**Submission to the Department of Communications and the Arts on the Online Safety Charter consultation paper**

**April 2019**

**Interactive Games & Entertainment Association**

Table of Contents

[Introduction 3](#_Toc5830802)

[Video games industry in Australia 4](#_Toc5830803)

[Video gaming in Australia 4](#_Toc5830804)

[Australian video games industry 4](#_Toc5830805)

[Video games and online safety 7](#_Toc5830806)

[National Classification Scheme 7](#_Toc5830807)

[Safety features on consoles and devices 8](#_Toc5830808)

[Safety features within games 9](#_Toc5830809)

[Industry advocacy, research and awareness-raising 10](#_Toc5830810)

[General comments on the draft Charter 12](#_Toc5830811)

[Contextualising online safety in video games 12](#_Toc5830812)

[Practical considerations for video games businesses 13](#_Toc5830813)

[Importance of a flexible, principles-based approach 14](#_Toc5830814)

[Relationship with the Safety by Design principles 15](#_Toc5830815)

[Specific feedback on the Online Safety Charter 16](#_Toc5830816)

# Introduction

The Interactive Games & Entertainment Association (IGEA) is the peak industry association representing the business and public policy interests of Australian and New Zealand companies in the interactive games industry. Our members publish, market, develop and distribute interactive games and entertainment content and related hardware. See [here](https://igea.net/about/members) for information on our members who we represent.

IGEA welcomes the announcement by the Minister for Communications and the Arts (the Minister) of the development of an Online Safety Charter (the Charter) and appreciates the opportunity to provide a submission to the Department of Communications and the Arts (the Department). Our submission highlights the importance of online safety, especially the online safety of children, to our members and provides some industry perspectives and practical recommendations which we hope the Government finds useful.

The first part of our submission sets the scene by providing an overarching summary of the nature of video gaming in Australia as a pastime and artform, as well as Australia’s burgeoning home-grown video games development industry. The second part explores the range of online safety features that are already part of the video games eco-system as well as the awareness-raising and research activities that our industry continually invests in to promote online safety. The third part outlines our general, overarching views on the Charter including, where appropriate, some concerns and recommendations. The fourth part provides some specific commentary on the draft text of the Charter. Rather than providing specific responses to the discussion questions, noting that most of the questions are not highly relevant to video games, we have tried to address the underlying basis of relevant questions throughout our submission.

We look forward to the results of this consultation process and may respond to comments and ideas from other stakeholders. We would also be happy to discuss the draft Charter with the Department in person and, if possible, we would encourage a further opportunity for comment on any revised text.

# Video games industry in Australia

## Video gaming in Australia

This part of the paper seeks to provide background on the state of video gaming in Australia and perhaps break down some old – but possibly lingering – myths about what video gaming actually is. First, while video games used to be regarded as kids play, most Australians who play games are adults. Research that IGEA conducted in 2018 found that the average age of an Australia game player is 34 and that 77 per cent of Australian players are aged 18 years or older. Australians who play games are also almost as likely to be female than male. Perhaps even more surprisingly, 43% of Australians aged 65 and over play video games, with older Australians amongst the fastest growing cohort of game players. IGEA’s full Digital Australia 2018 research can be found [here](https://igea.net/2017/07/digital-australia-2018-da18).

Video gaming is a creative artform, a form of entertainment and a way to promote wellbeing. According to our research, while fun is the most important reason why Australians play games, they also play games to de-stress and – particularly for older Australians – keep their minds active. Most people we surveyed also agreed that games can help improve thinking, dexterity and pain management. As outlined in [our submission](https://igea.net/2019/03/submission-to-consultation-on-a-renewed-national-arts-and-disability-strategy/) to the Department’s consultation on a renewed National Arts and Disability Strategy, we believe that playing and creating video games is particularly important to Australians living with disability.

Video games are also a highly varied and innovative form of entertainment. Games come in all shapes and sizes, from relaxing puzzle games that a person can ‘snack’ on while commuting on a bus, to highly thoughtful games where a person can build worlds and multiplayer game where friends and family members can share time together. Games are also played on a variety of platforms, including PC, consoles, phones, tablets and other handheld devices. Critically to this consultation, however, while many games allow some degree of interactivity or communication with other players, this interactivity is always limited and secondary to the focus of the game itself. This is one of the ways where we believe games stand apart from many other kinds of digital services that fall within the scope of this draft Charter.

## Australian video games industry

The interactive games sector is one of the fastest growing technology and entertainment industries in the world, eclipsing both the filmed entertainment industry and the music industry. The global games market was estimated to be worth almost $200 billion in 2018[[1]](#footnote-1) and $3 billion in Australia alone.[[2]](#footnote-2) While video games continue to be popular as entertainment for people of all ages across the world, games are also finding ‘serious’ applications, including in the education, health care, defence, business, research and community sectors. This makes the games industry highly diverse and increasingly important.

Video games businesses in Australia can broadly be placed into three categories: publishers, distributors and developers. Publishers generally market and distribute games that they or other parts of their broader organisation develop. Distributors market and distribute third party games, after having acquired the legal rights to sell those games in Australia. Developers create their own games which they publish themselves or through a publisher or distributor. Relevant for the Charter, the vast majority of games played in Australia are not made here and international publishers with marketing and sales offices in Australia will not generally have any input or influence in their games’ design or characteristics.

While Australia has an exciting and emerging game development industry, it remains small and fragile. A survey that IGEA conducted last year found that Australian game developers generated $118.5 million in revenue in the preceding year and employed just 928 full-time employees.[[3]](#footnote-3) In December 2018, IGEA released a [policy paper](https://igea.net/wp-content/uploads/2018/12/IGEA-building-a-thriving-game-development-industry.pdf) ‘[*Building a Thriving Interactive Games Development Industry in Australia*’](https://igea.net/wp-content/uploads/2018/12/IGEA-building-a-thriving-game-development-industry.pdf) that outlines why a game development industry is so vital to Australia and sets out the concrete steps for how the Australian Government can better support it.

The Australian video game companies that have been able to succeed, despite the current limited support from Australian governments, prove how unique, innovative and talented the industry can be. This is particularly seen in the context of ‘serious games’ described above. Some Australian game developers like Mighty Kingdom, SMG Studio, 3RD SENSE and Chaos Theory Games work very closely with the business and community sectors to develop diverse, innovative and often unexpected uses for games. The unique opportunities presented by video game technology also led to the acquisition of the Australian game studio Well Placed Cactus by Deloitte Australia, which turned it into the company’s specialist digital creative consultancy.

Examples of innovative and positive ‘serious’ games made in Australia include:

* *Sound Scouts*, a game to aid the process of detecting hearing difficulties in young children which has received $4 million in Australian Government funding for a national rollout.
* *ReachOut Orb*, a game created by SMG Studio for the youth mental health organisation ReachOut to teach Australian students about wellbeing.
* *Smartstep*, developed by Neuroscience Research Australia as a game-based stepping exercise for people with MS to help their balance and agility.
* 3RD SENSE, which created *Bring Back The Beat*, a music learning and appreciation app for Cochlear and *5 of 5*, a game designed to increase school attendance.
* *Rash Decisions*, a gamified learning app from Chaos Theory Games for the University of Sydney to deliver dermatological course content in an engaging and effective new way.

# Video games and online safety

The video games industry takes its obligation to protect game players seriously and it’s priority is to ensure that games provide both a fun and safe space for children and adults alike. It achieves this objective through a multi-level approach involving strong compliance with the National Classification Scheme, implementing safety features directly on the consoles and devices where people play games, providing further targeted safety features within games themselves and engaging with broader cultural, education and awareness-raising campaigns directed at the public, gaming community, children and their parents and guardians. These are addressed in turn.

## National Classification Scheme

First, unlike all other kinds of technology firms, video games are already subject to specific and thorough regulation under the National Classification Scheme (NCS), a cooperative arrangement between the Australian Government and state and territory governments where video games must be classified by the Classification Board, an independent government body, before they can be made available to the public. Since the start of the NCS in 1995, Australian video games publishers have maintained a policy of strict compliance to ensure that games that are bought and played in Australia have been appropriately classified. Just as importantly, the requirements of the NCS and corresponding ratings systems all around the world already play a key role in shaping the content of games and driving how games are developed, distributed and marketed.

Under the NCS, video games are classified against six classifiable elements - violence, sex, nudity, drug use, coarse language and themes – and assigned a classification ranging from G (General) to R18+ (Restricted to persons aged 18 and above). The Classification Board also has the discretion to assign specific consumer advice, or warnings, that must be displayed with the classification category on a game. The Board has absolute discretion to provide any consumer advice it considers appropriate and, relevantly, currently provides consumer advice of “online interactivity” on games that allow players to interact with others online so that parents and guardians are aware of this. Other ratings systems overseas even make “online interactivity” a formal aspect of the ratings process, such as the ESRB in the United States, an approach that could be considered here. To achieve this, the NCS would need to be subject to a legislative overhaul and modernisation process, which IGEA and its members support and have pushed for over many years.

We have also worked in partnership with the Australian Government to ensure games that are digitally distributed, including online and mobile games, are appropriately classified under the International Age Ratings Coalition (IARC) classification tool. This tool was built by the video games industry in collaboration with government and non-government ratings agencies around the world and has now been rolled out on Google Play, the Nintendo eShop, the Microsoft Windows and Xbox stores and the PlayStation Store among others. Hundreds of thousands of games have now been classified by the IARC tool, as well as countless non-game apps on Google Play. In addition to implementing IARC on the Google Play store, Google Play also allows parents and guardians to restrict what content can be downloaded or purchased from the store based on maturity level. Please see [here](https://www.globalratings.com/) for more information on the IARC classification tool.

## Safety features on consoles and devices

All of the major video game consoles provide a range of safety features to provide a safe environment for game players and their families – many of which are world leading and unique to the games industry.

Features of the Nintendo Switch device include:

* A Nintendo Switch Parental Controls smart device app to provide parents and guardians easy access to parental controls
* Time limits, alarms and a “suspend software” feature
* Ability to see what games their children have been playing and for how long, as well as monthly play reports
* Ability to prevent children from playing games that are inappropriate for their age, based on age ratings
* Ability to restrict the posting of screenshots of games to social media services
* Restrictions for Nintendo eShop to prevent game purchases by children

Features of the Microsoft Xbox One console include:

* Creating family groups and child accounts with special privacy and online safety settings
* Setting screen limits for children on Xbox and PC, including for both games and shows
* Setting age limits for content by choosing from preset recommendations by age
* Blocking inappropriate websites through a web filter
* Preventing unauthorised purchases by children, including through the use of a passkey
* Functionality to mute or block other players
* Setting standards and expectations through the Microsoft Services Agreement and Code of Conduct and ability to report other players for violations
* Safety and wellbeing resources including access to a free 24/7 Crisis Text Line
* Ability to hide and filter activity feed posts

Features of the Sony PlayStation 4 console include:

* “Family on PSN” settings to customise account restrictions for individual family members, parental controls and spending limits
* “Play Time” controls to give parent and guardians the ability to set limits on when during the day and for how long children can access the system
* Setting age rating levels for games as well as for Blu-ray and DVDs
* Setting monthly spending limits
* Restricting access to network features, such as disabling access to communicating with other players or viewing content created by others
* Disabling child access to the Internet Browser or PlayStation VR headset
* Availability of a PlayStation App to make it easier to customise parental settings

Nintendo, Microsoft and Sony all provide clear, transparent and easy-to-find information on their safety features and parental controls through their localised Australian websites: [Nintendo](https://www.nintendo.com.au/nintendo-switch/parentalcontrols), [Microsoft](https://support.xbox.com/en-AU/browse/xbox-one/security) and [Sony](https://www.playstation.com/en-au/get-help/help-library/my-account/parental-controls/ps4-parental-controls/).

## Safety features within games

Most games with a communications functionality use a range of measures to combat the risk of coarse language or the harassment of players. As previously mentioned, unlike other digital platforms like social media and messaging services, communication is always an ancillary function to gameplay itself and more heavy-handed approaches to filter or block inappropriate communications are often the norm. The limited functionality of communication in games means that risks in community behaviour are easier to address, safety can remain uncompromised and the enforcement of community harms like language and abuse can be efficient and effective.

Just some examples of safety features that have been deployed in games include:

* Strong community codes of conduct (often incorporated into terms of service and user agreements)
* Parental control of a child’s personal information (eg. *Pokémon Go*)
* Pre-emptive profanity filters in text chat (eg. *Battlefield V*)
* Pre-emptive prevention of personal information being posted (eg. *Roblox*)
* Providing educational automated feedback after a player uses profane language (eg. *Rainbow Six Siege*)
* Various options for muting other players in a game (eg. *Red Dead Redemption*)
* Ability to customise or turn off graphic content (*eg. Call of Duty: Black Ops 4)*
* Ability for gamers to report other players (eg. *StarCraft II*)
* Enforcement and penalties including the suspension or banning of users (eg. *FIFA 19*)
* Endorsement systems to encourage positive gamer behaviour (eg. *Overwatch*)
* Disciplinary systems to discourage negative gamer behaviour (eg. *League of Legends*)
* Incognito and offline modes to enable people to play games in complete privacy

## Industry advocacy, research and awareness-raising

The video games industry has taken a proactive approach to raising awareness and education around parental controls and responsible gaming. Our website provides information on [parental controls](https://igea.net/useful-links/parental-controls) and will always support other organisations in Australia that help to promote the use of these controls. We also support the [www.askaboutgames.com](http://www.askaboutgames.com) resource and parents’ guides developed by our industry counterparts in Europe. Together with our counterparts from around the world, we have established [www.healthyvideogaming.com](https://www.healthyvideogaming.com/industry) which provides a portal to guidance for parents and guardians on safety features and controls that they can use on the most popular platforms. The portal also provides our perspective on other issues like screen time and healthy gaming.

Through our bi-annual ‘Digital Australia’ report, we regularly conduct research with Australian players, parents and guardians which helps to identify issues that are of most concern. We work hand-in-hand with Bond University to undertake this research to ensure that it is robust, balanced and consistently conducted so that we can track changes in perception over time. The results of our research are provided to our members to help them appreciate and address risks and opportunities with online safety in their games. Our most recent report, Digital Australia 2018, can be found [here](https://igea.net/2017/07/digital-australia-2018-da18/). We have already commenced preparations on the Digital Australia 2020 report (including consulting with the Australian Government on topics to cover) which will be released this year.

We particularly recognise the importance of parents and guardians monitoring and playing games with their children. This is something that we support and also undertake research on. For example, our Digital Australia 2018 research found that:

* 60% of parents play with their children in the same room
* 44% of parents play online games with their children
* 81% are familiar with family controls on game systems
* 84% of parents have talked with a child about playing safely online

Despite these positive statistics, we would welcome an opportunity to work most closely with the Department and particularly the Office of the eSafety Commissioner (eSafety Office) to strengthen support and messaging to parents and guardians about both parental controls and the importance of appropriate supervision.

Furthermore, many of the largest video game companies in the world, including the parent companies of many IGEA members, have banded together with other stakeholders in the industry to create the [Fair Play Alliance](http://fairplayalliance.org/). The Fair Play Alliance is a global coalition of gaming professionals and companies committed to working together to develop and exchange best practices to encourage healthy and positive communities and player interactions in online gaming. Its members’ objective is to create games that encourage teamwork and positive social interactions that are free of harassment, discrimination and abuse. To do this, its members discuss and share strategies on all aspects of game design from the ground up, including communication, game mechanics, matchmaking, narrative, level design and online safety features and controls.

# General comments on the draft Charter

## Contextualising online safety in video games

As previously discussed, video games are not like social media or communication services and most games have limited or specific communications or networking functions, if at all. While a range of games and devices may have communications functionality, this functionality is generally limited to approved friends lists or a specific temporary environment like a game session or game lobby chatroom. Game session or lobby chat is generally ephemeral, sometimes lasting just a few seconds, and even then is often heavily protected by text filters. Where games allow voice-to-voice communication, this is almost always optional with players also able to mute talking or restrict talking to friends or teammates.

Screen-based communications available through consoles and in-game are also generally limited to text chat, while profiles and identities are often limited to avatars and “gamer tags” that provide little to no real-life identifying information. Furthermore, many of the more dynamic functionalities of social media or electronic communications service, such as posting images and videos, re-broadcasting, forwarding or sharing messages, or mass-messaging are simply not available functionalities in most games and gaming devices. Similarly, many of the more serious concerns of young Australians as outlined by the eSafety Office, including cyberbullying as an extension of real life inter-relationships, fake or imposter accounts of victims, sex-tortion and image-based abuse present far less of a risk within the gaming environment than in others.

Bearing all of this in mind, we also advocate the need for video games to be seen in the context of what they are – worlds for people to enjoy with each other but also to compete against each other. Just like in playgrounds, training and sporting fields, there will always be playful language, banter and sometimes arguments between players in games. While there is no place in games for harassment or abuse in games, robust conversations and self-expression should not necessarily be outlawed or moderated in the vast majority of gaming environments (with the exception of those involving very young children), just as they are not outlawed or moderated in real life.

In talking about the draft Charter, we have heard the Government use the term “standards of behaviour online should be the same as those that apply offline”. We note that the intention of this statement is to set the expectation that standards of behaviour that are not tolerated in real life should similarly not be tolerated online. We do not disagree with this, nor do we disagree that abuse and harassment does occur in some games which is why the industry as a whole continues to implement and experiment with new tools and technologies. However, we also note that this principle also goes both ways and the Charter should not set unnecessary or unreasonable expectations of restrictions on behaviour and expression online that would otherwise be acceptable in the physical world.

## Practical considerations for video games businesses

The global video games industry, unlike some other segments of the broader digital landscape, is comprised of hundreds if not thousands of companies and developers, from global multi-nationals to micro studios and individual developers. The Australian game development industry is particularly focussed on smaller independent studios creating online and mobile games. For example, while there are only a small number of social media services used by Australians, almost all of whom are well-resourced multi-nationals, there are hundreds if not thousands of video games played in Australia, many of which have been developed by small businesses.

As previously discussed, it will be vital that the Charter is drafted in a way that is supportive of – but does not place unrealistic expectations on – Australian start-ups, including the indie game developers that make up the backbone of our local industry. One reality of a “one size fits all” Charter is that the expectations placed on the most popular, highest-risk and most resourced platforms cannot be the same as the expectations placed on a platform that is the opposite of those qualities. Another reality is that some of the requirements set by the principles can only be achieved at significant financial, labour and management cost and are not realistic for businesses in their early growth stages. A necessary implication of these realities is that while online safety should rightfully be a priority, and we will continue to advocate for this in our industry, the Charter must, for practical reasons, remain voluntary.

On a similar point, the Charter should accommodate the reality that the major digital platforms and services that are popular among Australians have mostly been developed overseas. The local offices of technology firms here in Australia, if they even do have local offices, often have little if any influence over how their parent companies’ overseas products are developed. In this environment, we believe that flexible and high level principles will be far more likely to gain the support of offshore and parent companies than an incongruous and possibly unrealistic rules-based approach.

Another reality is that an unilateral Charter may present challenges in a global online eco-system. Other countries may not necessarily share the view of the Australian Government and in fact, some of the principles in the draft Charter may be inconsistent with the expectations or regulations of other countries. For example, some kinds of online safety mechanisms like heavy moderation or pre-emptive filters may sit uncomfortably with norms of free speech principles in other jurisdictions, while expectations around collecting or leveraging personally-identifiable information for online safety reasons may clash with stringent privacy and data protection laws elsewhere. What this means is that in a globally fragmented video games regulatory environment, developers and publishers will sometimes be faced with a delicate and sometimes impossible balancing act – further highlighting the need for a flexible approach in the Charter.

## Importance of a flexible, principles-based approach

There is no single digital industry or archetype digital business, platform or service in Australia or around the world. One of the most compelling and important aspects of the ‘digital industry’ is the level of variety and innovation of the businesses that collectively form it. Technology firms come in all shapes and size, from global multi-nationals that employ tens of thousands of people around the world managing multiple products, to Australian start-ups comprising a handful of like-minded individuals operating from co-working spaces and cafes who are seeking to build the next game-changer. The level of diversity of the digital industry is increasing each day as traditional businesses continue to digitalise, something that the Government strongly supports through programs like the Small Business Digital Champions project.

As a result, we do not consider that a “one size fits all” approach is possible with promoting online safety. With this in mind, we believe that the most effect and appropriate use of a Charter is one that:

* Focusses on providing general and high-level principles that both encourages and guides technology firms to consider the online safety of its users and engage in ongoing dialogue with their users
* Promotes outcomes over processes, recognising that there may be a range of ways for technology firms to address online safety and the solutions used will depend on both the business’s capabilities (size and resources) as well as the nature and scale of the risks
* Empowers, but also gives discretion to, technology firms to consider how they can best adopt and apply these principles within their platforms in the most appropriate ways, based on their size and unique characteristics
* Encourages technology firms to openly, collaboratively and continually engage with the principles, noting practically that a compliance-based approach that involves formal sign-up, reporting and “naming and shaming” is inconsistent with a voluntary Charter and is likely to be counter-productive

We believe that while many of these views are already captured in the overarching discussion paper, particularly at pages 3-4, there may be benefit in incorporating them into the Charter itself, even as a preamble, to better set and articulate the Government’s expectations to industry.

## Relationship with the Safety by Design principles

Finally, we are concerned with the risk of duplication and confusion caused by the concurrent progress of the Department on this draft Charter and by the eSafety Office on its Safety by Design (SbD) framework. We were simultaneously consulted on both projects in February 2019 and despite similarities between the two documents, unfortunately there has been little transparency or context surrounding their relationship. For example, the draft Charter only alludes to the SbD framework minimally, while the SbD framework does not addresses the Charter at all.

It is also unclear which set of principles has precedence in the event of inconsistency or ambiguity. The draft Charter at page 4 indicates that it sets the high level standards for online safety which the SbD framework draws from and provides additional detail around. However, this appears to be inconsistent with the fact that the eSafety Office finalised its consultations and is treating its SbD framework as final, even though consultations on the Charter (which the SbD is intended to take its direction from) has not even been completed.

It is our view that both the Charter and the SbD framework appear to be largely seeking to achieve the same objective and we encourage the Department and the eSafety Office to continue working together to combine or at least more clearly articulate or coordinate respective efforts.

# Specific feedback on the Online Safety Charter

\*We have provided in-line comments (in blue) against the draft text of the Charter.

**Draft Online Safety Charter**

*This Charter seeks to outline what the Australian Government, and the Australian community, expect of technology companies and online service providers operating in Australia in terms of protecting the most vulnerable in our community.*

As previously discussed, we would encourage moving into the Charter itself some of the commentary at pages 3-4 of the discussion paper around the voluntary nature of the Charter and recognition that a flexible approach to implementation is needed, taking into account the size and capabilities of the technology firm, the nature and popularity of its digital service, the scale of potential risks and the appropriateness or relevance of particular principles.

*It is underpinned by two fundamental principles:*

1. *Standards of behaviour online should reflect the standards that apply offline.*

We do not have concerns with this principle but as previously noted, this goes both ways. While abuse and harassment has no place online as it has no place offline, this principle should not restrict standards of behaviour, communication and expression online beyond what is acceptable in corresponding social and competitive ‘real world’ Australian environments.

1. *Content that is harmful to users, particularly children, should be appropriately restricted.*

*This Charter is directed towards technology firms that offer the opportunity for users in Australia to interact or connect, and technology firms whose services and products enable Australian users to access content and information. This includes social media services, internet service providers, search engine providers, content hosts, app developers, and gaming providers, among others. For the sake of simplicity, the Charter uses the term ‘technology firms’.*

While we understand the use of the umbrella term ‘technology firms’ for the sake of convenience, we reiterated our earlier discussion around the diversity of such firms and the importance for the Charter to be principles-based and be flexible to take into account the vast differences between digital businesses in terms of services, size, user-base, online safety risk and resources.

***1. Control and responsibility***

* 1. ***Content identification***

*Technological solutions should be fully utilised by technology firms to identify illegal and harmful content, and these solutions should be supported by human resources as appropriate.*

*There should be a specific point of contact within each technology firm for the referral of complaints about illegal and harmful content or legal notices from Australian authorities. This point of contact should be equipped and trained to manage Australian referrals, with a good understanding of relevant Australian legal requirements.*

As we have mentioned, there are thousands of games played by Australians and many are made by start-ups and small studios both in Australia but also around the world. For these businesses, Australia will likely be one of many markets they serve. While the call for specific points of contact for referrals is noted, it may not always be realistic or practical for each company to have a good understanding of all relevant Australian legal requirements.

* 1. ***Content moderation***

*The systems employed by technology firms should have the capability and capacity to moderate illegal and harmful content.*

*Where feasible, this should include a triaging system to ensure high risk content (e.g. content promoting self-harm or criminal activity) is addressed expeditiously and lower risk content is reviewed and actioned within a longer period (for example, within 24 hours).*

*This triaging system should ensure that complaints made by children, or by adults on behalf of children, are also expedited. Where appropriate, illegal, harmful or inappropriate content targeted towards a child should be removed immediately, and only reinstated once the complaint has been investigated and only if the complaint is not upheld.*

*The resources devoted to content moderation should be proportionate to the volume of content available to users and relevant to the Australian context. Human content moderators should meet minimum training standards.*

The principle that “the resources devoted to content moderation should be … relevant to the Australian context” is slightly unclear. Similar to our comment above, it will not always be possible for human moderators to be based in Australia or to have a deep appreciation of the specific Australian context, particularly for smaller games and platforms that may only need a small team of moderators.

*Minimum timeframes should apply to the review and moderation of flagged content, whether identified from internal flags, user complaints or regulatory authorities.*

* 1. ***Content removal***

*Content that is clearly and unambiguously illegal under Australian law should be removed proactively by technology firms.*

*Content that has been determined to be in breach of terms of use, or identified by regulatory authorities to be illegal or harmful, should be removed within clearly stated minimum timeframes.*

*Technology firms should take steps to prevent the reappearance of illegal, harmful or offensive content that has been removed.*

**2. Improving the user experience**

***2.1 User behaviour***

*Clear minimum standards for online behaviour should be set and applied consistently across services and service providers.*

We query whether it is possible to establish a single consistent minimum standards across services and service providers. For example, the minimum standards of behaviour on a public mass-communications platform would presumably not be the same as the minimum standards for communication on an in-game chatroom between friends. Similar, the minimum standards of behaviour within a game aimed at children would presumably not be the same as the minimum standards of behaviour within a game that has been classified R18+ and already restricted to adults. We suggest that a more nuanced principle is needed.

*• Behaviour standards should be visible, easy to find and easy to understand.*

*• Behaviour standards should be reviewed regularly to ensure they remain fit-for-purpose and user-friendly.*

*• There should be meaningful and material consequences for breaches of behaviour standards, including account suspension, access restrictions and banning of repeat offenders.*

*• Banned users should not be able to open a new account in a different name or register a different user name.*

While we support this objective in principle, in reality there is often no easy solution to this. Apart from registration email addresses, banned users may only otherwise be identifiable by IP address and not only may many technology firms not track the IP of banned users (for a number of reasons including legal reasons), we note that IP addresses can also easily be changed or masked.

**2.2 User support**

*User reporting and complaints systems should be easy to find, understand and complete.*

*They should include a swift acknowledgement of each complaint and outline expected response timeframes.*

*They should provide regular updates to complainants and affected users (including the person being complained about), enable decisions to be reviewed, and provide full information to users on how to refer complaints to regulatory authorities in Australia.*

To support technology firms to provide information on how to refer complaints to regulatory authorities in Australia, it is important that the Government make sure that this information is as accessible and easily found online as possible. This also includes providing this information in language that is easily adaptable and relevant to all forms of technology to which the Charter applies.

*Online safety resources should be actively promoted to users, age-appropriate and easy to understand. This should include mental health and other support services, where appropriate.*

**2.3 Account control**

*Instructions about how to adjust settings, including privacy settings, should be easy to find, understand and follow.*

*Users should be able to freeze their account in real time.*

This principle is less relevant to video games. Video games already provide a range of design features, settings and controls that means that it is generally unnecessary to freeze accounts. Many games and consoles simply do not enable communication and interactivity when they are turned off (eg. in many games the player can only receive messages if they are actually playing the game). Within games, controls like incognito mode, reporting players and instantaneous text and voice muting are often available to players and provide them greater control and empowerment over potential harassment.

*Users under 16 years should be required to secure parental or guardian consent to open an account or register as a user. Verifying parental consent should require more than just ticking a box.*

This is the principle that we believe most requires follow up discussion and revision. At the outset, we are not sure how the age of 16 has been identified and question whether a single age is appropriate or can be consistently applied across vastly different digital services and platforms. Some digital platforms that have multiple built-in safety features and limited communications functionality, like many video games, will have an inherently lower risk profile than other platforms. There may also be certain digital platforms, including some wellbeing-focussed services and serious games, where a requirement for parental or guardian consent may discourage use.

Furthermore, there is also an argument that this principle may be inconsistent with the use of video games and the operation of the National Classification Scheme, which allows games, including online games that require accounts, to be purchased and played subject to a game’s classification category. For example, a game that is classified G means that the game can be purchased and played by people of all ages, while even games classified MA15+, the second highest classification available for a game, can be purchased and played by 15 year old children without their parent or guardian’s consent.

Many games and platforms will require accounts to be set up for many reasons even for offline play, including for functionality, security, terms of use and code of conduct purposes (all of which may enhance online safety). Requiring parental or guardian consent for all games or consoles that require an account, including those with minimal communications functionality and robust built-in safety features, before a person under 16 can play it may be an onerous requirement and undermine the purpose of the NCS. In the context of video games, a better approach that we have previously discussed would be reform of the NCS so that the nature and scale of online interactivity within a game is considered more closely as part of the classification process itself.

However, we note that most of the major international games companies already have put in place minimum age restrictions for children to open user accounts and access online gameplay – but this age restriction may not necessarily be 16. For example, some consoles require an adult to open a full access account, with parents and guardians then able to create sub-accounts for the children they look after with built-in safety features. Many game publishers also have age restrictions on account creation which are often set at 13 or 16 depending on the market. These age restrictions may be dictated by privacy-related legal requirements which can differ around the world.

Notwithstanding our views above, regarding the principle that verifying parental consent should require more than just ticking a box, we make the general comment that age and parental identity verification remains an inherently challenging technological solution across the online sector and one that to date has not been easy to implement in a safe, robust, user-friendly and non-discriminatory way.

*Parental control settings should be easy to use and difficult to circumvent.*

***2.4 Content management***

*Users should be given full control of content safety options, such as the ability to delete unwanted comments, easily remove content, selectively hide content they no longer want to be visible and impose self-restrictions on uploading content such as time of day lockouts or type of content (for example, videos or images).*

**3. Built-in Child Safety**

***3.1 Default settings and age guidance***

*All products and services (including apps and games), and devices marketed to children, marketed as being appropriate for children, or that are likely to appeal to children, should default to the most restrictive safety and privacy settings at initial use or set up, and should include age guidance.*

As we have noted, our members take our responsibility of having games classified under the National Classification Scheme very seriously and worked hand-in-hand with the Australian Government to implement the IARC Classification Tool in this country.

Most of the major games companies already take special consideration with games and consoles that are popular with children. For example, we have already noted that many consoles require someone over 18 to open a full access account, with parents and guardians then able to create sub-accounts for their children with built-in safety features including communication restrictions, web filters, locks on non-age appropriate games, time limits, restrictions on sharing gaming content on social media and parental and guardian monitoring tools. Please refer to the more detailed list of safety features in consoles and games outlined at pages 7-9 of this submission.

***3.2 Supply chain***

*App and game supply points should require developers and suppliers to certify that they have considered built-in child safety and any relevant SbD principles before accepting apps and games for distribution.*

Most of the major game supply points, and certainly all who are also IGEA members, take their responsibilities to maintain high quality and community-friendly storefronts seriously, including compliance with classification and consumer laws and the provision of a wide range of parental controls. We imagine that all storefronts also maintain detailed distribution agreements that set out relevant conditions of distribution, with the Google Play Developer Distribution Agreement mentioned at Attachment B of the draft Charter as an example.

While it would be up to individual supply points to consider whether this principle is one that is appropriate for them, we would suggest replacing “built-in child safety and any relevant SbD principles” in the text of the draft Charter with more generic language like “appropriate child safety considerations”. Both “built-in child safety” and “SbD principles” are specific to the Charter and the eSafety Office’s SbD framework respectively. Given the Australia-centric nature of the Charter and SbD framework, a more general and flexible certification requirement would be appropriate in a global distribution environment.

*Information about privacy, online safety and parental control settings should be available at all relevant points in the supply chain, including point-of-purchase (including by download), registration, account creation and first use.*

**4. Accountability and transparency**

**4.1 Reporting and compliance**

*Technology firms should engage broadly with experts and key stakeholders in relation to the development and application of online safety standards.*

*Technology firms should publish regular reports on:*

*• content controls, including the type of content is identified, moderated and/or prevented from being uploaded, how it was identified, and the action taken;*

*• complaints, including the number of complaints received, investigated and resolved, the time taken to resolve complaints, the category of complaint, the action taken and generalised demographic information (including, where known, age and geographic location of complainants); and*

*• compliance with the standards in this Charter, identifying any gaps and outlining the proposed approach to improving safety outcomes in relation to these gaps.*

*For firms with a significant presence in Australia, a local version of these reports should be published and the underlying data should be made available to relevant Australian authorities on request.*

*User safety considerations and practices should be embedded in the leadership structures, operating practices and governance arrangements for technology firms, and appropriate policies and procedures should be core business for all individuals who work within technology firms.*

1. <https://www.gamesindustry.biz/articles/2018-12-18-global-games-market-value-rose-to-usd134-9bn-in-2018> [↑](#footnote-ref-1)
2. [https://igea.net/2018/02/australian-consumer-spend-video-games-cracks-3-billion](https://igea.net/2018/02/australian-consumer-spend-video-games-cracks-3-billion/) [↑](#footnote-ref-2)
3. [https://igea.net/2018/01/australian-game-developers-march-generating-118-5m-spite-limited-recognition-support](https://igea.net/2018/01/australian-game-developers-march-generating-118-5m-spite-limited-recognition-support%20)  [↑](#footnote-ref-3)