Microsoft Submission to Enhancing Online Safety for Children Discussion Paper

Executive Summary

Microsoft welcomes the opportunity to make a submission to the Discussion Paper, "*Enhancing Online Safety for Children*." We have also contributed to the submissions by the AIMIA Digital Policy Group and IGEA.

Microsoft Corporation is based in Redmond, Washington, in the United States of America. It was founded by Bill Gates and Paul Allen in 1975 and is today one of the world's most significant information technology companies. Microsoft operates subsidiaries in 110 countries, in addition to the USA, and directly employs around 90,000 people across the world and engages more than 100,000 contractors and vendors. The company's core business is the development, manufacturing, and licensing of software products, including operating systems, server applications, business and consumer productivity applications and software development tools; the manufacture of hardware and peripherals, and the provision of a range of technology services, including online consumer services.

Microsoft Australia is a marketing and sales subsidiary of Microsoft Corporation. It directly employs around 800 people and has offices in Sydney, Melbourne, Brisbane, Perth, Adelaide and Canberra.

Microsoft maintains that technology providers, governments, law enforcement, community organisations, and internet users have a "shared responsibility" to promote a safer, more trusted online environment.

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.

We have included more detail on these and other activities in **Appendix 1** to this submission

We support international best practice and Australian research which confirms that prevention, education and empowerment are the most powerful policy levers for producing optimal cyber-safety outcomes. More importantly it is this focus that prevents incidences of bullying before they occur which should be the aim of Government and industry.

We do not believe a Government-mandated process will result in the quicker or more efficient removal of 'harmful' content than those processes already put in place by responsible providers. The Government's stated aim is to 'get harmful material down fast,' however, we have strong concerns about the effectiveness of this process to achieve this goal.

With regard to the intention to introduce legislation to back a rapid removal scheme outlined in the discussion paper, we have a number of concerns.

In the first instance, we do not support the need to develop yet another piece of legislation to deal specifically with cyber-bullying. It is already an offense to engage in online harassment and it is important that the public are educated about existing criminal laws to make sure they are complying with these laws.

We are concerned about the capacity to define a 'large social networking site' given the rapid changes in the consumer technology space, the emergence of new players and the proliferation of collaboration tools embedded in all sorts of new and older technology. We have concerns about the potential for this legislation to only impact on the larger providers who already have efficient self -regulatory processes in place, whilst leaving smaller and newer players un-regulated.

We are concerned about the ability of legislators to define 'harmful'. We are already seeing in New Zealand the challenges around drafting the legislation and how to define something that is ultimately subjective to how the victim views the content.

We have broad concerns with the powers to determine which platforms will be in scope for the new legislation being vested in the Minister of the day, and believe that should the proposal go ahead, this should be determined by the Parliament.

Microsoft is supportive of strong self-regulatory principles which create a standard all providers should meet. We believe the Co-oeperative Framework for Complaints Handling Protocol that Microsoft and other responsible providers voluntarily signed up to should be extended to more providers.

Broad Principles on Imposing Further Regulation on Social Networking Site

Microsoft is committed to creating a culture of positive engagement online and fostering responsible use of technology to help its users, and young people in particular, stay safer online.

We, however, have a number of concerns with the proposal put forward in the Government's discussion paper, which we will outline in broad terms.

1. **Understanding how social media platforms work is critical**

   We do not believe a Government-mandated process will result in the quicker or more efficient removal of content than those processes already in place by responsible providers, and we think the focus on dealing with content after it has been posted is the wrong policy objective.

   Popular social media platforms are large networks with millions of users. They allow users to post content and send updates in real time. They are not moderated forums. Unlike a newspaper or a television network, there is no editor-in-chief or program director who oversees what can be posted.

   It is these elements that make social media so unique. If social media was a moderated forum, where a central person approved content, social media could never be used in the many positive ways we have seen over a very short period of time. With millions of users, simultaneously posting tweets, updates, and hours of video content every minute, the platforms would come to a grinding halt and certainly would not be able to work in real time.

   Of course, these features of social media also have a down side. Despite having specific user policies or rules in place for what can and can't be posted, some people will choose to ignore such rules. When someone uses the platform to post something that is untrue, hurtful or threatening – with no moderator, the content goes live for anyone to see as soon as it is posted. The social media platform cannot possibly be reading everyone's feed/page/channel to watch for such content. The best avenue they can provide is a 'report abuse' function so that if the content is in breach of the rules, it can be removed in the most efficient timeframe.

   For many vulnerable people, once the harmful content is posted, the damage is done. It is not a question of how long the content remains.

   So, how can we stop people from posting harmful content in the first instance? Quite simply, without moderation of content – any regulatory process will fail. And, if we want moderation on social networking sites, we need to accept we will lose many of the benefits of social media.

If we are not prepared to do that, the focus must be on education, self-responsibility and building resilience in our children so that they become strong, spirited adults.

2. Doubts that a legislated process will meet the objective "to get harmful material down fast."

The Government has repeatedly stated its aim is to 'get harmful material down fast,' however, we have strong doubts as to whether this process will actually achieve its desired goals.

The quickest way to get content which breaches a provider's use policy removed or unable to be shared, is to use the platform's report-abuse mechanism.

Microsoft supports the Australian Government's Cyber-Safety Help Button, which helps users navigate their way to find the appropriate help or advice, including how to report their concerns.

However research tells us that many Australian students do not know how to report concerns about content on popular social media sites.

We believe more could be done by both industry and Government to help younger users understand how to navigate these processes, and Microsoft is open to exploring ways to do this.

We also need to be conscious of the types of tools and systems that will resonate with children. Research shows that a claim of "cyberbullying" is a guaranteed invitation for adult involvement[1], something most teens are determined to avoid. Rather, they would prefer to address their own "drama" in ways that suit them.

In addition working through the Government's proposed approach to remove content, the process looks anything but fast and at best case looks to take at least a week.

Even if the E Commissioner was able to handle complaints in real time, and there was no backlog, this process does not look to meet the objectives of removing content quickly – in the context of how quickly content comes and goes in the online environment.

3. Defining a Social Media/Networking Site

Even using the boyd and Ellison definition, it will be exceptionally challenging to determine what services should fall within the scope of the legislation. Even within Microsoft there are questions about which, if any, of our platforms would fall within the scope of the proposal as, whilst not operating a social networking site in the generally understood definition, products are increasingly having the collaborative functionality of social networks built into them.

[1] Rosalind Weisman, *Masterminds & Wingen*, 2013.

The boundaries between search, social networking, workplace productivity and mobile technologies is blurring.

For example the way email is used today has all the capacity of a social network site with the ability to send group emails and post content to a peer group of a child that could cause distress. It is a similar scenario with text messages. Examples exist of people being bullied using this medium.

Online dating apps also have social media-like functionality. Internet news sites now have social media analogous forums. Professional networking sites are a social media network and, whilst not directly aimed at children, there is no reason why children wouldn't use the platform.

Facebook is probably the most widely understood social networking site today. However, there are many new players and new platforms that have 'social networking functionality' built into them. We are even starting to see social networking functionality being used in a variety of different ways, including by business with extraordinary productivity benefits.

As the provider of an online games platform (Xbox) we do not support online games being part of the scheme for several reasons.

- Game communications are transitory in nature and not the type of content that would be capable of being addressed by a rapid removal scheme; and
- Online games and game platforms including Xbox currently enforce codes of conduct and utilize sophisticated reporting technologies as well as enforcement measures such as user suspensions and bans.

With the speed of change in the technology industry, it is highly unlikely legislation will ever be able to keep pace.

4. Defining 'harmful' content

We think defining what constitutes harmful content is problematic. The terms used in the Government's discussion paper are inconsistent and vague. We are already seeing the challenges of defining this in legislation with the New Zealand Harmful Digital Communications Bill. Without a very tight definition, any single point of contact to deal with complaints is likely to be flooded and the system will become unworkable.

5. Determination of scope

We have broad concerns with the powers to determine which platforms will be in scope being vested in the Minister of the day, and believe that should the proposal go ahead, this should be determined by the Parliament.

The intention for the regulation to apply only to large social networking sites is problematic. Large providers already invest heavily in sophisticated tools and devote significant resources to

deal with cyber-safety concerns. Companies like Microsoft have well-established links to, and work closely with government, child safety organisations and law enforcement agencies.

That the proposed regulation fails to cover smaller and newer providers who may not have the same knowledge, make big investments and have established links to deal with cyber-safety risks, is putting the focus on the wrong area. The Government should be looking to the large, responsible providers as setting the standard to which all providers should reach.

To impose heavy handed regulation on the larger providers may push users onto platforms with less highly developed standards and increase their risk.

6. One-Size-Fits-All Approach unlikely to achieve aims

Large social networking site providers recognise the need to manage potential risks of social networking, especially to children and young people. The services they provide vary greatly in terms of their user demographics, the scale of their audiences, the markets they serve, the technology platforms they operate on, and the jurisdictions in which they are based. This diversity significantly affects the types of risks users may be exposed to and providers are best placed to determine the appropriate strategies to address these risks. This diversity also means that a one-size-fits-all approach to risk management is unlikely to be successful in its aims and, at the same time, is likely to create unnecessary regulatory burdens on providers and erect steep barriers to innovation.

Microsoft cares greatly for its users and for our own reputation. Users have a variety of choice of technology platforms and closing an account is only a click, touch or tap away. Users will quickly leave a platform if they don't like the user policies and a platform can quickly go from extremely popular with millions of users to almost unused. We are very conscious that we need to meet the expectations of our users although it must be pointed out that community expectations are neither static nor equivalent across demographic or contextual dimensions.

7. Function and Establishment of E Commissioner

Without commenting directly on the various models put forward in the discussion paper, we raise a number of points for consideration.

As a founding partner with the Australian Federal Police of the ThinkUKnow program, we do not support this being moved under a single organisation where the aim is to 'create efficiency and avoid duplication'. The ThinkUKnow program is unique because of the role the AFP play, and its target audience is different to many of the other programs out there. ThinkUKnow aims to bridge the knowledge gap between adults and youth, and hence focuses on minimising this gap by educating those responsible for the care and custody of children. We believe it serves a very worthwhile purpose and would be very concerned about it being homogenised into other cyber-safety programs.

Should the Government favour the proposal to designate a non-government organisation with expertise in online child safety, we would want to be sure that any conflicts are dealt with appropriately. The likely candidates for this position are likely to run their own cyber-safety programs and, if they are to become responsible for the administration, governance and funding of all programs, we would want to ensure their programs are not favoured at the detriment of others.

8. No need for new laws to deal with cyber-bullying

Microsoft does not believe there needs to be new laws created to deal with cyber-bullying. Commonwealth and State and Territory Laws already allow for the prosecution of harassing, threatening and intimidatory behaviour.

The AIMIA Digital Policy Group submission which Microsoft has contributed to, outlines the Australian laws that already provide remedies to address cyber-bullying behaviour.

There may be a lack of awareness of existing laws to deal with cyber-bullying and again we would support the need for education amongst young people, teachers and parents.

9. Need for a safe harbour provision

Should the Government proceed with a legislated approach we believe it must include a safe harbour provision for intermediaries.

A properly constructed safe harbour for intermediaries is an essential element of any regulation that seeks to address user behaviours online. Safe harbours allow intermediaries to continue to invest in innovative services that delight end users while at the same time deploying technical solutions and education to help maintain a safer online ecosystem.

An important consideration here is ensuring that the safe harbour can adapt to changes in technology. While safe harbour provisions have traditionally addressed a "takedown" of material, suggesting the material exists in a concrete location, a safe harbour provision that focuses on *disabling access to content* more accurately reflects the current direction of technology, where online material can exist in many ways and in many locations.

Conclusion

Thank you for the opportunity to comment on the Government's paper *Enhancing Online Safety for Children.*

Appendix 1

Microsoft's commitment to cyber-safety

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.

Mandatory Company Policy

On July 1, 2013, Microsoft implemented a new mandatory company policy on online safety, as well as accompanying operational procedures. The new Online Safety Policy, Standards and Procedures formally codify Microsoft's long-standing, self-imposed internal requirements for helping to make our products safer for individuals and families, and, in particular, for children. We will closely monitor the implementation of our new Online Safety Policy, Standards and Procedures across our services and devices to ensure any enhancements and developments respect our online safety guiding principles: suitability, transparency, awareness, fairness, control and choice.

Chief Online Safety Officer

In 2013, Microsoft appointed the company's and industry's first-ever Chief Online Safety Officer. Microsoft's "COSO" is responsible for all aspects of the company's online safety strategy, including cross-company policy creation and implementation, influence over consumer safety features and functionality, and communications to and engagement with a variety of external audiences.

Educational Resources

Microsoft is continually adding to its wealth of free public awareness-raising and educational materials that provide prescriptive advice and guidance about keeping children, youth, and indeed all individuals safer and more secure when they go online.

All of Microsoft's resources can be found at www.microsoft.com/safety.

Microsoft's commitment in Australia

Microsoft has been a member of the two previous Government's Consultative Working Groups on Cyber-safety, as well as a member of the current Government's CWG on Cyber-Safety.

In 2013, Microsoft became a founding signatory to the previous Federal Government's Co-operative Arrangement for Complaints Handling on Social Networking Sites. A copy of our undertaking is attached to this submission.

Microsoft Australia is particularly proud of our ThinkUKnow (www.thinkuknow.org.au) partnership, which is both an educational program and a significant collaboration with Government. ThinkUKnow is an Internet safety program, delivering interactive training to parents, caregivers and teachers through schools, churches, community groups and other organisation's 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), Microsoft Australia and DATACOM and is proudly supported by ninemsn.

Training sessions at local schools and community organisations can be organised through the website. The ThinkUKnow site also provides a "Report Abuse" mechanism and supports the Australian Government's Cyber Safety 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 since its inception for National Cyber Security Awareness Week, now the Smart Online Week Steering Group.

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.

Online Bullying

On online bullying specifically, Microsoft has invested in this collection of free, informative and educational resources over the years:

- Brochure
- Fact sheet
- Quiz
- PPT deck
- One-pager for policymakers

Online bullying has been a key issue for Microsoft in the online safety arena for the last six years. So much so that in 2012, we commissioned a global study [2]to examine the more negative online behaviors occurring among youth in 20 countries, including Australia.

On a worldwide basis, data showed 54% of children between the ages of eight and 17 were worried they would be bullied online. Meanwhile, 24% admitted to having cyber-bullied someone at one time.

These statistics show that the media's focus on the most severe and tragic cases has children the world over fearing that they will be cyber-bullied. Meanwhile, the large majority of youth are "doing the right thing" – 75%+ are *not* bullying.

To be clear, Microsoft agrees that even one child being bullied online is one too many, but the media's intense focus on the issue is suggesting a borderline epidemic, when the data does not support such a conclusion. The data can be reviewed in the work of leading thinkers on the issue, including Emily Bazelon[3] and Microsoft Research's own danah boyd[4].

Research centres and online safety organisations[5] are now focusing on empowering teens, including peer mentoring, "nice it forward," and random acts of (online) kindness to change the culture of online interactions.

Report Abuse

Microsoft has in place simple and easy-to-use reporting mechanisms for child exploitation issues, complete with a robust and thorough operational system on the back-end. This system enables Microsoft to appropriately categorize and address an alleged report of abuse based on its type. Our centralized Customer Service and Support (CSS) organization of several hundred includes a sizable team dedicated to handling customer reports of abuse of all types. In addition to CSS's central function, various individual products and services have their own enforcement teams. These teams, of which Xbox Live is a clear standout, monitor public activities and interactions among customers, and address user complaints, including unsportsmanlike game-play, "griefing," questionable gamer tags or profile pictures, etc. Microsoft takes such reports very seriously; investigates in a timely manner, and takes appropriate action, as necessary.

---

[2] http://www.microsoft.com/security/resources/research.aspx#onlinebullying

[3] http://news.nationalpost.com/2013/02/23/overblown-and-sensationalized-author-says-bullying-issue-is-more-nuanced-than-black-and-white/

[4] http://www.danah.org/

[5] http://cyberbullying.us/

Simple, robust, reporting tools will be one online safety focus area for Microsoft in 2014. Most importantly, we are exploring ways to develop reporting tools that can easily be used by children and other more vulnerable members of our global society.

Parental Controls

Microsoft has developed and deployed "parental controls," or "Family Safety Settings" in a broad range of our products and services. (For detailed descriptions of the Family Safety features and functionality across our range of products and services, see this fact sheet or brochure noted below.[6])

In 2013, with the major release of Xbox One, we continued our commitment to offer advanced parental controls, empowering adults to choose the content, communication and sharing settings that are right for their families. We know that even within families, one size doesn't always fit all. That's why all parental controls on Xbox One can be set and customized for each family member's individual profile. In addition, over the years, parents and caregivers have shared valuable feedback about parental controls on Xbox 360.

Accordingly, we now offer some finer levels of control on Xbox One, including:

- Content controls that apply on an individual-user basis, letting adults choose the settings they feel are most appropriate for each of their children.

- Content controls that apply on any Xbox One, so parents can be confident that wherever their child signs in, they'll be subject to the same rules, including any exceptions that are set.

- For children younger than age eight, content restrictions are enabled by default.

- Xbox One filters content based on the user with the most restrictive settings, customizing what is seen depending on which users are signed in. With guest-account settings, even if no family members are signed into Xbox One, parents can help ensure the settings that are right for their households are enabled.

- Web-filtering allows adults to decide what types of websites their children can browse using the Internet Explorer app.

---

[6] (http://go.microsoft.com/?linkid=9835005)or this brochure (http://go.microsoft.com/?linkid=9677447).

- Xbox One designed its controls to allow adults to control access to content how they want, taking into account children's maturity levels, family values, etc. Every game, app and video is assigned a rating. Parents can get a sense for the type of content that is or is not allowed at a particular level by browsing the Xbox Stores. And, if they want to know a particular app or game rating, they need only search for it.

Microsoft will continue to improve and innovate our family-safety functionality across our range of products and services, in an effort to make it easier for parents to enable and configure such settings for their children.

Child Abuse Material (CAM) and Law Enforcement

Microsoft already has in place notice and take-down procedures for CAM in all relevant consumer products and services. Indeed, procedures for handling CAM are detailed in the new internal Microsoft Online Safety Policy, Standards and Procedures.

In addition, as part of UK Prime Minister David Cameron's efforts to rid the web of these horrific images, Microsoft introduced process and technology improvements for Bing search designed to prevent the spread of child sexual abuse content.

And, although this important dialogue began in the UK, Microsoft plans to implement these changes across Bing globally for the benefit of all customers.

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).

PhotoDNA[7] is a technology created by Microsoft Research and Dartmouth College that enables fingerprinting of child abuse images. This 'fingerprint' enables us to find any previously discovered child abuse image that may have been uploaded by a user, even if the image has been cropped, resized or modified. Initially deployed to monitor Microsoft online sites, in May 2011 Microsoft partnered with Facebook to begin deploying this technology across all of Facebook[8].

In March 2012, Microsoft announced our intention to licence for free, the PhotoDNA technology to law enforcement organisations around the world. During 2012, an Australian government organisation integrated PhotoDNA into their child exploitation investigations platform and is currently using it to streamline their investigations.

[7] http://www.microsoft.com/en-us/news/presskits/photodna/

[8] http://www.huffingtonpost.com/2011/05/20/facebook-photodna-microsoft-child-pornography_n_864695.html

In July 2013, Twitter announced[9] that it too will incorporate the Microsoft PhotoDNA technology into their services.

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. Microsoft is 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.

[9] http://www.theguardian.com/technology/2013/jul/22/twitter-photodna-child-abuse

Appendix 2

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."[10]

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,"[11] 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.

[10] 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

[11] 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.[12]

XBOX Live

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

[12] 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.