

MICROSOFT Windows Live

EU SNS Safer Social Networking Principles Self-declaration Form

5th November 2010

In the interest 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. Microsoft hereby submits this updated self-declaration as of 5th November 2010.

1. About the Social Networking Service(s)

Founded in 1975, Microsoft (NASDAQ:MSFT) provides software, services and solutions that help people and businesses realise their full potential. We operate in all EU Member States and elsewhere in Europe.¹

Windows Live, a business group of Microsoft, offers a collection of free PC programs, web services and mobile services for web-enabled mobile devices that helps people stay in touch and keep their online lives organized in one place.

In September 2010, Microsoft launched the latest version of Windows Live software and services, including Windows Live Messenger, Windows Live SkyDrive, and Windows Live Family Safety. Windows Live Messenger is an instant messaging service with over 300 million active users. From the Windows Live Messenger or from the Windows Live Profile page, users can share personal status messages with their network and connect with friends and family on Windows Live and other online services, like MySpace and Facebook. With Windows Live, users can also use Windows Live Skydrive or Windows Live Messenger to share photos and videos with friends and family.

Windows Live also includes non-social networking services and applications like:

- Windows Live Essentials is a suite of free programs for Windows PC. Windows Live Essentials includes Family Safety, which provides tools for parents to monitor their children's activities

¹ http://www.microsoft.com/presspass/inside_ms.mspix;
<http://microsofteurope.eu/MainHome/MicrosoftinEurope.aspx>.

online and whilst using Photo Gallery, Movie Maker, Mail and Mesh;

- Windows Live Hotmail is one of the world's largest email providers with more than 350 million active accounts, via the web, a mobile phone or a PC.

Windows Live is available at <http://explore.live.com/home>.

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

The following is an outline of how Microsoft has considered the EU Safer Social Networking Principles in relation to its social networking features.

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

Providing Education:

- All users must review and accept the Microsoft Service Agreement (also known as our "Terms of Use"), which incorporates the Windows Live "Code of Conduct" and our Privacy Statement when they register to use the service;
- There is a link to the Terms of Use and Privacy Policy on the sign-in page;
- Once users are signed into the service, from Windows Live Profile, users can update their Profile information, change their privacy settings or choose to connect their other services to Windows Live;
- There is a "Terms of Use" link on every page;
- There is a "Privacy" link on every page;
- There is a "Code of Conduct" is available from every page;
- The Windows Live service also includes a "Code of Conduct" that applies to any parts of the service that allow consumers to post or share content with others. It defines various prohibited uses of the Windows Live services;
- The Windows Live web services include a "Report Abuse" button on pages where users can post, share or view other users' content;

- From the Windows Live icon on every page of the service, users can access “All Services”. From the “All Services” page, users can use Windows Live “Family Safety” features in Windows Live or click the “Learn More” link to learn more about how Windows Live Family Safety works to help parents protect their children online. See <http://explore.live.com/windows-live-family-safety?os=other>;
- Windows Live Family Safety settings are provided for free as part of the Windows Live Essentials. “Family Safety” is part of both the Windows Live web services and PC programs. To use “Family Safety”, consumers download and install “Family Safety” on each computer their children use. Parents or guardians can control their children’s Windows Live settings by using the “Family Safety” website from any computer;
- The Windows Live Help Centre provides a FAQ on our privacy settings.

Providing Education – Corporate (for all Microsoft services)²:

- Microsoft’s primary online safety education site is centralised and is broadly available to all consumers. This “Protect site” can be found at: www.microsoft.com/protect and is available in every EU member state in their local language;
- Microsoft makes fact sheets, white papers and how-to safety guides available for free to consumers, policymakers and employers on safer internet practices here: <http://www.microsoft.com/protect/resources/brochures.aspx>;
- Microsoft makes aged-based online safety guidance and other tips specifically for parents and guardians available at: <http://www.microsoft.com/protect/familysafety/childsafety.aspx>;
- Microsoft produces online safety guidance specifically for educators: <http://www.microsoft.com/downloads/en/details.aspx?FamilyID=4F413D00-52B8-4ABA-B6D8-6B9427BE87C3&displaylang=en>;
- Microsoft conducts and publicises research on critical safety issues, including this recent study on Online Reputation conducted in the UK, France and Germany: <http://www.microsoft.com/privacy/dpd/research.aspx>;
- Microsoft recently conducted additional research on safer social networking use and refreshed its safer SNS guidance here: <http://www.microsoft.com/protect/parents/social/socialnet.aspx>;

² The following information is not accessible via Windows Live.

- Microsoft conducts global quarterly safety education around a broad range of safety topics to generate awareness, including specific guidance around safer social networking, and participates in major global privacy and safety awareness events, including Data Privacy Day and Safer Internet Day. Please see: <http://www.microsoft.com/privacy/sid/>;
- Microsoft provides a monthly safety and security newsletter for parents and consumers: <http://www.microsoft.com/protect/resources/newsletter.aspx>;
- Microsoft provides a safety and security tips blog: <http://blogs.msdn.com/b/securitytipstalk/>;
- Microsoft has an online safety channel on YouTube: <http://www.youtube.com/MSFTOnlineSafety>;
- Microsoft educates Twitter users on safety at http://twitter.com/Safer_Online;
- Microsoft UK makes available a parent's guide to online safety education: <http://www.microsoft.com/uk/citizenship/safeandsecure/parentadvice/default.aspx> and delivers "ThinkUKnow" safety presentations to parents, teachers and care givers;
- Microsoft has education partnerships with a broad range of partners, including the National Centre for Missing and Exploited Children, Netsmartz, iKeepSafe, iSafe, the National Cybersecurity Alliance, WebWiseKids, Enough is Enough, the Safe Internet Alliance, LookBothWays, Wired Moms.com and Web Wise Kids.

General social networking tips: <http://www.microsoft.com/protect/parents/social/socialnet.aspx>

Kid-specific social networking guidance:

<http://www.microsoft.com/protect/parents/social/kidssocial.aspx>.

Partnering with Non-Profit Organizations and Governments:

Microsoft partners with organisations and task forces worldwide to help further our joint interest in making the Internet and online services safer for children and families. Some of our partnerships are highlighted here: <http://www.microsoft.com/protect/community.aspx>. Other notable partnerships in Europe and elsewhere are noted below:

- Microsoft works in partnership with European Schoolnet and INSAFE;
- Microsoft and the Council of Europe have partnered on the Cybercrime Project to help

eradicate cybercrime and child exploitation;

- We have a broad-reaching partnership with the National Centre for Missing and Exploited Children (NCMEC) and the International Centre for Missing and Exploited Children (ICMEC) including a recent donation of our PhotoDNA technology to track down paedophiles;
- Microsoft is a financial guarantor of INHOPE, the International Association of Internet Hotlines, and has been a partner since 2005;
- Microsoft is a partner with ICMEC and other technology and financial institutions in the Financial Coalition Against Child Pornography;
- In 2004, Microsoft, Interpol and ICMEC joined in partnership for the Global Campaign Against Child Pornography to train law enforcement officials around the globe;
- Microsoft is an active participant in the global Technology Coalition Against Child Pornography
- Microsoft is a supporter of the Virtual Global Task Force and partners with the UK's Child Exploitation Online Protection (CEOP) and the Australian Federal Police in the ThinkUKnow online safety education program;
- Microsoft has joined in partnership with numerous European NGOs on safety education campaigns including: Child Focus Belgium, Nobody's Children Foundation, Helpline, Click.de, NGO Safer Internet Austria, Save the Children, Garda, ChildNet, Italiano Genitori, amongst others;
- Microsoft Poland and the Nobody's Children Foundation recently received an award for the "Best Educational Initiative of the Year" from the President of Poland for the "3...2..1..Internet Safety Curriculum";
- Microsoft has participated in numerous task force efforts around online safety including the Internet Safety Technical Task Force, the Online Safety Technology Working Group, the UK Council for Child Internet Safety (UKCCIS) and the EU Safer Social Networking Task Force, and;
- Microsoft is a signatory to the EU Safer Social Networking Principles.

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

Complying with local law related to parental consent and verification for children:

- The Windows Live services are general use services and are not primarily directed at children under the age of 18;
- Because our services are provided world-wide, Windows Live complies with the laws of various countries that require parental consent and verification before children under a certain age may use the services;
- We place a session cookie on the registration page, so prospective users cannot change their age if the initial age is below the age required in a specific country for age verification;
- Microsoft's Privacy Policy also (1) describes its information practices for children's personal information; (2) provide parents with access to their child's personal information; (3) maintains the confidentiality, security, and integrity of information collected from children, among other things; (4) provides parents a choice about whether the child's information may be shared with 3rd parties, and (5) give parents the ability to delete the information and opt out of future collection of the child's information.

Protecting Users from Inappropriate Content:

- All hosted images are reviewed by use of filters to detect pornography;
- Users are prohibited from upload, post, transmit, transfer, distribute or facilitate distribution of any content (including text, images, sound, video, data, information or software) or otherwise use the service in a way that:
 - Depicts nudity of any sort including full or partial human nudity or nudity in non-human forms such as cartoons, fantasy art or manga;
 - Incites, advocates, or expresses pornography, obscenity, vulgarity, profanity, hatred, bigotry, racism, or gratuitous violence;
 - Provides or creates links to external sites that violate this Code of Conduct;
 - Is intended to harm or exploit minors in any way;
 - Is designed to solicit, or collect personally identifiable information of any minor

(anyone under 18 years old), including, but not limited to: name, email address, home address, phone number, or the name of their school;

- Is illegal or violates any applicable local and national laws; including, but not limited to child pornography, bestiality, incest, illegal drugs, software piracy, and harassment, among other things.

In all contractual agreements related to use of or integration with Windows Live, partners accept the responsibility to comply with our Terms of Use, Code of Conduct and Privacy policy.

Principle 3: Empower users through tools and technology

Windows Live Family Safety:

As part of our larger effort to provide a safer way for children and families to use the web, we spent a lot of time thinking about how to best balance control with simplicity in the new version of Windows Live Family Safety. In particular, we understand that parents are facing new challenges around what information their children access over the internet, who they meet, and what kind of conversations they have. With that in mind, we designed the new Family Safety to help parents empower their children online, while providing simple controls to monitor and protect their children when needed.

We're doing this by focusing on three core areas:

- Safer social networking;
- Safer searching across all major search engines, and;
- Safer browsing with enhanced filtering choices.

Safer social networking:

- As a parent, knowing who are your child's online friends is just as important as knowing whose house they are hanging out at. Parents and guardians can use Windows Live Family Safety to manage their child's contact list so that only people they added to their child's contact list may send them email or instant messages. As children become older, parents may allow them to

manage their own contact list, but can still use the contact management feature to see their children's new contacts and ask about their new friend, just as they would about a new friend at school. This works with both Windows Live Messenger and Hotmail;

- In addition, Family Safety also offers web filtering settings that have the ability to filter out social networking sites. So, if a parent's child is too young to be on Facebook or other similar sites, parents can block or restrict their access to them. It is important to note that children do not need a Windows Live ID to use Family Safety – all parents need is the local Windows account that their child uses;
- Parents and care givers can also use Windows Live Family Safety to allow access to a small number of websites which they have personally reviewed, so that parents know where their children can go and what private data they might be able to share.

Safer searching:

Over the past year, we have seen most of the popular search engines introduce Safe Search features to help users avoid inappropriate content for both themselves and their children. All of the sites have different ways of turning on the lock, and parents might not use the same search engine their children do. If parents have web filtering turned on in Family Safety, safe search will be used automatically for many of the popular search engines that have a lock, so that parents ensure their children would not accidentally encounter inappropriate content while searching on these search engines.

We currently support search engines on Bing, Google, Yahoo, Ask, Yandex, Virgin Media, and Mail.ru.

Safer ads in Windows Live:

A lot of the ads on the internet are inappropriate for children, and we are doing something about it in Windows Live. If parents add their child's Windows Live ID to Family Safety, we would not show any paid advertisements on live.com websites when your child is logged into Windows Live.

Child-friendly websites:

We also provide a child-friendly web setting, which lists about 8,000 sites that have been reviewed and determined to be designed for and safe for children of all ages. Windows Live users can use Bing to

search across all the sites from the children's page in Windows Live Family Safety. The link can be found here: <http://fss.live.com/kids/>.

Users under 18:

Windows Live services have additional default settings for our younger audiences:

- Profiles of users registered as under the age of 18 are not searchable (Note: Individuals with no age listed in their Profile are not considered under 18);
- The default permission setting for Windows Live accounts where the user identifies themselves as under 18 is set to "friends" which only allows contacts that the users has added to view their information;
- Users under 18 may change their default settings.

Providing Tools for All Windows Live ID Accountholders:

- All users can set their profile or photos to private; users choose how public or private they want to make their accounts;
- All new user profiles are automatically set to limited (only friends see a user's activity and information; the user's profile is available via a public search);
- When users visit their profile, they see their own view of their profile, which includes all of the information they have entered about themselves and lists all of their activities;
- Users decide who is allowed to see each piece of information on their profile, including their last name, e-mail address, mobile number, profile picture, age, and occupation and so on;
- When a user signs in to his or her Windows Live account, a general message appears on the profile encouraging the user to learn more about the privacy settings, options and managing permission;
- Users can:
 - Block other users from contacting them;
 - Change or conceal their online status;
 - Allow access to everyone, their own network, and certain groups of friends or only certain individuals;
 - Specify who can post and view comments on their shared photos, files, blog posts or

guestbook;

- Specify who can tag people in the photos they share and which other people can tag them in photos;
 - Create a manually selected list of allowed instant messaging contacts and be notified whenever someone tries to add them to their Messenger Contacts list;
 - Set their personal account filters so Windows Live Hotmail will deliver mail only from people in their contacts list and trusted senders;
 - Can block all e-mail from a particular e-mail address.
- The service identifies, based on colour-coded alerts, whether an incoming message might be malicious or fraudulent.

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

Reporting Inappropriate Content:

- For services where users can view, post or share user-generated content within Windows Live, we provide a “Report Abuse” link that is accessible at the bottom of web pages. For example, a “Report Abuse” link is available for Windows Live Profile, Photos, SkyDrive, Spaces, Documents and Groups;
- Users can “Report Abuse” via the menu in Windows Live Messenger;
- Users can also access a report abuse link from the Windows Live Messenger application.

The Report Abuse mechanism was designed to ensure that the service handles priority abuse issues related to content users post or share via the Windows Live services. As such, we sought to ensure that issues of child pornography and child exploitation were flagged, reviewed and handled appropriately and that other priority safety fields were entered so that these could be responded to accordingly.

Beside predefined categories, we also encourage our users to provide as much detail as possible regarding the abuse or offensive behaviour to help our trained agents investigate the issue. We

respond to all types of abuse reports following standardised internal handling practices and operate a complaint centre where users anywhere in the world can report incidents of abuse on our sites.

Principle 5: Respond to notifications of Illegal content or conduct

- Microsoft’s online properties employ mechanisms for responding to notifications of illegal content or conduct, such as the “Report Abuse” link, and “Feedback” accessible from our services;
- We respond to reports of abuse, including those potentially involving illegal content or conduct, and work in close cooperation with law enforcement and government agencies in response to lawful request.

Partnering with Law Enforcement:

- We provide support for local, state, federal and international law enforcement in investigations and prosecutions, as applicable;
- We provide on-going training to cybercrime units on how to investigate and prosecute cyber law criminals using Microsoft software and services;
- Microsoft created Computer Online Forensic Evidence Extractor (COFEE), designed exclusively for use by law enforcement agencies. COFEE brings together a number of common digital forensics capabilities into a fast, easy-to-use, automated tool for first responders. Moreover, COFEE is being provided—at no charge—to law enforcement around the world;
- To help combat the growing number of ways that criminals use computers and the Internet to commit crimes, Microsoft is working with INTERPOL and the National White Collar Crime Centre (NW3C) to provide COFEE at no cost to law enforcement agencies in 187 countries worldwide.

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

Microsoft’s Online Privacy Statement is available from the relevant pages within the Windows Live

services.

We design our privacy features with the following basic assumptions in mind:

- People care very much about their privacy;
- People want to control how much of their information is made public;
- People want simple, intuitive options to control the publishing of their information;
- Privacy controls need to be flexible to accommodate different privacy needs;
- Privacy controls need to allow individuals to set different levels of access for different contacts.

Information collected at registration is used to create a Windows Live ID. Other than the username selected for the Windows Live ID, the pieces of information in a profile remain separate, with no automatic mapping taking place.

With Windows Live profile, customers can choose from three settings:

1. Public: Everyone can see the customer's activity and information; and everyone can search and find a customer's profile;
2. Limited: Only friends can see the customer's activity and information; and everyone can search, find and see a customer's profile;
3. Private: Only friends can see the customer's activity and information; and no other people can search, find or see a customer's profile.

However, it's important to note that if a user comments on his/her friends' photos, posts or other activities, his comment along with his name and picture will be visible to people he may not be friends with.

Furthermore, across Windows Live, a user will see the following permissions choices (privacy selector):

- Everyone (public): the whole internet has access, and this content is findable via web search;
- My friends and their friends: includes all your friends and acquaintances, including those with limited access, plus all of their friends;
- Friends: includes all your friends and acquaintances, including those with limited access;
- Some friends: this excludes any friends whose access you've limited;
- Just me: no one but you has access.

For example, these options appear in the new permissions control for individual items like photo albums or shared documents.

Sharing with social networking sites (such as Facebook, LinkedIn and MySpace):

When a user set sharing of activities to “Friends”, “My friends and their friends”, or “Public”, those activities will be published to the user’s other connected services (like Facebook, MySpace, and LinkedIn). When any update from Windows Live appears on a connected social network, it will follow the privacy controls of that network.

This also works for Office documents, allowing you to publish Word, Excel, PowerPoint, and OneNote documents on your connected networks.

Choosing a default privacy setting:

- The user can use the privacy selector (see above);
- The privacy settings page can be visited at any time by clicking a link on the user’s profile page to view or change the privacy settings used as his default across Windows Live.

Advanced privacy settings:

- Clicking on Advanced on the Privacy settings page to find dozens of granular settings presented in an easy to understand layout;
- The advance settings page presents each privacy setting organized into categories, with sliders that allow you to set permissions from most restrictive to least restrictive.

For more information <http://www.microsoft.com/privacy/> or <http://microsoft.eu/Posts/Viewer/tabid/120/articleType/ArticleView/articleId/690/Giving-you-more-meaningful-choices-to-control-your-privacy.aspx>

See also Principle 2: Work towards ensuring that services are age-appropriate for the intended audience and Principle 3: Empower users through tools and technology for additional information.

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

- Microsoft allows users to identify and report issues that might violate our terms of use;
- We utilise a range of automated technologies to ensure the integrity of our services;
- When we become aware of a violation of our terms of use or code of conduct, we take prompt steps to remove and take down illegal or prohibited content/conduct;
- We have established global processes and standardised handling practices and trained personnel on those processes and practices to ensure we respond in a consistent manner and to meet all applicable laws and regulations worldwide related to this subject.

See Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the terms of service and Principle 5: Respond to notifications of illegal content or 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.

- In compiling this document, Microsoft EU has taken a cross-departmental approach in order to highlight the efforts we are making across our services.
- IT innovation is consistently evolving therefore Microsoft will continue to invest in online safety for its consumers.

Contact:

Mr. Ronald Zink

Chief Operating Officer EU Affairs and Associate General Counsel

Microsoft Avenue des Nerviens 85

B-1040 Brussels

ronz@microsoft.com

+33 1 57751179