Cooperative arrangement for complaints handling on social networking sites

Microsoft Corporation

In the interests of transparency, providers supporting the Cooperative Arrangement for Complaints Handling on Social Networking Sites agree to provide information on how they give effect to the Principles in relation to the social networking services they offer, using this form.

1. About the Social Networking Services

Since the advent of the Internet and online services, Microsoft has maintained that technology providers, governments, law enforcement, community organisations, and Internet users have a "shared responsibility" to promote a safer, more trusted online environment.

To that end, Microsoft takes a comprehensive approach to online safety that includes: (1) developing and deploying family safety technologies, (2) creating and enforcing strong governance policies, including responsible monitoring of our online services, (3) making available guidance and educational resources for families and children, and (4) partnering with others in industry, government, and within civil society to help combat online crime. These efforts align directly with Microsoft's overall commitment to promoting greater trust online, and to building products and services that enhance consumer safety.

For these reasons, Microsoft is pleased to become a signatory to the "Cooperative Arrangement for Complaints Handling on Social Networking Sites (SNSs)." Per the Arrangement preamble, Microsoft operates major online communications services with "SNS-like functionality," rather than a

discrete social network that facilitates "one-to-many" communications or community engagement within a "bounded system."[1]

Microsoft considers this functionality to include two primary consumer-facing services that facilitate broad, persistent and multi-modal interactions between users inside a single interface: (1) Xbox Live, and (2) Windows Services, formerly known as "Windows Live,"[2] which is now part of the Windows 8 suite of services.

Xbox LIVE is an online gaming and entertainment service that connects nearly 32 million members across 41 countries, including Australia. Use of the service requires an Xbox 360 console, as well as a broadband internet connection. Details about the service can be found at: http://www.xbox.com/en-AU/live/.

Windows Services, now part of Windows 8, offers a collection of free PC programs, and web and mobile services for web-enabled mobile devices, that helps people stay in touch and better organise their digital lifestyles. Windows Services are used by more than 500 million people every month and include: Hotmail, the world's leading web email service with 350 million active users, and SkyDrive, a cloud-based storage service, which has more than 130 million users.

Windows Services also include other, non-social networking services and applications, namely Windows Live Essentials, a suite of free programs for Windows PC. Windows Live Essentials include Family Safety, which provides tools for parents to monitor their children's activities online. Additional information on Windows Services is available at: http://windows.microsoft.com/en-AU/windows-8/meet.

---

[1] To that end, Microsoft considers the scholarly definition of "social networking site" to be applicable in this context: *"We define social network sites as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site ….''Networking'' emphasizes relationship initiation, often between strangers. While networking is possible on these sites, it is not the primary practice on many of them, nor is it what differentiates them from other forms of computer-mediated communication (CMC)."* ***Social Network Sites: Definition, History, and Scholarship:*** danah m. boyd and Nicole B. Ellison, Michigan State University, 2007; Page 1. http://mimosa.pntic.mec.es/mvera1/textos/redessociales.pdf

[2] It is important to note that Windows Live Spaces, Microsoft's former blogging and social networking platform, was decommissioned in 2010.

2. How will the provider give effect to the complaints handling aspect of the Cooperative Arrangement?

1. Policies for Acceptable Use
Xbox Live The "Terms of Use" for Xbox LIVE are available on the Xbox 360 console and on the Xbox Live website (http://www.xbox.com/en-US/Legal/LiveTOU). Users must abide by these Terms of Use, as well as the Xbox LIVE usage rules (http://www.xbox.com/usagerules) and the Code of Conduct (http://www.xbox.com/en-AU/Live/LIVECodeofConduct). Similar to Windows Live, there are easily discoverable "Terms of Use," "privacy," and "Code of Conduct" links on every page of the Xbox LIVE website (http://www.xbox.com/en-AU/Xbox360/index). Xbox LIVE users may report Code of Conduct violations (or "abuse") directly through the Xbox 360 console. When Microsoft becomes 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. Microsoft also provides users with clear guidance on how to identify and report issues that might violate our Terms of Use or Code of Conduct (http://www.xbox.com/en-au/live/abuse). In fact, the European Commission found in its evaluation of Xbox Live as part of the EU Safer Social Networking Services Principles effort that, "*The Xbox Live Code of Conduct which applies to both the console and the website is a clear and succinct statement of the standards of behaviour and content required of its users. Players can easily report violations of the code and Xbox Live undertakes to review every complaint filed*." **Windows Services** All users are prompted to review and must accept the Microsoft Service Agreement (also known as our "Terms of Use"), which incorporates the Windows Services "Code of Conduct" and our Privacy Statement both of which are encountered when consumers register to use the service. There

are also links to the Terms of Use and the Privacy Policy on the sign-in page.

To heighten discoverability, there are "Terms of Use," "privacy," and "Code of Conduct" links on every page. The Windows Services Code of Conduct applies to all parts of the service that allow consumers to post or share content with others. It defines various prohibited uses of the Windows Services.

2. & 3. Complaints Mechanisms and Review Processes

We share the Australian Government's view that online service and platform providers need to ensure that there are discoverable, easy-to-use report-abuse mechanisms backed with thorough review processes and robust moderation. To that end, our Customer Service and Support (CSS) organization of several hundred includes a sizable team dedicated to handling customer reports of abuse. This team is comprised of agents, who are trained to handle abuse reports and make referrals to law enforcement as appropriate.

Microsoft reports images of apparent child pornography on its sites to the National Center for Missing & Exploited Children (NCMEC), removes them, and bans the individuals or entities responsible for publishing them from using our services. We also operate an international complaint center where users can report incidents of abuse on Microsoft websites. Our safety experts moderate use of the company's online services and web properties to address illegal activity and content that violate the established terms of use—including child pornography, violent images, and hateful messages.[3]

XBOX Live

Microsoft's online properties employ mechanisms for responding to notifications of illegal content or conduct, such as the "Report Abuse" link,

[3] Because this important work requires our trained online safety agents to view highly objectionable material on a daily basis, Microsoft has established a "Wellness Programme" specifically for these employees. Services include one-to-one counseling, monthly group discussions, and a 24-hour crisis hotline. The program has been instrumental in helping Microsoft retain a pool of dedicated online safety experts and in strengthening our efforts to combat child exploitation.

and “Feedback” accessible from our Xbox Live 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 requests.

Microsoft allows Xbox and Xbox Live users to identify and report issues that might violate our terms of use and 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 or /conduct. We have established global processes and standardised handling practices, and have trained personnel on those processes and practices to ensure we respond in a consistent, lawful manner in all instances.

Investigation into a complaint in this regard may lead to the suspension or banning of an offending player from XBox Live. This process is detailed at http://support.xbox.com/en-AU/xbox-live/account-banning-and-player-feedback/account-suspensions-and-console-bans.

Xbox LIVE provides two mechanisms that allow users to manage interaction with other users and report inappropriate content or behaviours. In the first instance, users can select the profile of someone they are playing a game with or have recently played against and mute that player’s communication. Or, they can select other options to help block further interactions with that person.

We provide facilities for users to complain about another user’s content or behaviour, including profile content, language, cheating and “griefing” (making it hard for others to play, such as by driving a race car backward and crashing into others).

The Xbox LIVE Services Enforcement team reviews each complaint for accuracy (to determine, for example, whether the complaint is merely an attempt to get good players off the system). If the complaint appears to be legitimate, the Enforcement team can take the following actions:

- Mute the offender;
- Suspend the offender for a day, a week, or some other period of

time;

- Ban the offender's account from Xbox LIVE permanently;
- Ban the offender's console from Xbox LIVE permanently;
- Report egregious, potentially criminal offenses to law enforcement;
- Provide information for individuals to directly report potentially criminal activity to law enforcement. We have also deputised certain trusted, non-Microsoft, individual players to report on our behalf when they encounter inappropriate behaviour on our services. Their reports automatically lead to a service penalty for that offender appropriate for the severity of the offense.

It is worth noting that other online services operated by Microsoft have similar capabilities for users to register complaints online or by contacting Microsoft via phone, email, or chat. Such instances are generally handled through Microsoft's local support channel with full details available at http://support.microsoft.com/?ln=en---au.

Reporting Inappropriate Content on Windows Services

For services where users can view, post, or share user-generated content within Windows Services, we provide a "Report Abuse" link that is accessible at the bottom of the web pages. For example, a "Report Abuse" link is available for Windows Services Profile, Photos, SkyDrive, and Documents and Groups.

These Report Abuse mechanisms were designed to ensure that services prioritize content-related abuse reports, particularly those involving content that users post or share via Windows Services. As such, we sought to ensure that issues of child pornography and child exploitation are flagged, reviewed, and handled appropriately, and that other priority safety fields are entered so that these could be responded to accordingly. In addition to designating pre-defined categories, we encourage users to provide as much detail as possible regarding the alleged abuse/offensive behaviour to assist our agents in their investigation. We respond to all

types of abuse reports following standardized, internal handling practices, and operate a complaints centre where users anywhere in the world can report incidents of abuse on our sites.

4. Child Abuse Material (CAM)

Microsoft takes the matter of abuse reporting, and especially matters of potential child exploitation, very seriously. We have been strong advocates for child safety and responsible industry leaders participating in the eradication of child pornography for the past two decades.

Like other service providers, Microsoft reports images of apparent child pornography on its sites to the National Center for Missing & Exploited Children (NCMEC), removes them, and terminates any accounts containing these images. NCMEC, in turn, manages a data base of all reported child pornography (CP) both inside and outside of the United States. NCMEC has established ties with Australian law enforcement and works through the U.S. Immigration and Customs Enforcement Agency (ICE) to refer apparent Australian child abuse images or activity to local law enforcement.

As noted above, Microsoft has procedures and policies in place for removing child abuse material and appropriately notifying law enforcement. Microsoft remains committed to proactively identifying and removing child abuse material from the web, as evidenced by our work on the PhotoDNA Initiative, a technology used on Microsoft and other social networking sites to automatically identify child abuse material.

In 2012, Microsoft made PhotoDNA technology available free of charge to law enforcement to help with child sex abuse investigations, and further advance the fight against child pornography by empowering worldwide law enforcement to more quickly identify and rescue victims. PhotoDNA is a signature-based image-matching technology developed by Microsoft Research in partnership with Dartmouth College, which is already used by Microsoft, Facebook, and NCMEC for identifying known images of child pornography. Microsoft and our partner NetClean make PhotoDNA available to law enforcement via NetClean Analyze, through direct licensing and through the Child Exploitation Tracking System (CETS).

CETS is a technology-supported collaboration effort developed by Microsoft in conjunction with international law enforcement agencies that allows investigators to share and analyse information related to criminal acts such as possessing or distributing child pornography, kidnapping, and physical or sexual abuse. Being that child exploitation is a global crime, CETS is an

important facilitation and coordination tool, and is utilized by Australian law enforcement.

It is worth noting that Microsoft has had long-standing partnerships with a range of global organisations involved in the eradication of global child abuse images, including the International Centre for Missing and Exploited Children (ICMEC), Interpol, the Internet Watch Foundation, and the Virtual Global Task Force, which was recently chaired by the Australian Federal Police.

Notably in recent years, Microsoft, ICMEC, and Interpol jointly launched the International Training Initiative to educate global law enforcement officers on the latest techniques for investigating online child exploitation. Microsoft sponsored 36 training sessions worldwide for more than 3,100 law enforcement officers from 112 countries, including a well-attended in Brisbane in 2006.

Finally, Microsoft has partnered with the International Association of Internet Hotlines ("INHOPE") since its formation, by providing financial backing, technical training, and software license. To date, INHOPE consists of 33 member hotlines in 29 countries — including Australia's — that respond to reports of illegal content in an effort to make the Internet safer.

5. Identified Contact Person

Microsoft's local contact person is its Chief Security Advisor for Microsoft Australia.

6. & 7. Education and Awareness Raising & Collaboration with Government

Consumer education is a key pillar of Microsoft's online safety efforts, and we have created an extensive collection of resources and guidance on our Safety and Security Centre http://www.microsoft.com/en-au/security/default.aspx. Microsoft has partnered with hundreds of organisations around the world to deliver robust online safety awareness-

raising and educational materials, including the following:

- **Childnet International** (http://childnet-int.org/kia), a UK-based charity that helps educate teachers, parents, and young people about safe and positive use of the Internet through resources such as the "Know IT All" for parents guide.
- **Family Online Safety Institute** (www.fosi.org), an international non-profit organisation working to develop a safer Internet through education, public policy, education, and events.
- **GetNetWise** (www.getnetwise.org), a project of the Internet Education Foundation highlighting the latest web safety issues and teaching users how to steer clear of risks.
- **Internet Keep Safe Coalition** (www.ikeepsafe.org), a partnership of governors, attorneys general, public health and educational professionals, law enforcement, and industry leaders working together for the health and safety of youth online.
- **Netsmartz** (www.netsmartz.org), an interactive educational program of the National Center for Missing & Exploited Children (NCMEC) that provides age-appropriate resources to help teach children how to be safer online and offline.
- **OnGuard Online** (www.onguardonline.gov), a U.S. Federal Trade Commission website offering consumer tips, articles, videos, and interactive activities.
- **Stop. Think. Connect.** (http://safetyandsecuritymessaging.org), an international online safety campaign that promotes public awareness and safer behavior on the web.

Microsoft Australia is particularly proud of our ThinkUKnow (www.thinkuknow.org.au) partnership, which is both an educational programme and a significant collaboration with Government. ThinkUKnow is an Internet safety program, delivering interactive training to parents, caregivers and teachers through schools and organisations across Australia, using a network of accredited trainers. Originally created by the Child Exploitation and Online Protection (CEOP) Centre in the UK, ThinkUKnow Australia has been further developed by the Australian Federal Police (AFP) and Microsoft Australia, and is now proudly supported by ninemsn and

DATACOM.

Training sessions at local schools can be organised through the website. The ThinkUKnow site also provides a "Report Abuse" mechanism and supports the Australian Government's CyberSafety Help Button Initiative.

Microsoft has also partnered with the Australian Government on a range of initiatives to promote computing privacy, safety, and security, including support for National CyberSecurity Awareness Week since its inception. We have also been long-standing partners in the Australasian Consumer Fraud Task Force http://www.scamwatch.gov.au/content/index.phtml/itemId/694357, and have participated in Safer Internet Day and Data Privacy Day activities around the world for the past several years.

Last year, Microsoft's Data Privacy and Safer Internet Day efforts focused on promoting "digital citizenship." We recognise that responsible and appropriate use of technology by each individual promotes a safer, more trusted online environment for all individuals. Our "Fostering Digital Citizenship" whitepaper explores why digital citizenship matters; outlines the risks young people face online, and highlights what they and others need to do to stay safer online. Related to this, we commissioned research to build our understanding of consumer behavior, including a study on Online Reputation Management: Parents and Children 8–17, a Worldwide Online Youth Behavior Survey centered on the global prevalence of online bullying, and developed the Microsoft Computing Safety Index (MCSI), a catalog of more than 20 steps people can take to help avoid cyber threats. These and other research projects then guided us to develop the most comprehensive and effective materials to educate customers worldwide: our Digital Citizenship In Action Toolkit.

8. Continued Innovation

Microsoft is deeply committed to developing and deploying innovations that promote a safer, more trusted online environment. This is evidenced by our commitment to initiatives like PhotoDNA and the Child Exploitation Tracking System (CETS), and by fundamental innovations within our technology platform, such as SmartScreen in Internet Explorer, a feature

that helps detect phishing websites and helps protect against downloading or installing malware).

For instance, another Microsoft technology developed for law enforcement agencies, the Computer Online Forensic Evidence Extractor (COFEE), uses digital forensic tools to help investigators—including those with limited technical expertise—gather evidence of live computer activity at the scene of a crime. Computer files and activity logs retrieved using COFEE have helped law enforcement agencies build stronger cases against suspected spammers, identity thieves, child pornographers, and other cybercriminals. We are working with the National White Collar Crime Center and INTERPOL to make COFEE available free of charge to law enforcement investigators in 187 countries, including Australia.

As part of our efforts to thwart cybercriminals and help legitimate users more easily determine whom to trust online, Microsoft is also developing stronger digital identity verification technologies and protocols, and collaborating with others to generate ideas for advancing trust. For more details about this work, please visit: www.microsoft.com/mscorp/twc/endtoendtrust/default.aspx.

But ultimately, our technology innovations are designed for consumers, to help enable them to be in control of and manage their online experiences as safely as possible. One area where we have invested significant technical and market research is parental controls, and we have made several significant innovations with the past few releases of Family Safety.

Windows 8 Family Safety
http://windows.microsoft.com/en-AU/windows-vista/Protecting-your-kids-with-Family-Safety

In Windows 8, from the moment a child's Windows user account is created and the parent enables Family Safety, Family Safety gives parents meaningful insight into how their children use the computer to access the internet, play games, and run applications. Should parents decide to set boundaries, Family Safety provides easy to use options that let parents turn on web filtering, set time limits, or restrict the type of games and apps their

child can use. We believe parents are best-placed to determine such parameters for their children, based on an individual family's values, maturity level of the child, and other factors.

In the past, many industry software solutions for family safety (including Microsoft's) focused on web-filtering and other software-based restrictions. This resulted in a more complex setup experience and a constant stream of parental approval requests that could be difficult to manage. The end result was that many parents abandoned family safety products and returned to in-person supervision only—a tactic that has become less effective as computing has become more mobile.

Within a week of the parent enabling Microsoft Family Safety, the parent will receive informative activity reports for each child, which detail the child's web activity, applications downloaded and used, and time spent on the computer. Activity reporting has proven to be a helpful strategy for many parents to understand how their children use the computer. However, for those parents who want an even greater degree of control, the following features can be utilised:

- **Web filtering**: Choose between several web filtering levels;
- **SafeSearch**: When web-filtering is active, SafeSearch is locked into the "Strict" setting for popular search engines such as Bing, Google, and Yahoo. This will filter out adult text, images, and videos from search results;
- **Time limits**: With Windows 8, parents can restrict the number of hours per day a child can use his or her PC. For example, a parent might set a limit of one hour on school nights and two hours on weekends. This is in addition to the bedtime limits currently available in Windows 7;
- **Windows Store**: Activity reports list the most recent Windows Store downloads, and adults can set a game-rating level, which prevents children from seeing apps in the Windows Store above a particular age-rating, and;
- **Application and game restrictions**: As in Windows 7, parents can block specific applications and games, or set an appropriate game-rating level.

With Windows 8, parents and caregivers can monitor what kids are doing, no matter where they use their PC.

Xbox 360 and Kinect Safety Features
http://support.xbox.com/en-US/billing-and-subscriptions/parental-controls/xbox-live-parental-control

To help promote safer gaming by younger users, the Family Settings tools in the Xbox 360 game console allow parents to limit the use of some functionality. Parents can also configure the console to limit online gaming and communication using Xbox LIVE to approved friends and require parental approval for new friends. As previously noted, it also allows users to report inappropriate use of the service.

In November 2010, Microsoft introduced an innovative new hardware accessory, Kinect, to the popular entertainment console Xbox 360. Kinect enables individuals to sign in, navigate, play games, and use applications in the Xbox console by simply acting the movements or speaking the commands in front of the Kinect device that they want to make.

The Kinect sensor for Xbox 360 includes additional safety and privacy controls. Xbox 360 Family Settings allow parents to:

- Block or limit sharing of a child's profile information, adding of new friends, receipt of user-generated content, and viewing of mature-rated content;
- Specify which games a child can play, based on game rating;
- Create Xbox LIVE account settings for a child that will be enforced on any machine the child uses to access his or her account;
- Require parental approval of a child's list of online friends, and
- Specify which types of online communication (i.e., text, voice, video) are allowed and with whom.

Users can also control the following Kinect-specific experiences:

- Specify whether photos taken by games that use the Kinect device

can be uploaded to a website outside of Xbox LIVE;
- Turn off the Kinect sensors, including the microphones and camera, when the Xbox console is not being used for a Kinect-enabled game;
- Disable face recognition for identifying Kinect players, and
- Disable Kinect's voice-recognition feature.

9. Transparency

Microsoft strives to publish clear, user-friendly global online safety policies and usage information through its Terms of Use and Codes of Conduct, and these policies govern our takedown and moderation practices. As indicated in this self-declaration, we work with Governments, NGOs, and law enforcement agencies around the world to share best practices and collaborate on wide-ranging online safety efforts. We look forward to supplementing this engagement with periodic updates to Government on our progress, through bilateral meetings, and via our continued engagement in the Consultative Working Group on Cybersafety.

3. Other actions taken on implementation of these arrangements

Protecting individuals—especially children—has been a priority for Microsoft since the company began delivering services online in 1994. Today, we work to promote greater online trust and safety through a range of measures.

We incorporate online safety features and tools into our products and services. Our internal business policies and practices support safer and more responsible Internet use. We work with organisations worldwide to educate consumers about online risks and how to avoid them. We support law enforcement in investigating and prosecuting cybercriminals. And, we collaborate with policymakers on a range of issues associated with online safety. This is why we are proud to be a member of the Consultative Working Group on Cybersafety, and are pleased to be a signatory to this cooperative arrangement.

Indeed, from the advent of online services in the early 1990s, Microsoft has maintained its commitment to Internet safety for people of all ages and abilities. Our experience has led to a multi-part approach that includes: (1) developing and investing in innovative technological tools; (2) partnering with others in industry, government, and members of civil society; and (3) creating and delivering resources that help the public better understand, and thus reduce, online risks. Our goal is to empower individuals and families with the resources they need to more safely and securely live out their digital lives.

We pay special attention when it comes to keeping children safer online. Indeed, all Internet participants should embrace the goal of helping to protect the most vulnerable members of our global society, especially children. Through these and other efforts, we aim to support the creation a global "culture of online safety" that delivers safer, more trusted online experience for children and all individuals.