ISPCC

Never give up on a child. Ever.

Joint Committee on Children and Youth Affairs

ISPCC Briefing on Children and Cyber Safety

February 22nd 2017

Contents

1	Summary and Recommendations	3
2	Introduction to the ISPCC and our Work on Cyber Safety	5
2.1	The ISPCC's Experience	5
2.2	The ISPCC's Data and Evidence on Cyber Issues	6
2.3	The ISPCC'S Partnership Work on Cyber Safety	6
2.4	The ISPCC's Cyber Safety Interagency Work	7
3	The ISPCC's Review of Cases involving Cyber Safety: Findings and Case Examples	8
4	ISPCC's Key Recommendations – Items for inclusion in a National Cyber Safety Strategy for Children	15
5	Appendices	
5.1	External Studies and Research	20
5.2	ISPCC Case Examples	23
5.3	ISPCC Submission Excerpts	27
5.4	ISPCC Internal Case Review Methodology	31

1. Summary and Recommendations

- Over the past several years, the ISPCC has concluded that cyber safety is the child protection issue of our time.
- There are many benefits to the use of technology by young people and children. The educational, social and developmental opportunities presented are immense; however, there are also dangers associated with online use that require significant attention from policy makers.
- The ISPCC is well-accustomed to spotting trends in risks to children. Nearly two decades ago, we first received calls to Childline from children who were being bullied through messages sent to their phone. Long before the term 'cyberbullying' was coined, Childline provided a listening ear to children who felt overwhelmed by harassment and were suffering real harm as a result. 'Cyberbullying' is now recognised as a form of harmful behaviour and we understand much more about its effect on children, how to prevent it and alleviate its impact.
- As technology has developed, the issue of cyber safety has itself become more complex, incorporating issues such as sexting, viewing inappropriate material and exploitation, all of which pose serious risks for children.
- However, a distinction needs to be made between (1) behaviour that should or does constitute an offence, and (2) behaviour that is harmful. As a result the current legislative and policy provisions need to be modernised. This briefing paper intends to give a comprehensive insight into the concerns and experiences of children and young people in relation to cyber safety and outlines some key recommendations as to how children can be better protected online.
- In July 2016 the ISPCC's internal working group on cyber safety began a case review of the cyber related issues that the ISPCC were encountering from the children, young people and families with whom we work.

The main themes identified were:

1. Cyberbullying
2. Excessive Time Spent Online

3. Access and Exposure to Inappropriate Content
4. Sexting
5. Online Grooming
6. Sextortion
7. Identity and Wellbeing
8. Lack of Knowledge and Skills

- Cyber safety should be considered in the broader context of safety by recognising the effects online interactions can have on young people's wellbeing. It was repeatedly highlighted throughout our case review that young people were fearful of accessing support to deal with cyber safety issues.
- It is evident from the case examples we have gathered that many children and young people can behave differently online than they would do in a similar face-to-face situation. For example, young people can experience a lack of empathy when behaviour takes place behind a screen. They are not always fully aware of the implications of posting nasty commentary about others.

This further emphasises the need for a national dialogue on children's cyber safety; a dialogue which includes the voice of the child.

Key Recommendation

Ireland requires a **National Strategy on Children's Cyber Safety**. The Committee should recommend the immediate development of a strategy as a priority by government.

Below, we have outlined the potential components of such a strategy;

1. Implementation of key education measures regarding online behaviour
2. Reform of the legal framework regarding children's cyber safety
3. Establishment of an Office of the Digital Safety Commissioner and a regulatory policy framework

2. Introduction to the ISPCC and our work on Cyber Safety

The Irish Society for the Prevention of Cruelty to Children (ISPCC) appreciates the opportunity to brief the Committee on Children and Youth Affairs on the topic of children's cyber safety. As the national child protection charity, providing support services to children and families all over Ireland, the ISPCC is well placed to comment on the specific issues arising for children in relation to cyber safety.

The ISPCC is the national child protection charity[1]. It provides a range of child-centred services including childhood support services, family support services and mentoring, all of which are focused on building resilience and coping skills. These services support children and young people and their families to develop their own skills and enable them to deal with challenges and situations in their lives, and to promote their wellbeing.

Our Vision

An Ireland where all children are safe, heard, and valued

Our Mission

To make the protection of children everyone's priority

Our Work

We listen, we support, we protect.

2.1 The ISPCC's Experience

The ISPCC has based this briefing on its experiences of working with children, this work being grounded in the principles of the UN Convention on the Rights of the Child (UNCRC).

The ISPCC's Childline service answers over 400,000 contacts from children and young people across its phone, online and text platforms annually. In

[1] Further information about the ISPCC's services and financial statements can be found in the Annual Report 2015 http://www.ispcc.ie/campaigns-lobbying/publications/-ispcc-annual-report-2015/14783

addition in 2016, we worked with 552 children on a one to one basis through our childhood support and mentoring services. We will make reference to case studies under each theme with additional case studies provided in the appendix at the end of this briefing.

The ISPCC's Children's Advisory Committee (CAC), via their participation in our internal services review, were in a position to provide us with insight into their thoughts on cyber safety and what they see as key remedies for this issue, which we will make reference to throughout this document.

The ISPCC has made several recommendations to progress children's cyber safety in recent policy submissions. The relevant excerpts from these submissions are available in the appendix.

2.2 The ISPCC's Data and Evidence on Cyber Issues

In July 2016 the ISPCC's internal working group on cyber safety began a case review of the cyber-related issues that the ISPCC had encountered from the children, young people and families with whom we work over an 18-month period.

Over 500 calls and 250 online contacts, over 50 calls to our support line (adult helpline) and 30 childhood support cases were reviewed, along with staff and volunteer interviews and focus groups.

The ISPCC sought to have a clearer understanding of the challenges children, young people and their families were facing and to understand how regularly they were coming across these challenges. Further information on our methodology is in the Appendices.

Key Questions Asked

- What are the cyber related issues experienced by children, young people and their families and how often do they occur?
- What are the impacts/effects of cyber related issues on children/young people, on their parents/carers, families?
- What more could the ISPCC do to support children, young people and their families on cyber related issues?

Main Themes Identified

- Cyberbullying
- Time Spent Online
- Access and Exposure to Inappropriate Content
- Sexting
- Online Grooming
- Sextortion
- Identity and Wellbeing
- Lack of Knowledge and Skills

The findings of the review are discussed in more detail in section 3.

2.3 The ISPCC's work on Cyber Safety

Over the last several years the ISPCC has conducted a range of work in this area, in its support work, anti-bullying programme, inter-agency work and in research. In 2016 the ISPCC joined forces with Vodafone with a shared vision of keeping children safe by keeping them connected.

The results of this partnership work include

1- As part of our partnership, in December 2016 the ISPCC conducted a shared conference event entitled Working to Keep Children Safe Online. This was attended by cyber safety specialist, industry experts, policy makers, child protection professionals and educationalists.
2- Findings from the conference report which will be joined with findings from a consultative event with young people to be held in March 2017. One clear outcome from the conference was the need for a National Cyber Safety Strategy for Children.
3- A consultative event with children and young people will be held in March 2017 to explore their experiences online, the findings from the expert-led conference and provide feedback on what is required in a National Cyber Safety Strategy for Children
4- Guidelines for parents on keeping children safer online https://www.vodafone.ie/foundation
5- ISPCC and Vodafone are planning a piece of major research on children and young people's online behaviour that will explore how children make decisions online and inform future practice in supporting young people to build resilience and stay safer online.

The clear purpose of all of the above work is to inform best practice in the area and to effect change in the policy landscape through achieving a National Cyber Safety Strategy for Children.

2.4 The ISPCC's Cyber Safety Interagency Work

The ISPCC has worked extensively over the years with stakeholders regionally, nationally and internationally to progress children's cyber safety. The ISPCC is part of the Safer Internet Ireland Project coordinated by the Office for Internet Safety where we work alongside the National Parents Council (Primary), the Professional Development Service for Teachers ((Webwise) and Hotline.ie. The ISPCC is also a member of the Internet Safety Advisory Committee and eNACSO the European NGO Alliance for Child Safety Online and works closely with An Garda Síochána too. Childline is a member of Child Helpline International also. Most recently, we are a member of the Ministerial Task Force on Mental Health, and are also a member of the Better Outcomes Brighter Futures Advisory Council, which advises the Minister for Children and Youth Affairs.

The ISPCC is an advisory member to the Tacklebullying.ie website. An innovative feature of the website is the forum which gives young people in Ireland a unique opportunity to learn, get advice and talk to their peers or, one of this sites moderators, who are trained in how to deal with bullying. This platform facilitates a safe moderated supportive environment for young people who have experienced any form of bullying. This forum is another example of how technology can be used in a positive way to support children and young people.

At a local level the ISPCC is represented on the internet safety sub-group of the Galway and Roscommon Children's and Young People's Services Committee (CYPSC).

3. The ISPCC's Review of Cases involving Cyber Safety: Findings and Case Examples

As outlined above, based on our knowledge and experience, the ISPCC has highlighted over the last number of years a number of key concerns with regards to children's online safety;

1. Cyberbullying

2. Excessive Time Spent Online
3. Access and Exposure to Inappropriate Content
4. Sexting
5. Online Grooming
6. Sextortion
7. Identity and Wellbeing
8. Lack of Knowledge and Skills

In order to further explore these issues, a thematic analysis of data on cyber safety concerns from across the ISPCC was carried out and the main findings are outlined below:

3.1 Cyber bullying

Cyber bullying featured as the most prominent theme within our review. When bullying happens online, using social networks, games and mobile phones, it is often called cyberbullying. A child can feel like there's no escape because it can happen wherever they are, at any time of day or night.

Key Findings

- Very young users of the internet are learning to **perceive aggressive, threatening and bullying behaviour online as the norm**.
- Staff encounter cyber bullying in up to one-third of their client cases.
- Cyber bullying happens within "Group Chats" which are hosted by mobile messenger applications such as Viber and WhatsApp.
- Some young people can deliberately manipulate and edit WhatsApp messages to make it appear that someone said something when they did not. This content is then spread/shared and used to humiliate a young person.
- In some cases children think that the purpose of social media is to taunt and insult others and this is becoming increasingly normalised.
- Information from children who call Childline demonstrates that children are not always aware who is bullying them

- Calls to the ISPCC support line show an increase in concerns from parents regarding cyber bullying/use of social media platforms etc. Also, parents reported that they did not have a good understanding of how to deal with cyberbullying

Case Studies

Case Example: 14 year old girl who was invited to a group chat thread which was created for the purpose of bullying her. Having seen the negative comments about her by friends, she opted to "leave the group" but was continuously re-added by other members. She felt she had no control over her exposure to the taunting and felt it was "non-stop".

Case Example: In another case a 14 year old girl reported having being deliberately excluded from Viber chat groups. A staff member also worked with an 11 year old boy who spoke about feeling left out by his peers because he did not enjoy using Snapchat like they did.

Case Example: This staff member talked about a case where a parent responded to offensive messages with an offensive message in "defence" of their child. Another parent had a contrary response when they discovered that their daughter (10 yr. old) and her classmates set up an Instagram account to "hate on" another girl. The parent found out about the account and had it closed down.

3.2 Time Spent Online

This is an area of serious concern as excessive amounts of time online can lead to social isolation. mental health difficulties and a lack of physical activity.

Key Findings:

- Some children are spending in excess of five hours a day online – this can be on social media platforms, gaming and chat rooms.
- There is a belief by some parents that because young people are in their rooms, they are safe but there was a lack of knowledge about what sites their son/daughter was accessing or with whom they were engaging.
- Children as young as five reported to have unlimited and unsupervised access to the internet.

- The age from which children receive their first smart device (i.e. tablet, phone or laptop) is decreasing.
- In cases of parental separation, access to the internet was often an area of conflict between parents and this was often brought to the attention of the judge during custody and access agreements.
- Through the support line the issue of excessive time spent gambling was also identified as a concern.

Case Studies

Case Example: At the Ferrybank Network Sub-Group which is focused on internet safety, the ISPCC heard from staff at the local community crèche who were extremely worried as to the impact of spending excessive amounts of time online for very young children. District nurses at this network also noted how parents and carers of very young children appeared very proud of their 18 month old babies' digital skills and liked to show nurses how their infants were able to access their mobile phone or navigate a tablet with ease. This highlights the need for education for parents/carers on how to make decisions regarding age-appropriate use of technology.

3.3 Access and Exposure to Inappropriate Content

Accessing and viewing of inappropriate content is a major concern identified by the ISPCC and also widely reported in the media.

Key Findings:

- Some children and young people were coming across this inadvertently while others were seeking out this content.
- Some of the inappropriate content was being shared peer to peer.
- The ease at which children can access inappropriate/explicit content is concerning
- The impact of exposure to sexualised imagery is impacting children's behaviour online.
- Young people logging onto adult sites or under age children using sites with higher age limits.
- Children are sometimes exposed to pornography on friends phones or in friends' homes – this is concerning as parents may feel they have

set firm boundaries and supervision in place but need to cognisant of the fact that they are not an control of how other parents monitor safety online.

- Our Children's Advisory Committee (CAC) has stated that children have to "...grow up too fast" because of their access to the cyber world. They believe that some children are possibly being exposed to inappropriate material online on seemingly innocuous platforms such as YouTube.
- The support line received 53 calls from members of the public directly related to cyber safety. Callers were seeking advice on how to respond to a situation, on how to support someone, on how to report concerns and seeking legal advice and the key concerns are highlighted below.

Case Examples

- Children exposed to sexual content online
- Concerns about accidentally seeing child sexual abuse material online
- Concern for child accessing self-harm sites online
- Inappropriate content/messages on Facebook
- Concern regarding young person using an adult dating site
- Concern for young people swapping/sharing pictures of themselves self-harming on Snapchat
- Child experiencing ongoing bullying who is accessing suicide websites
- Concern that child sending/receiving explicit content on Snapchat about a vulnerable girl

3.4. Sexting

Sexting is the sending or receiving of sexually explicit messages or images by text messaging or via email. It is an area of serious concern and is becoming more and more a feature of our daily work.

Key findings

- The levels of stress and anxiety created by reputational damage from sexting is evident from calls to Childline, the support line and through our face to face work.
- Young people are feeling pressurised to share self-generated sexual images, with many considering it the new online version of flirting.
- Schools reported that girls were self-generating images of themselves and these were being shared amongst students. Some girls are feeling pressure from their friends to send an image but are then often criticised for this behaviour.
- Blackmail is being used to persuade young people to take images of themselves with one young caller to Childine stating "he will break up with me if I don't"
- Parents find it difficult to talk to their young person about this issue

Case Studies

Case Example: A 16 year old girl was referred to the ISPCC child and family support service due to concerns of her sharing intimate pictures and content with male peers. Within sessions this girl discussed male students in her school sending her unsolicited inappropriate pictures and she said that this was a common problem in her school. She became the recipient of explicit messages and pictures long after she had engaged in sharing explicit pictures of herself. She was concerned about the implications for her reputation which she felt was blighted due to her past decisions.

Case Example: A staff member reported the young age at which some children are engaging in this behaviour and they referred to a nine year old girl sending nude photos of herself to boys in her class.

3.5 Online Grooming

Online grooming occurs when a perpetrator builds an emotional connection with a child online. This happens through the development of a relationship and the perpetrator gains the child's trust for the purpose of sexual abuse or exploitation. The process of grooming happens when a perpetrator of the abuse initiates an innocent relationship yet manipulates this for sexual gratification or exploitation. The anonymous nature of the cyber world is used as an advantage to hide any threat. Technology has changed the manner in which young people are groomed. In the past perpetrators could spend considerable time building up a relationship

with their victim. Now perpetrators can groom many young people simultaneously and within a relatively short space of time.

- Parents have contacted our support line, concerned about grooming via gaming networks and chatrooms
- Children are engaging with people they do not know online. In some instances, a seemingly innocent online interaction can escalate to a more sinister situation.
- It is difficult for young people to recognise if they are being groomed until the situation has escalated to a dangerous level. An Garda Síochána have reported that children are being groomed in 3-4 interactions.
- Young people are less likely to talk about grooming than other issues because of shame or painful personal feelings associated with this form of abuse.
- The CAC raised concerns about the danger of "catfishing" a term they used to describe how people create a false identity online, this is not always done with malicious intent, but it could be used as a means for predators to have access to children. This highlights the importance of being aware of how easily fake accounts and profiles can be created.

Case Studies

Case Example: In one particular case a parent phoned the service for support as they had been made aware that their child was being groomed by an online paedophile ring. This fearful experience impacted on the emotional wellbeing of the whole family.

Case Example: One example they gave was when a 17 year old girl called Childline to talk about how she had been on a website where you can chat via a webcam, to anyone in the world, anonymously. She was talking to someone she felt she could trust. During their chats the caller said that she had undressed while she was on the camera. Following this she realised the person she was communicating with was not who they said they were and she was afraid they had recorded the images of her. This young person was terrified and cried hysterically throughout the call. She was close with her family and had close friends but was adamant she wanted no one to find out. She was anxious about how this would affect

her future and whether the images would be put online. She was hurt and embarrassed that she had believed this person was who they had portrayed themselves to be.

3.6 Sextortion

Sextortion refers to a broad category of sexual exploitation which is marked by a threat of public humiliation, an abuse of power and for young people it often takes the form of threatening to release sexual images on social media sites and apps as a means of intimidation. They can threaten to publically release private images to intimidate or hurt their peers due to fall-outs, relationship break up's or revenge. In some cases young people are sometimes blackmailed for money or asked to send further intimate pictures or coerced into doing sexual acts in attempts to stop a perpetrator from sending their personal images to others.

Key Findings

- Through Childline online service where young people have talked about their concerns and fears for others "blackmailing and threatening to share their private information" online.
- Fear and anxiety regarding people's private information and images being stolen is a recurring theme for young people, with the damaging effects being far reaching from financial, emotional and reputational. In one case, two friends had exchanged nude pictures, but after a disagreement one of the friends posted the nude pictures of her friend on her parents' Facebook page as an act of revenge.
- In a recent worrying case a girl contacted the ISPCC after being threatened online. Conversations and photos from her boyfriend's Snapchat account had been stolen and posted online without her permission. Her original intention- to share personal information with her boyfriend in a private setting was spoiled. Faced with comments online about her personal life, her looks, her behaviour, she was distraught.

Case Studies

Case Example: A Childline volunteer spoke about how two friends aged 14 called Childline together one evening. They talked about how they had sent pictures of themselves "in their underwear to a guy they had

randomly met online". This person had taken screenshots of the pictures and was threatening to post them online unless they sent him more pictures. The girls were very distressed and unsure of whether to respond to this person's demands or not. They did not want to speak to anyone about it and they did not want the Gardaí to know because they were afraid of being judged and talked about in school. They felt their only option was suicide. This indicates the level of stress the friends experienced, they continued to engage with Childline but during the call they felt there were no viable solutions to this situation.

3.7. Identity and Wellbeing

For young people identity development was forged through a dynamic interplay of validation from family, friends and peers, and personal experiences along with biological factors. The cyber world has added a new dimension to the development of identity for young people. Children and young people have always sought out validation and recognition of their identities. This behaviour has remained the same, but what is different today is how young people seek that validation; the level of exposure to the limitless supply of people they can now compare themselves to. In the context of this report the theme of identity and wellbeing refers to the impact online activity can have on one's own sense of self and mental wellbeing.

Cyber identity, particularly on social media sites is a mixture of true and exaggerated events, interests, activities and images. The digital culture is changing the way children and young people play, interact, learn, communicate and experience the world with them seeking identity validation not only from friends, family and people in their community, but now from strangers – through online activity. The challenges that faces young people today are to be able to recognise the dynamic interplay between their real and cyber worlds and protect themselves from the negative impacts online activity can have on their view of their self.

Key Findings

- Childline callers report that they feel sad because they don't get 'likes' on Facebook. This has a huge impact on their self-confidence and self-worth.

- The pre-teen & teenage years are typically the time when young people struggle with their identity, this can be compounded by their experiences online. Staff talked about concerns for young people with poor self-image and how these negative experiences impacted their self-esteem, their confidence and their relationships along with their overall wellbeing.
- Young people are using photo shop technology to 'enhance' photos before they post them online

Case Studies

Case Example: Another client Carrie* who was 12 years old had engaged in arguments and disputes with friends through WhatsApp and Viber and she talked about how her friends were not responding to her messages in group chats and the hurt she felt as a result of this. Carrie struggled with her confidence as a result. She was deleted from a Viber group set up by her peers, this exclusion had a huge impact on her emotionally, of which she required emotional support to help her overcome this negative experience.

3.8. Lack of Knowledge and Skills

Throughout the review it is clear that a pattern of confusion was emerging for our service users. Children and young people felt unable to control inappropriate activities, they were unsure of where to turn or how to address concerns. Parents were particularly feeling ill-equipped to deal with issues of safety online. Feedback from our external network say that parents are not knowledgeable on cyber safety and this was reiterated by the ISPCC's CAC.

Key Findings

- The sharing of inappropriate pictures was a problem in schools, and young people did not know what to do to stop this.
- Young people did not know how to stop receiving inappropriate messages on Snapchat.
- Children and young people were not aware of risks from online predators or hackers, they did not know how to spot unusual activity or how to respond if approached online by someone unknown.

- Fear of exposure is blocking people from accessing appropriate supports and advice. It is also preventing young people from speaking to friends and family about their experiences, which only isolates them more and can put them in a more vulnerable position.
- Childhood support workers felt that some young people were over sharing personal experiences online and did not anticipate the negative responses/comments they would receive. For example: a 13 year old was regularly accosted by a group of teenagers while out in public areas–they were able to tell her location because of her online "location check-ins".
- General knowledge on reporting and responding to inappropriate online activity.
- Parents are unfamiliar with their children's online activities.
- Parents are unsure how to respond to cyberbullying; for example: who do they report to, how do they report concerns?

4. ISPCC Key Recommendation:

Ireland requires a National Strategy on Children's Cyber Safety. The Committee should recommend the immediate development of this as a priority by government.

The potential components of such a strategy are outlined below:

4.1 Recommended Strategy Component: Implementation of Key Education Measures regarding Online Behaviour

Education and Support for Children

Technology has many positive impacts on the lives of young people but the ISPCC's work has informed us that our education system and society are failing to prepare children to identify and understand online risks. Cyber safety education needs to be twofold; empowering on the positives of the internet and educating on the potential dangers, while ultimately building online resilience. Children need to know what options are available to them should they encounter certain risks.

- **Curriculum:**

Within the broader curriculum, from primary level onwards, children must be supported to become more aware of issues that can arise when posting and publishing online as well as the dangers of exposures to harmful communications. The UK government made internet safety a compulsory part of the new curriculum in 2014. Schools can also teach e-safety during PSHE lessons and they are all required by law to have measures in place to prevent bullying and cyber bullying.[2]

- **Resilience building**

Children need to be supported to build their coping skills and online resilience, to make the right decisions. They can be experts in the actual technology but not necessarily capable of using it in the right way. This is

a key issue, and one which underpins all of the educational measures required.

- **Sex Education**

The current sexual health education of children at primary school level does not reflect the digital world and the changing environment that they live in. Education around cyber safety needs to be made part of the primary school curriculum. From 4th class on children should be educated and made aware of how they can protect themselves online.

The ISPCC knows that children are now exploring their sexuality more online. However, the unintended consequences of this are not being explored. This issue needs to form part of sex education in both formal and informal settings.

- **Freedom of expression and privacy**

Through education, children should be informed of the importance of balancing the right to freedom of expression with the right to privacy.

- **Empathy and online behaviour**

It is evident from the case examples highlighted in this briefing that many children and young people can behave differently online than they would do in a similar face-to-face situation. Young people can experience a lack of empathy when behaviour takes place behind a screen. They are not always fully aware of the implications of posting nasty commentary about others.

- **Legal and other Implications**

Children should be educated on online behaviour and made aware of potential legal and other consequences of this behaviour.

Education and Support for Parents

- **Establishing safe and healthy boundaries**

A coordinated approach is needed to support and educate parents on establishing safe and healthy boundaries and ground rules at home

around acceptable internet usage. This would help to highlight the importance of supervision and monitoring while ensuring better child protection online.

- **Education on risks and consequences**

Education needs to be provided around the risks, reach and consequences of certain online behaviours and sites being visited (gaming, etc.) by children and young people. Some parents are aware of sites being visited but may not be aware of potential dangers. Cybersecurity issues and practical options of what to do when certain issues are encountered need to be explored

- **Recognition of parents' support role**

Parents need to familiarise themselves with the platforms their children are using and engage in open conversations about them. This can help to create an environment where the child knows they can speak to their parent without being judged.

Support for Teachers

- **Training on Impact of online behaviour**

Teachers would benefit from training to help spot the signs or impact of harmful behaviour online –the risks, reach and consequences of certain online behaviours. This training should equip them to be open to the possible danger signs that may be exhibited in a classroom.

- **National Guidance on supporting children who have accessed harmful material**

National guidance is required for teachers to support them in handling situations where children have knowingly or unknowingly accessed harmful online material.

- **Appropriate Training**

Where curriculum materials are developed to embed cyber safety awareness in key subjects, e.g. SPHE, appropriate training should be provided.

Raising Awareness

As technology increasingly becomes embedded in daily life it is essential that young people are well informed about all aspects of the cyber world. Targeted national media campaigns on cyber safety are needed, which should be developed with key stakeholders.

4.2 Recommended Strategy Component: Reform of Law regarding Children's Cyber Safety

The current legislative landscape has not kept pace with the advances in technology with regards to the protection of children online. The sharing of personal information without someone's permission has become an extremely harmful form of activity, often undertaken as part of a broader tactic by criminals to exploit individuals. The shock of finding out that photos or personal information has been shared leaves the person extremely vulnerable, and often prevents them from making the right decision, i.e. speaking to a trusted adult. Instead they often agree to the demands of the criminal – which can include sending further intimate photos, money or both.

This has a profound effect on children and young people in particular because it is such a breach of trust and privacy. Adults are usually better equipped to deal with the problem, to recognise exploitation and extortion and better able to understand who is at fault. Many young people blame themselves, and fear reporting this behaviour in case they are held responsible.

It is vital that while a legislative response is necessary, it does not seek to criminalise children and that laws are supported by education and support to empower children to navigate the online world safely.

- **Enactment and Implementation of the Criminal Law Sexual Offences Act**

The ISPCC welcomes this recently passed Act but it must be enacted and commenced in full with haste.

- **Implementation of the Recommendations of the Law Reform Commission in relation to the reform of the Criminal law**

The law cannot necessarily prevent young people from engaging in risky behavior online – it cannot and should not criminalise children;

however, it can and should make it as difficult as possible for criminals to target and exploit children. In September 2016, the Law Reform Commission grasped this challenge with the launch of its report *Harmful Communications and Digital Safety* which set out how the law in Ireland needs to change. The ISPCC has warmly welcomed its recommendations and called for swift implementation.

- **Blocking, Filtering and Peer to Peer Networks**

The nature of crimes against children online has changed. Technology, online platforms and social media are used effectively as tools by individuals who have a criminal interest in children, to target them, communicate with them and exploit them. It is vital that the legislation makes this more difficult for people who seek to prey on children

- **Legislation needs to be underpinned by a National Cyber Safety Strategy for Children**

New laws will go some way to responding to insidious behavior by criminals who target children. But they must be matched with a national strategy that gives children every opportunity to enjoy the huge educational and social benefits of technology and social media, in a safe and protected environment.

4.3 Recommended Strategy Component: Establish the Office of a Digital Safety Commissioner and a Policy and Regulatory Framework

Based on data from our internal review there appears to be many independent companies and organisations advising on cyber safety, yet there appears to be no unified or coordinated approach to dealing with these issues.

- **Establishment of an Office of a Digital Safety Commissioner**

The ISPCC recommends that an Office of the Digital Safety Commissioner be established. Its remit could include the coordination of key stakeholders in the development of a national strategy on children's cyber safety. They could lead in research, policy, education and service delivery of all cyber related issues.

- **Centralised reporting and recording of issues**

ISPCC staff noted that there is an under reporting of case of cyber issues. It was suggested that there needs to be a centralised unit or pathway for people to report issues they are facing – this will lead to tighter monitoring and documenting of cyber safety threats and help to develop a more coordinated and effective response if issues are being identified at an earlier stage.

Ill-thought out and spontaneous sharing of images, self-generated or otherwise is a growing problem among children and their peers. Children have told us that there is general confusion about where they can go to report these concerning activities. The ISPCC supports the establishment of the Office of a Digital Safety Commissioner with responsibilities as outlined in the Law Reform Commission's Report.[3]

Children have reported to us that effective take down procedures are a key ask for them when it comes to online safety. Adequate resourcing and cross sector support will be fundamental to an effective and functional Office of the Digital Safety Commissioner.

The Office of the Digital Safety Commissioner's role should encompass the following:

- Advise government on law, regulation and policy in this area
- Under take an educational function to build awareness of risks to children
- Oversee a Code of Guidance for the industry and monitor compliance with that code
- Have an investigatory role to respond to complaints as well as power to undertake 'own initiaitve' investigations

Industry has a role to play in ensuring that when they sell any technological device or connected toy that they educate both children/young people and parents/carers on safe and responsible use. This office should have a role in promoting this, so that industry organisations that are doing good work can be recognised, and those that are not adequately protecting children online can be sanctioned.

[3] http://www.lawreform.ie/_fileupload/Final%20Report%20on%20Harmful%20Communications%20and%20Digital%20Safety%2021%20Sept%20PM.pdf pgs 157-159

5, Appendices

5.1 Excerpts from **Relevant External Studies / Research**

Law Reform Commission Report on Harmful Communications and Digital Safety September 2016[4]

The ISPCC supports the recommendation of the establishment of a statutory body to promote online and digital safety and to provide oversight of "take-down procedures" operated by online service providers such as social media sites. The recommendation to focus on education with regards to digital safety in the report is key to ensuring that young people are better equipped to navigate the online world safely.

Cyberbullying in Ireland A survey of Parents' Internet Usage and Knowledge – National Anti-Bullying Centre at Dublin City University (DCU) 2016[5]

Over 900 parents of 9 to 16 year olds answered the online questionnaire. In summary, the survey revealed that while Irish parents perceive themselves to be vigilant in monitoring computer and internet usage, there is an over-reliance on their children giving them accurate accounts of their online activity – especially on social media, where only 18% of parents supervise activity. And while many children may show honesty in this area, there is also a well-established "digital deceit" pattern in pre-teen and teen dealings with their parents that can leave them vulnerable online, especially to cyberbullying. [6]

Zeeko Digital Trend Report 2016[7]

Highlights of the trends in 2016 include;

- 86% of primary school children use a mobile device (smart phone, tablet or iPod).
- Children are starting younger to use the internet (on average 1st class students first went online at 4.9 years old vs 6th class students first went online at 7.6 years old).

---

4 http://www.lawreform.ie/_fileupload/Reports/Full%20Colour%20Cover%20Report%20on%20Harmful%20Communications%20and%20Digital%20Safety.pdf

5 http://www4.dcu.ie/sites/default/files/institute_of_education/pdfs/ABC-Cyberbullying-Survey.pdf

6 Ibid. Pg. 4

7 http://zeeko.ie/press-3/

- 66% of primary school children self-report they know more about online games than their parents and 59% self-report they know about Apps then their parents.
- 34% of primary school children have more than 2 hours screen time per day during weekdays, rising to 54% having more than 2 hours screen time per day at the weekend.
- Cyberbullying: Percentage of primary school children who reported being cyberbullied
    - 1st class 7%
    - 2nd class 13%
    - 3rd class 15%
    - 4th class 10%
    - 5th class 11%
    - 6th class 12%.
- Snapchat has taken over Instagram as the most popular social media app with 45% of 6th class pupils using Snapchat.
- % of children who see the following as serious or very serious
    - Cyberbullying, 77%
    - Talking to a stranger online, 58%
    - Digital footprint, 40%
    - Spending too long online, 40%.

Older boys engage in risky behaviour online, of 6th class boys surveyed 34% spoke with a stranger online, 70% played with a stranger online, and 60% played an over 18 game online.

Webwise Parenting Survey 2017[8]

- 45% of parents say the risks to children of using the internet outweigh the benefits. This is a sharp increase on 25% in 2012.

[8] https://www.webwise.ie/news/webwise-2017-parenting-survey/

- Exposure to pornography (71%) and cyberbullying (70%) remain prominent risks cited by parents just as they were in 2012.
- Four main risks stand out in equal numbers as the most serious concerns for parents: Cyberbullying; spending too much time online; online grooming or sexual exploitation, and Accessing pornographic content.
- The ranking of top parental concerns remains the same irrespective of the age of the child.
  Some parental concerns increase with the child's age (e.g. accessing pornographic content and damaging their reputation) while other concerns diminish as the child grows older (e.g. online grooming and sexual exploitation).
- The concerns that worry parents the most are those that pose a direct threat to the child, e.g.
  cyberbullying and online grooming, despite the fact that actual incidence is rare.

ISPCC 2016

The ISPCC conducted a brief survey with young people attending a young person's event in Dublin in October 2016.

- 283 children and young people surveyed.
- Age Range -13 years old -19 years old
- Average Age of respondents: 15.5 years
- Children reported spending an average four hours online on a school day and over seven hours online on a non-school day.
- 86% of respondents had no parental controls installed on a device they use while 36% reporting feeling unsafe online.

5.2 ISPCC Case Studies

Cyberbullying

Case Example: One support worker spoke about the case of an 11 year old girl who disclosed that she was being bullied on Facebook. When her mother was made aware of this, the child was made to block to the bullies. The child suffered from low-esteem and appeared to think that bullying and taunting via social media was normal and happened to everyone. The child's mother was quite active on Facebook and had been involved in some online altercations herself, of which the child was aware.

Case Example: Another ISPCC Support Worker talked about how a young person they worked with received a "very nasty message from a friend". This act was perceived as the norm by the young person, in that it was ok to write hurtful comments and send them or make them public. In their work they talked about how easy it was for someone to detach from the accountability of hurting someone, the young person noted that it was easy for people to "hide behind a screen".

Case Example: In another case a young person had to move from their school due to bullying, she settled in well to her new school and had made new friends however she reported how she was still getting nasty messages online from friends in her old school. Social media in this case definitely prolonged the stress and anxiety for this young person and eliminated the protective barrier that distance or separation could provide.

In another example it was noted how many of our workers had come across many clients who had experienced a mixture of cyberbullying on Facebook and Snapchat alongside more traditional forms of bullying which were carried out face-to-face. For this staff member she felt that it is easy for young people to write an offensive message online and to minimise the impact they are having. Support workers highlighted that young people show a lack of empathy when these comments are posted online compared to face-to-face with someone. When cyberbullying occurs it is easy to forget that there is a real person with thoughts and feelings on the receiving end. There is a detachment from the act and therefore a lack of accountability and acknowledgement regarding the potential negative effects this type of online activity can have.

Case Example: One childhood support worker noted that in the review of her work over the last 18 months one third of the cases had a cyberbullying element to them, however they were not the main reason for referral. For these young people they were both the perpetrator and the victim of cyberbullying and she noted that many parents and young people often felt that responding to cyberbullying would aggravate the situation but the concept of "they started it and standing up for yourself" was used as a rationale for reacting with offensive or hurtful comments. These conflicting ideas demonstrate people's inability to respond to these situations appropriately.

Case Example: Sue* is 14 years old and is being bullied by a group of people from her school in an online chat group. She said this has been going on for the last few months and it makes her feel bad. Recently she spent the weekend hanging out with a boy in her year, he posted pictures of them together online and since then girls have been calling her names like slut...Sue said that she feels the only way to stop the bullying in school is to strike back the same way at the bullies. She talked about feeling very bad and stated that she doesn't care if someone kills me anyway. Sue said her parents and teachers are worried about her but this makes her feel she is a problem to everybody.

Case Example: Caller was a 16 yr. old girl who was being bullied in school by a group of girls. She was hoping she "would get a break over the summer" but they started targeting her online and by phone. She felt there was no escape from the bullying. They were sending her messages threatening her safety and telling her to take her life by suicide. She was nervous about reporting it for fear the bullying would escalate.

Excessive Time Spent Online

Case Example: A support worker talked about her concern relating to a young person engaged with our Mentoring programme who had a poor peer support network in "real life" but had many friends online whom they had never met. Furthermore, this young person did not seem concerned by their lack of "real life friends".

Case Example: A staff member pointed to the ongoing conflict between a teenage boy and mother regarding the amount of time he spends on his phone. According to his mother "he is never off that phone". On further

discussion it was discovered that this boy's mother had never discussed boundaries or rules regarding phone usage and provided credit for downloads that she knew very little about. So while the parent in this case was concerned about the amount of time their child spent on their phone, they were also enabling this to happen.

Sexting

Case Example: "Another issue that came up with some young people is sexting. One of the young people I worked with told me of issues relating to a friend who had sent nude pictures which were then posted to her friend's parents' Facebook page as an act of revenge. My client had a good relationships with her mum and would have had open discussions about nude pictures and sexting, it was something she was encountering and one boy was requesting of her. This happened during our intervention so she was able to be assertive about it but I would wonder if someone has low self-esteem and hasn't supportive relationships what would happen."

Case Example: A staff member reported how a 12 year old girl she worked with had been sharing sexualised content online and that this was reinforced by her mother who would comment "look at my beautiful daughter." Following the uploading of this content, this girl received threats and rumours were spread about her regarding alleged sexualised behaviour. This young girl is now in care and the court has ordered that she have no access to Wi-Fi, however, she does buy credit when she can.

Childline Online reported that young people as young as 10 and 11 were presenting to this service to talk about sexting. Childline reported that some young people explain that they have used sexting as a way to express or explore their sexuality. However some young people contacted Childline after they had sexted as they were worried and concerned as to any possible long lasting consequences for them, e.g. who could have saved their image, etc.

Online Grooming

Case Example: In the case of Jay* a 15 year old girl who contacted Childline Online, she talked about how she had recently met an "older guy" online, someone she "did not know in real life" and they had been talking for a couple of weeks. She really enjoyed talking to this person

online but suddenly he started asking if she would like to send "nude pictures of herself" to him. Jay was very concerned and confused about this, she felt embarrassed and was unsure if it was "right or wrong". She felt pressurised to send the pictures but was worried about being thought of as "frigid". Jay was also concerned that if she did send the pictures that this person could put them online, even though he had reassured her that he would not do this.

Jay had not spoken to friends or family about this and talked about how her family would not be happy and she may have her phone confiscated. She spoke about how this would be done to protect her. Jay spoke in more detail with Childline and towards the end of the engagement she said she felt more confident to end the contact with this person. Jay's case study highlights the conflict that can occur when a young person is being groomed online; while she was aware of the risks and dangers and recognised how this situation made her feel uncomfortable, she still felt extreme pressure to comply with the demands of the person grooming her. This person had initiated contact with Jay, built trust, and then manipulated this relationship to try to extract sexualised images from Jay. And, while Jay reached out to Childline, it is also a concern that she felt unable to speak to her friends and family about what she was going through. It highlights how relatively quickly an online relationship was established and how easily a risky decision could be made in haste when under pressure.

Case Example: A 12 year old female client of the Childhood Support Service. This young person was very lonely, disconnected from her parents and had no real friends in whom she could confide. This young person turned to social media for company and connection. During sessions she talked about how she had recently been in contact with an adult in America via Facebook. The childhood support worker was very concerned that this young person displayed no understanding of the risks or potential consequences of developing an online relationship with an unknown adult.

Identity and Wellbeing

Case Example: Jack* who was 16yrs old was a client who shared his difficulties with low self-esteem which he felt were affected by using

Facebook and subsequently resulted in him feeling inadequate when comparing his life to his peers. Jack had low self-esteem and felt that others' lives compared better to his. Jack struggled with mental health difficulties and he discussed using social media to gauge positive reactions from others and feeling let down and low in himself when this didn't match his expectations.

Case Example: One staff member talked about a client who had posted a photo of herself on rateme.com asking other people to rate her appearance. For this 12 year old girl, "this was a normal thing to do". She explained how her friends do it all the time, but when the staff member explored the situation with her further it was clear to them that her self-image and self-esteem were greatly dependant of ratings from others on this site. This is also validated by the increase in picture filtering options/image altering apps (e.g. BeautyPlus) on technology that are now in high use by young people.

Lack of Knowledge and Skills

Case Example: The following case describes a call from Mia* who was 14 years old, she contacted Childline saying she had been asked to send a "nude" picture of herself to a boy who she had befriended on a social network site. She did not know him previously. His first interaction with her was to ask for a "nude". Mia contacted Childline looking to see what she should do; should she block him or "mess around" with him first. By messing she meant chatting. Mia said he looked "hot" in the pictures he had sent her but she did not know if these pictures were genuine. Childline explored with her if she thought it was safe to send pictures to somebody she did not know. Mia said she was not quite sure now, but since she didn't know him, maybe not. Childline informed Mia that once a picture is sent to anyone, you no longer have control of who sees it or where it could end up.

Childline explored how Mia would like to be treated by boys. She said she would like to be respected and not criticised for everything she does (like her ex-boyfriend did). Childline then explored if Mia thought the boy was showing her respect by asking her for a nude picture. Mia told Childline this was not the first time she was asked to send a "pic" of

herself to someone, there was another time, on a dating app she had "randomly downloaded", but that she has since deleted it. She could not remember the name of it. Mia went on to say she had blocked this "guy", but wanted to know if he will get mad. Childline explored with her if it mattered to her, if he got mad?

Mia also said she had almost 1,000 friends online, but she now thinks she should start checking who she is adding. She questioned if some "pics" are real. Childline explained that unless we actually know the person, we cannot be sure that they are real. Mia asked if she gets a "pic of a guy's thing" should she chat with them or block them. Childline reflected that they had chatted about respect earlier and did she feel respected when she received pictures like that? She said it makes her feel "disgusting". Mia said she deleted that message and blocked that guy now too. Mia asked was it weird that she was only 14 and had experienced "all these". Childline validated that she had shown maturity by how she was dealing with the situations. She was directed to the ISPCC and Childline websites to look at information available on protecting yourself online.

What is significant about Mia's case is her response to this situation, it demonstrates the lack of knowledge and skills some young people have when presented with challenges online. The call from Mia clearly shows the vulnerability of some young people online. It shows how Mia struggled to understand what is considered appropriate online behaviour. It shows the ease with which unknown people had on numerous occasions contacted her and how these encounters are becoming normalised for young people. From her story Mia has experienced real confusion about whether to engage or not with this person, she is unsure how to respond, concerned if she will make them angry and appears to lack the skills to deal appropriately with these situations (by not reporting or seeking support from friends or family). Mia has a sense that some of what she has experienced online is not acceptable (makes her feel disgusting) but this is being challenged by the frequency of these encounters and what she is observing. It has also highlighted her lack of awareness regarding privacy settings, which may have been overridden by her want to have high numbers of on online friends.

5.3 ISPCC Submissions (Excerpts)

ISPCC Submission into the New National Women's Strategy January 2016

Key ISPCC Priority: Modernisation of Current Sexual Health and Technology Curricula for Children

Ireland's sex education does not meet the needs of children; it is outdated and needs an overhaul in order for children to make informed choices and be better protected.[9]

Children are becoming aware of their sexuality and their desire to explore it at a younger age. Increasingly, they are using online platforms to do this. A recent internal ISPCC case review confirmed the pressure that some children are now under to share self-taken images of themselves with others.

Case Study: A 16 year-old girl was referred to the ISPCC's child and family support service due to concerns regarding the sharing of inappropriate pictures and content with male peers. Within sessions this girl also discussed male students in her school sending her unsolicited inappropriate pictures. This was a common problem in her school. She became the recipient of explicit messages and pictures long after she had engaged in sharing explicit pictures of herself. She was concerned about the implications for her reputation which she felt was blighted due to her past decisions.

In his ninth report Ireland's special rapporteur on child protection Professor Dr Geoffrey Shannon highlights that one of the Sustainable Developmental Goals is to 'Ensure universal access to sexual and reproductive health-care services, including for family planning, information and education.'[10] This new national women's strategy must support this if it is to keep children informed, safe and protected on their sexual health.

CAC Members: Same-sex schools are not equipping girls and boys to communicate effectively with each other. This situation does not reflect

[9] http://www.irishtimes.com/news/education/sex-ed-in-ireland-it-s-all-disease-risk-and-crisis-pregnancy-1.2212770

[10] http://www.dcya.gov.ie/documents/publications/201611189thReportoftheSpecialRapporteuronChildProtection.pdf pg. 69

reality where girls and boys will be mixing with each other. Programmes in schools should teach everyone to embrace difference.

OUTCOME: Revised and Updated Positive Sexual Health Education on National Curriculum

By failing to ensure a mandatory and consistent approach to sex education, we will fail to keep children safe. This education needs to be developed age-appropriately, to include children in primary school. The curriculum should teach young people about autonomy, consent and other important concepts to enable them to build their resilience. Children, girls and boys alike, need to be educated positively on their sexual health. They need a platform where they can speak openly about this and their sexuality; a space where they can learn and develop emotionally and psychologically, not just where facts are handed down with little opportunity to discuss them further.

ACTION 1: Review Current Sexual Health Education

A review of current sexual health education is required in order to revise and update it to make it relevant to children today. A proactive modernisation of our sex education curriculum which meets the needs of children is urgently required.

ACTION 2: Consultation with Children

Children need to be part of the discussion on any proposed updates on the reform of sexual health education. A public consultation seeking input from children is required. Any consultation with children should be child-centred, participatory and meaningful. The children's consultation unit in the Department of Children and Youth Affairs has a lot of resources on this.

OUTCOME: Better Understanding of the Role of Technology in Children's Sexual Health Exploration

Our support workers have found that sending self-generated intimate photos as a new form of flirting is increasing in prevalence among children. Some consider this a "safer" way of exploring their sexuality while engaging in sexualised behaviour. Unfortunately, our internal case review has shown, this is not always the case. The resulting 'body

shaming' (publicly making the person feel embarrassed about their body and about their behaviour portrayed in the images) can be devastating for the child or young person, and in some cases, can lead them to contemplate self-harm or suicide.

ACTION: Empowering Children to be Safe when using Technology to Explore their Sexuality

For many generations in Ireland talking, even thinking about one's sexuality was taboo. Today's children are not so inclined and many talk openly about their sexuality and sexual activities face to face with their peers and online; sometimes with people they know, sometimes with strangers.

From primary level onwards, children must be supported to become more digital savvy: they can be experts in the actual technology but not necessarily capable of using it in the right way. We need to communicate the importance of balancing the right to freedom of expression with the right to privacy. Information and advice for parents and guardians as well as for teachers and educators must be improved, both by government and by industry providers.

The need for regulation for industry and the role of industry in self-regulating must also be considered. Organisations which benefit from the use by young people of their platforms and apps online must have robust protection systems including easy to use reporting and swift take-down procedures where issues arise.

Key ISPCC Priority: Commitment to Developing a National Strategy on Children's Cyber Safety

The recent report on Harmful Communications and Digital Safety from the Law Reform Commission referenced two studies which showed that girls disproportionally experience bullying, including cyber bullying compared to their male counterparts.[11]

One ISPCC case study highlighted how one client told their support worker of issues relating to a friend who had sent nude pictures which were then posted to her friend's parents' Facebook pages as an act of revenge. Their

[11] http://www.lawreform.ie/_fileupload/Reports/Full%20Colour%20Cover%20Report%20on%20Harmful%20Communications%20and%20Digital%20Safety.pdf pg. 200

client had a good relationship with her mum and had open discussions about nude pictures and sexting; it was something she was encountering and which one boy was requesting of her. This happened during the client's intervention with the ISPCC so she was able to be supported to be assertive about it.

Children's online safety is the child protection issue of our time. A national strategy must give children every opportunity to enjoy the huge educational and social benefits of technology and social media, in a safe and protected environment.

OUTCOME: Publishing a National Strategy on Children's Cyber Safety

There is currently no national strategy on children's cyber safety. This strategy must include the previously mentioned proactive modernisation of our sex education and technology curricula.

A national strategy on children's cyber safety will need to strike a balance between highlighting the new and emerging risks to children while also promoting the positive aspects of being online. Promoting responsible behaviour online is important.

ACTION 1: Review of Children's Cyber Safety Strategies Internationally

A review of children's cyber safety strategies internationally along with best practices will help to inform a national strategy for Ireland. Australia has established an Office of the Children's eSafety Commissioner where potential learning could be initiated.[12]

ACTION 2: Attain Commitments from Key Stakeholders

A national strategy on children's cyber safety will need the support of all key stakeholders: input from industry, parents and children themselves is paramount. When children are exposed to dangers online they need to feel confident in the relevant internet service providers and/or social networks to support them in dealing with the issue. Parents needs to be engaged in educating themselves on their children's internet usage and be in a position to listen and support their children when required.

[12] https://www.esafety.gov.au/

- **ISPCC Submission to Department of Communications, Climate Action and Environment on the Law Reform Commission's Report on Harmful Communications and Digital Safety January 2016**

ISPCC Key Recommendations

1. **Implementing Key Education Measures regarding Online Behaviour**

It is evident from the case examples highlighted in this submission that many children and young people can behave differently online than they would do in a similar face to face situation. Young people can experience a lack of empathy when behaviour takes place behind a screen. Young people are not always fully aware of the implications of posting commentary about others. Children need to be educated on online behaviour: they need to be made aware of potential legal and other consequences of this behaviour, including what constitutes defamation.

The ISPCC knows that children are now exploring their sexuality more online. However, the unintended consequences of this are not being explored. Children need to be educated about these unintended consequences in line with proposed changes to the law, including this review of the Defamation Act 2009.

Separately, and within the broader curriculum, from primary level onwards, children must be supported to become more aware of issues that can arise when posting and publishing online as well as the dangers of exposures to harmful communications. Children need to be supported to build their coping skills and emotional resilience, to make the right decisions online. They can be experts in the actual technology but not necessarily capable of using it in the right way. We need to communicate the importance of balancing the right to freedom of expression with the right to privacy. Information and advice for parents and guardians as well as for teachers and educators must be improved, both by government and by industry providers.

2. **Establishing the Office of a Digital Safety Commissioner**

Ill-thought out and spontaneous sharing of images, self-generated or otherwise is a growing problem among children and their peers. Children have told us that there is general confusion about where they can go to report these concerning activities. The ISPCC supports the establishment of the Office of a Digital Safety Commissioner with responsibilities as outlined in the Law Reform Commission's Report.[13] Children have reported to us that effective take down procedures are a key ask for them when it comes to online safety. Adequate resourcing and cross sector support will be fundamental to an effective and functional office of the digital safety commissioner.

3. Publishing a National Strategy on Children's Cyber Safety

There is currently no national strategy on children's cyber safety which is hugely concerning to the ISPCC. This must include proactive modernization of our sex education and technology curricula. We are currently failing to keep children safe if we fail to ensure a mandatory and consistent approach to sex education.

Children's online safety is the child protection issue of our time. New laws will go some way to responding to insidious behavior by criminals who target children. But they must be matched with a national strategy that gives children every opportunity to enjoy the huge educational and social benefits of technology and social media, in a safe and protected environment.

ISPCC Submission to Department of Justice & Equality's Consultation Process on 'Age of Digital Consent' – December 2016

Summary of our proposals:

1. Department to consult with children on their views re introducing national legislation on age of digital consent
2. An awareness campaign to inform children and their parents/carers/guardians of the Regulation

[13] http://www.lawreform.ie/_fileupload/Final%20Report%20on%20Harmful%20Communications%20and%20Digital%20Safety%2021%20Sept%20PM.pdf pgs 157-159 Joint Committee on Children and Youth Affairs – ISPCC briefing on Children and Cyber Safety

3. Government should encourage those companies with a base in Ireland who may be processing data as per the Regulation to consult with children to create 'child-friendly' T's & C's.
4. The ISPCC recommended that national legislation set the age limit at 13 years for Ireland where services provided are commercial.
5. The ISPCC notes the recommendations in the Ninth Report of the Special Rapporteur on Child Protection on the 'Right to be Forgotten'. 'Right to be Forgotten' – the age at which a child posts information online should be considered an important factor in decisions whether to remove an individual's personal information from sites (Education piece on this Right is needed).

Appenndix 3 ISPCC Case Review Methodology

In July 2016 the ISPCC's internal working group on cyber safety began a case review of the cyber related issues that the ISPCC had encountered from the children, young people and families with whom we work over an 18-month period. Over 500 calls and 250 online contacts, over 50 calls to our support line (adult helpline) and 30 childlhood support cases were reviewed, along with staff and volunteer interviews and focus groups.

The ISPCC sought to have a clearer understanding of the challenges children, young people and their families were facing and to understand how regularly they were coming across these challenges. **What We Aimed to Achieve**

- A review of data from all our services as well as from the local, national and international networks in which the ISPCC participates.
- Data was gathered from several different sources including our Childline services (phones, text & online), child and family support services, our support line and our interagency networks.

- Recommendations were compiled from staff and volunteers on how we could support children, young people and their families with these issues.
- These case studies would in turn support our media and policy work.

Key Questions Asked

- How often has a cyber related issue occurred within the service during the time period?
- What are the cyber related issues experienced by children, young people and their families?
- Sharing of case studies with peers
- What are the impacts/effects of cyber related issues on children/young people, on their parents/carers, families?
- What more could the ISPCC do to support children, young people and their families on cyber related issues?

Time Frame

We reviewed 18 months' of ISPCC work (from January 1st 2015 to 30th of June 2016.)

Evidence

This review is based on evidence from:

832 Calls to Childline 1 focus group with the CAC

3 External Networks 263 Contacts on Childline Online 53 Support Line Calls 31 Childhood Support Work Cases

16 Interviews with staff and volunteers 1 Case study from Shield Campaign

Main Themes Identified

- Cyberbullying
- Excessive Time Spent Online
- Access and Exposure to Inappropriate Content
- Sexting
- Online Grooming

- Sextortion
- Identity and Wellbeing
- Lack of Knowledge and Skills

While this review focused on the challenges and risks that the cyber world poses for children and young people, it is important to highlight that within the review, the positive benefits that the internet affords to young people were also clearly evident. Yet for the purpose of this review the themes identified relate solely to the risks and challenges that children, young people and parents encounter through their online use and interaction. A greater understanding of these issues will lead to the development of greater protections for children and young people using the internet.

The CAC (ISPCC's Children's Advisory Committee) also expressed the importance of highlighting the positives of the internet; it is helpful for communicating with family members who are abroad; using the internet as an educational and learning tool; a forum to express views and share experiences.

Throughout the review we identified case studies where young people found the internet a huge positive e.g. children moving into a new foster family used online social networks to connect to new friends at their new school. The internet can also be used as a positive tool for emotional support which is evident through our own Childline service.