Submission to the discussion paper "Enhancing Online Safety for Children: Public consultation on key election commitments" January 2014

Enhancing Online Safety for Children

A submission by Child Wise and PwC

March 2014

pwc

child wise
creating child safe communities

The Director
Cyber Safety Policy and Programs
Department of Communications
GPO Box 2154
Canberra ACT 2601

Sent via email: onlinesafety@communications.gov.au

7 March 2014

Submission to the discussion paper "Enhancing Online Safety for Children: Public consultation on key election commitments" January 2014

This submission responding to the Federal Government's Enhancing Online Safety for Children public consultation paper has been written by Child Wise and PricewaterhouseCoopers Australia ("PwC"). We chose to jointly write the submission because it highlights the importance of business and not-for-profit sectors working together on an issue which encompasses a diverse range of interests.

Continuous technological change has transformed the way we work, communicate, and learn. PwC suggest we change our approach to cyber risks as the environment evolves. Child Wise recognises that for children, engaging online can be a formative experience, but one that exposes them to unique risks.

Child Wise and PwC approach online safety from somewhat different perspectives. However, both organisations are committed to creating a safer online environment for everyone and the recommendations in this paper reflect the alignment of our objectives. The objectives outlined in this paper represent the experience of both organisations in cyber safety and child abuse prevention.

Our submission is based on considered and practical experience in response to the questions raised in the consultation paper. We support the proposals including the establishment of an e-Safety Commissioner which will simplify and enhance the protections afforded to children online.

However, we suggest that to limit the scope of an e-Safety Commissioner, or any response to online safety, to children fails to account for a key characteristic of cyber risks. The risks of bullying, extortion and blackmail are not confined to those under 18, and those over 18 are not always better equipped to deal with them. Our submission is written with the understanding that cyber risks cannot be limited to any one segment of the population.

We trust our submission serves to help decision makers as they consider responses to cyber risks to children, and the community as a whole. We welcome the opportunity to discuss the details of our submission with you in person.

Regards

Steve Betinsky
Chief Executive Officer. Child Wise

Steve Ingram
Partner, PwC

PricewaterhouseCoopers, ABN 52 780 433 757
Darling Park Tower 2, 201 Sussex Street, GPO BOX 2650, SYDNEY NSW 1171
T: +61 2 8266 0000, F: +61 2 8266 9999, www.pwc.com.au

Contents

Executive Summary

Child Wise and PwC welcome the Government's commitment to protecting children online by actively addressing cyber-bullying, an area of growing concern.

To aid the Government in implementing an effective policy that seeks to improve Internet Safety conditions, our submission responds to the following themes:

A Commissioner for all

The role of an e-Safety Commissioner should not be limited to children. Cyber risks do not end at age 18 – improved cyber literacy and safety for adults will contribute to child safety online. We suggest the Government should allow the e-Safety Commissioner to act for all Australians, and be administratively supported by ACMA in line with Option 2 of the consultation paper.

A focussed rapid removal policy

A mechanism for the rapid removal of harmful content is a necessity. However, legislating specific content, methods of transmission, and responsible parties in a constantly changing online environment is neither practical nor effective. Child Wise and PwC propose the Government consider a modified voluntary 'best practice' response protocol with a strong oversight role for the Commissioner.

A considered approach to enforcement

The existing laws only address serious cases of cyber-bullying. If the Government considers a new penalty necessary, the creation of a lesser offence under the existing category with a penalty that focuses on alternative sentencing options would be the most agreeable to address mid-range cyber-bullying offences. We recommend that the best policy response is to focus on improving behaviour online, and that criminal penalties are unlikely to effectively regulate the behaviour of children online.

An emphasis on prevention

While the Government's proposals touch on preventing poor behaviour online, we suggest that prevention measures through better education receive greater consideration. The Commissioner should contribute to improving the cyber literacy of adults and teachers, as well as encouraging the creation of in-school programs for children. A focus on prevention will provide the best outcomes for individuals.
Our attached submission is organised to respond thematically to a selection of the consultation questions listed in the discussion paper titled "Enhancing Online Safety for Children: Public consultation on key election commitments" dated January 2014.

1 The Commissioner

Establishment of an e-Safety Commissioner

The creation of an e-Safety Commissioner as a central focal point for online safety within the Australian community is a positive undertaking. Yet the issues that children face online are often the same that adults face, and it is not clear that adults are always better equipped to respond to these concerns.

Child Wise and PwC suggest that the remit of an e-Safety Commissioner should not be limited to children, but extend to online safety for people of all ages. Adults experience extortion, blackmail and bullying online, and are not always in a position to respond effectively to these threats. Certain categories of adults who have lower cyber literacy and poorer coping mechanisms for managing cyber safety issues may be at greater risk of harm. Those at great risk may include people with a disability,

people from a culturally and linguistically diverse (CaLD) background, and Indigenous people. Many middle-aged and elderly people, as they begin to interact online in an environment that is constantly changing, may also be at greater risk.

Specific functions of an e-Safety Commissioner may be required to address the vulnerability of children. Children are more vulnerable and prone to risk-taking behaviours. At the same time, there are many areas of concern for children that cross over to how adults engage online.

Increasing the scope of an e-Safety Commissioner to include adults meets a number of the proposed objectives of this public consultation:

- Creating a central focal point for issues of online safety
- Reducing duplication of services and functions across Government departments
- Heightening the safety of people engaging online
- Improving the ability of adults to respond to concerns about children's behaviour online.

Functions of the Commissioner

We recommend that the functions of an e-Safety Commissioner should be broader than covering children and cyber-bullying exclusively, and only focussing on social media platforms.

- Cyber-literacy is an area of growing concern. Improvements in this area will translate to general cyber- safety in the community including parents and teachers better able to respond to concerns about children active online and adults better able to protect themselves from extortion or online scams. A Commissioner should be able to oversee a whole of community approach to cyber-literacy
- Legislated rapid removal is likely to prove impractical. Rather, we suggest working with industry to develop a 'best practice' response protocol for the removal of harmful content will be more effective. Section 2 of our submission explores this in more detail
- A research fund that invests in understanding cyber-safety and providing practical advice on how to mitigate online risks for the whole community. In a rapidly changing online environment, understanding emerging trends in online risks for adults will better protect both adults and children
- The support for a certification process for online safety programs offered at schools and in the broader community, depending on the placement of the Commissioner (if the Commissioner is not fully independent from Government or the sector/NGO realm, this certification may lack legitimacy or authority)
- Formalised links with each State and Territory Children's Guardian and Commissioners, to ensure that children in out-of-home care are provided with additional protections that recognise the increased levels of risk-taking behaviours online.

Existing Government online safety resources and programs should be transferred to the Commissioner's control. However, the focus of many of these programs is wider than just children or parents. The breadth of the existing programs reflects recognition that online safety is an issue that affects the whole community, not just children. The programs such as Think U Know and The Line, but also the Easy Guide to Socialising Online, have been developed to respond to risks identified for adults and children.

If the Commissioner's role was to extend beyond children and include adults, the transfer of programs and resources may be cleaner and more efficient. However, to

deliver a broader reach and greater access and use, some programs should remain with their current areas. It would also allow for specialisations to develop based on Departmental expertise. One such example is the Department of Education 'Safe Schools Hub'.

We recommend that the Australian Communications and Media Authority's ("ACMA") programs and resources would be best administered by a new e-Safety Commissioner, but that all other programs and resources listed in Appendix 1 of the discussion paper should remain with their respective administrators. The Commissioner may liaise with these Departments and bodies to ensure consistency of approach.

Placement of the Commissioner

We recommend that the proposed e-Safety Commissioner should be established in line with Option 2 of the consultation paper, with administrative support to be provided by ACMA. The reasons for this recommendation include:

- Lower cost base than a new and fully independent statutory authority
- Shared institutional knowledge through administrative links with ACMA
- A dedicated/singular focus for the office of the Commissioner is more likely to lead to effective engagement with industry, than one tied directly to ACMA's current undertakings
- Independence from Government will lead to a more effective response when dealing with companies and sites than a Department.

Ultimately, the independence of the Commissioner as an independent statutory office, linked to the ACMA's expertise in this field, is likely to lead to more favourable outcomes than the other options.

Option 1 is too costly, and is likely to lead to duplication of functions or administrative actions.

Option 3 lacks independence, and the transfer of functions, powers, and roles from within ACMA will be complicated, a situation that may be exacerbated by changes to legislation. Aligned with Government, Option 3 makes it challenging for the Commissioner to respond to complaints and failings by social media sites independently and in contravention of political concerns.

Option 4 also lacks independence – Non Government Organisations ("NGOs") are likely to have an advocacy component and agenda to their work, which may clash with the proposed functions of the Commissioner. The need to raise funds for both this work and their other work may lead to conflicts of interests for NGOs, and a further deterioration of their independence. The effectiveness of this option is in question, as an NGO will not be able to clearly enforce their functions. They will also lack impact when challenging potential breaches of the proposed regulations, as they do not automatically have the backing of Government. Additionally, there is a lack of certainty for NGOs with staff turnover and a lack of oversight from Government over quality of services in a regulatory role.

2 Rapid Removal

The Government's intention to limit the damage caused by harmful material posted on social media sites is commendable. While safeguards can be put in place, it is not practical or desirable to regulate the Internet. We have identified several concerns with the scheme the Government proposes.

Issues with the proposed bill

Definitions

In a rapidly changing online environment, attempting to legislate the boundaries of social networks that pose a risk to children is an unrealistic goal.

While Facebook and Twitter are currently the most popular social media sites, it was only a few years ago that Internet chat rooms were the primary way for groups of people to interact online There are now signs that Facebook's popularity among teenagers has peaked.[1] The new frontier is mobile, with Instagram, SnapChat, Vine, Tinder, and Secret among the newly popular social networks. They are no longer 'social media sites', but integrated mobile and online applications. The proposed definition of 'social media sites' already appears out of date.

These new networks meet aspects of the definition the Government proposes, but not all of them. Legislation based on a narrowly defined concept of a social media site would need to constantly update its definition to meet the characteristics of new online networks and engagement.

Defining social media sites by a rigid set of criteria draws artificial boundaries for activity on the Internet that could harm children. It is difficult to delineate a social news aggregator or a forum from a social network that may be covered under the scheme, but all three are capable of hosting content harmful to children or others.

Unfortunately, while the specifics of the medium change, human behaviour does not, and the potentially harmful nature of content viewed by children will stay the same on emerging networks and sites that do not meet legislated definitions.

Enforcement

We suggest the Government would face a number of challenges in enforcing a mandatory rapid removal scheme on participating social media sites. Almost all participating social media sites are headquartered and managed offshore, and the Government has no punitive power with which to force sites to comply.

The business model of emerging social media sites popular with children also needs to be considered. While established social media networks such as Facebook have large teams to respond to reports of inappropriate content, emerging social media networks may not have even designed a mechanism for user complaints. Social media start-ups can operate with very few staff – for example the company behind WhatsApp employs only 55 people, despite having a substantial 450 million user base.[2] Emerging social media sites would be an enforcement issue whether or not the Government decided to include these sites in the scheme – in either circumstance, children may experience abuse without any recourse, and the Commissioner can do little to help.

Enforcing the scheme will require a level of proof that the Commissioner, and those who complain to her/him, will not be able to meet. While there are some social media sites where the offending content may be public, and therefore linked to, most content will only be able accessible by a person connected to the victim or the offender. Screenshots can be easily manipulated and are not a solid basis for reliance.

1 Bercovici, Jeff. Forbes, "Facebook Admits It's Seen a Drop In Usage Among Teens" Last modified September 30, 2013. Retrieved from http://www.forbes.com/sites/jeffbercovici/2013/10/30/facebook-admits-its-seen-a-drop-in-usage-among-teens/

2 Burnham, Kristin. Information Week, "Facebook's WhatsApp Buy: 10 Staggering Stats" Last modified February 21, 2014. Retrieved from http://www.information-week.com/software/social/facebooks-whatsapp-buy-10-staggering-stats-/d/d-id/1113927

The proposed rapid removal scheme could involve the Commissioner issuing notices, formal warnings and infringement notices to individuals. In our view, it is unrealistic to expect that an offender's social media identity could always be traced to their personal identity and proven as such.

A case to consider is how the proposed rapid removal approach would tackle reported content in a social-based game within a social media site. The norms of behaviour in a video game are different to those of face to face interaction. Swearing and taunts are commonplace, and are not necessarily intended to offend or harm other players. Video game players are more likely to play using a pseudonym, which may not be possible to trace back to an individual, and there would be no way for a victim to prove that an offensive comment had occurred in a way that could be validated. In the future, it is possible that social interaction online will be through voice or video channels without a lasting footprint online. Monitoring and enforcing behaviour for possible future networks is highly impractical.

Government intervention alone cannot solve the problem

A mandatory, legislated rapid removal program would not be the most effective way of reducing instances of cyber-bullying on social media sites. Rapid removal of offensive content is a reactive step that at best can only mitigate the damage that has already been done. By the time a 48 hour deadline had elapsed, offending content would have been viewed by most users, with the old content replaced with fresh updates.

We recommend that the Government consider an alternative proposal for rapid removal of offending content, while focussing its efforts on preventing offensive content from being posted to social media sites in the first place. The best way for the Government to achieve this is to embrace a strategy of prevention, education, and behavioural change. We discuss our thoughts further on this topic in Chapter 4.

Proposed rapid removal alternative

Key principles

We recommend that industry and the Commissioner agree to a set of social media best practices. The scheme should be voluntary, with the Commissioner to publish the names and logos of all companies that are a part of the scheme to encourage participation. Under these best practices:

- Companies should have a published complaints mechanism for offensive/harmful content that meets an agreed standard
- Companies should take action against reported complaints within 48 hours
- Companies should have a plain language user agreement or policy for all users, and one that is accessible to minors.

The Commissioner should maintain guides on its website outlining how to report inappropriate content on social media sites. These guides should be frequently updated and include all social media sites. Guides should be published for emerging social media sites, with new guides written as new social media networks gain popularity. By keeping up to date, the Commissioner will maintain relevance and usefulness to children.

Proposed process and timelines

We propose a rapid removal process based on the following, with specifics developed with industry bodies:

1 Individual complaints to social media site. Social media site to respond within 48 hours.

2 If no response, late response, or the individual disputes the response of the social media network, the individual can raise a complaint with the Commissioner.

3 Within 24 hours, the Commissioner's office assesses and refers on the complaint to the company/social network if the complaint is upheld.

a. Commissioner to notify complainant if complaint is referred.

b. If complaint is not upheld, Commissioner to inform individual of reasons for decision.

4 The social media site has 48 hours to respond.

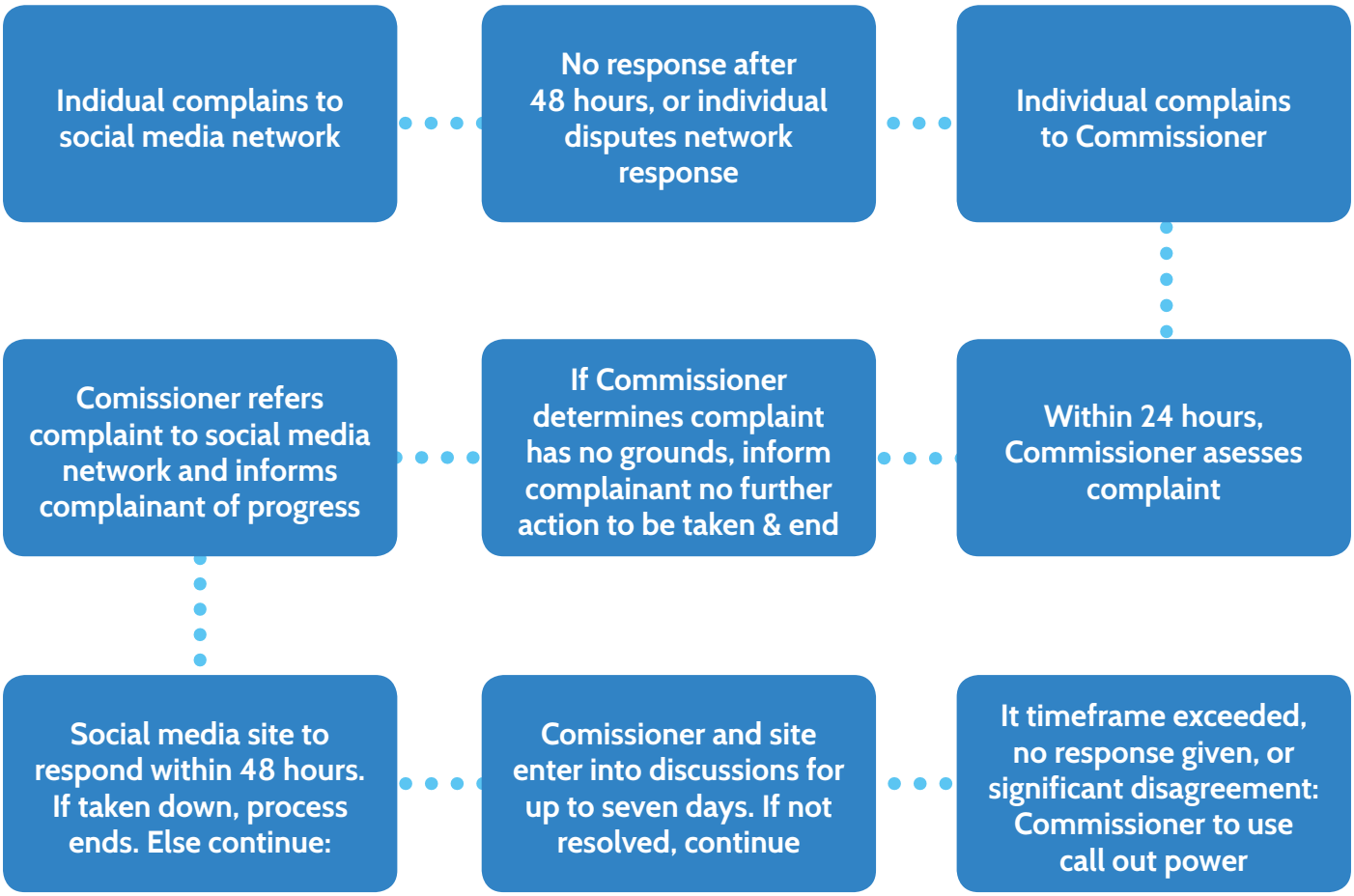
a. If content is removed, process ends.

b. If the social media site disagrees with the Commissioner, then the Commissioner and site to enter into discussions for up to 7 days. If not resolved, then the Commissioner can exercise name and shame power.

5 Commissioner to call out/name and shame/warn people against the site/network, after egregious cases or after a number of complaints.

This process will provide a method for resolving cases that are not dealt with by the social media network's complaints systems. The process would be applied to all social media networks whether they participate in the scheme or not. This would encourage participation in the scheme as social media networks will be subject to the same process. It will also allow the Commissioner to follow offensive content wherever it manifests, not just on specific sites.

This process balances the need for rapid removal with the current reality: established social media sites such as Facebook currently take considerable steps to respond to reports in a timely manner.



Proposed complaint information

The information collected from complainants should be minimal and a link to the material or screenshots would allow the Commissioner to make a determination on content. We suggest that children have access to systems that enable them to make complaints without the support of an adult.

We recommend the Commissioner collects the following information:

- Age of complainant
- Name of complainant
- Age and Name of victim (if different from complainant/if known)
- Contact details (for follow-up communication)
- If the content is repeated
- A link to or screenshot of the material

The test

The Government propose that the test for assessing material under the scheme should be "Material targeted at and likely to cause harm to an Australian child". We broadly support the proposed definition, though we argue that the scheme should not be limited to material targeted just at children. This would mean that the scheme has no impact on workplace bullying, and bullying targeted at disabled and disadvantaged persons, as well as those from minority groups.

The Government identifies several factors that the Commissioner should take into account when making a determination. We welcome the inclusion of a provision giving the Commissioner the power to consider any other matter which the Commissioner may consider relevant. We suggest that flexibility is vital in the development of a scheme that can operate in the rapidly changing environment of the Internet.

We are concerned with the proposed consideration of "the risk of triggering suicide or life-threatening mental health issues for the child". This provision suggests that the Commissioner is able to understand how content might affect the state of mind of an individual complainant, despite never having met them. The state of mental health of a child making a complaint cannot be known from afar. Additionally, many other factors may weigh on such a determination, and the other factors are sufficient criteria to consider complaints.

Other considerations

The proposal for a safe harbour for social media sites that join the scheme is an agreeable one, but we do not consider it vital to achieving a positive policy response under our proposed alternative scheme.

Dealing solely with sites that host the content, rather than individuals, eliminates the need for a right of appeal mechanism as proposed in the discussion paper. While individuals should not be a part of the rapid removal scheme, they should continue to be subject to criminal penalties as outlined in Chapter 3.

3 Enforcement

The existing laws are adequate

We welcome debate on how criminal penalties should be applied when dealing with cyber-bullying. We suggest that while criminal penalties should exist, threatened punitive measures are not effective at changing the online behaviour of a child. We contend that the policy response that can really make a difference is a focus on preventing bullying in the first place (discussed further in Chapter 4). As such, we do not find an imperative to change the current law.

We suspect that criminal penalties against cyber-bullying are generally not enforceable, and a new 'cyber- bullying law' would be impractical. Offenders are often under 18, police can be reluctant to charge minors and a child under 10 is not criminally responsible for an offence. It is not practical, nor desirable to turn to the courts with every instance of cyber-bullying, even if the identity of the offender can be established beyond a reasonable doubt. It may not always be a positive outcome to criminalise minors for making poor decisions, particularly when improvements in online behaviour education are required.

As mentioned in the discussion paper, section 474.17 of the Criminal Code Act 1995 (Cth) (the Criminal Code) already makes it an offence for a person to use a carriage service, including the Internet, in a way that reasonable persons would regard, in all the circumstances, as being menacing, harassing, or offensive. Section 474.15 of the Criminal Code makes it an offence to use a carriage service to threaten to kill or cause serious harm to a person, a provision which could be used in extreme cases of cyber bullying. We suggest that creating a better understanding of the existing laws is a worthy goal, and would render the creation of new offence unnecessary.

If a new offence were to be created that was used more frequently, we are concerned that it may breed complacency at the lower range of cyber-bullying, as the laws would likely be used only for high-range cases.

If changes must be made

An offence could be created as a subcategory of the current crime with a civil response only. This would involve penalties taking the form of infringement notices, work orders, or community service. Consistent with our support for a broader policy response, any new law should apply to adults and to cases with adult victims. The age of an offender is already taken into account by the courts, so the crime does not need to specify an age limitation.

4 Other Considerations

The proposals we have outlined respond to the questions and content of the discussion paper. Child Wise and PwC suggest it is important to propose additional considerations and recommendations that are important to achieving greater online safety for all. Specifically, there should be a greater imperative on preventative measures.

Prevention

There are some elements outlined above that address the issue of prevention in the online space. Child Wise and PwC contend that prevention measures should receive greater emphasis than the discussion paper implies.

There is some evidence to suggest that traditional forms of regulation, such as supervision, work well with offline bullying, because the physical aspects of supervision are easier to implement. When it comes to the online space and the proliferation of devices and access, a different approach is needed. Effectively, this requires a culture of 'self-regulation' in behavioural practices.

For instance, punitive responses, particularly for children, do not seem to be effective – they appear to be damaging and reinforce the problem. Additionally, denying access (i.e. by taking a phone away) doesn't ensure they cannot access the internet, and is also taking away an important tool for learning, social interaction, and identity formation.

Risk taking behaviours online, which take different forms in adults and children, can be well managed through emotional regulation, empathy education, and responses in this vein, rather than specific responses to the online issues. Such a program is beyond the scope of an e-Safety Commissioner. There has been some success internationally through using an 'ethic-of-care' model within schools to address broader risk taking concerns, which led to improved online safety.3

Cyber-literacy programs for adults and children may form a useful tool in responding to online safety concerns with a prevention focus. This is particularly important for children, who are often reluctant to approach adults about problems or bullying online because they see adults as out of touch. In an environment that changes so quickly, programs and regulations cannot focus just on the problems of a particular form of social media, they must consider all forms of cyber-literacy and interactions. This introduces better safeguards for adults engaging with an often confusing and complex online landscape.

5 Conclusions

The need to protect children from the risks that the online environment presents is pressing. In preparing our submission, Child Wise and PwC began with a key understanding – that cyber risks extend beyond any one part of the population and that these risks have the potential to impact people of all ages. It is our contention that any efforts to protect children from cyber risks can only be bolstered by expanding the efforts to include adults.

Education is key to creating a safer online environment for the whole community. Preventing poor behaviour online through a focus on education will include improving the cyber-literacy of children and adults.

To impose legislative restrictions in an environment of such rapid change is challenging. Our recommendations articulate that such an approach is likely to hamper future efforts at protecting children and others from cyber risks. In this environment, we suggest that a 'best practice' response model supported by oversight from an e- Safety Commissioner will lead to a positive outcome for children and adults.

Our submission argues that the introduction of a specific cyber-bullying offence should be treated with caution. Punitive responses may seem to have a limited impact, and there are legitimate questions that should be asked of such an offence's enforceability. Civil and prevention based behavioural interventions are preferred to criminal sanctions, particularly for children and young people.

Child Wise and PwC would like to thank the Government for the opportunity to respond to the issues under consideration in the Enhancing Online Safety for Children public consultation paper.