will make reference to the recommendations made in the Principles document, where they are applicable and outline how they are applied.

| **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** |
| --- |
| |

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

**Principle 3:  Empower users through tools and technology**

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

**Principle 5: Respond to notifications of Illegal content or conduct**

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

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

### 3. Other information

This section provides an outline of any other information that is relevant with regards how the company has considered the Principles.