Tithe an Oireachtais
Houses of the Oireachtas

Tithe an Oireachtais

An Comhchoiste um Leanaí agus Gnóthaí Óige

Tuarascáil ar an gCibearshlándáil do Leanaí agus d'Aosaigh Óga

Márta 2018

Houses of the Oireachtas

Joint Committee on Children and Youth Affairs

Report on Cyber Security for Children and Young Adults

March 2018

32 CYA 011

Tithe an Oireachtais

An Comhchoiste um Leanaí agus Gnóthaí Óige

Tuarascáil ar an gCibearshlándáil do Leanaí agus d'Aosaigh Óga

Márta 2018

Houses of the Oireachtas

Joint Committee on Children and Youth Affairs

Report on Cyber Security for Children and Young Adults

March 2018

32 CYA 011

Table of Contents

CHAIRMAN'S FOREWORD

Alan Farrell T.D.

Internet safety and security for children and young adults is one of the most urgent and pressing child protection concerns facing policy makers, parents and guardians, teachers and, most importantly, children and young adults themselves. For this reason, the Joint Committee on Children and Youth Affairs agreed to consider this complex and challenging topic as part of its Work Programme for 2017, and again for 2018. This is reflective of the importance to which Members of the Committee placed on addressing cyber security for children and young adults in our society.

The internet provides wonderful opportunities for children and young adults to connect with each other, to learn, to explore and to engage with the world around them. In that regard, it is a portal of discovery and a tool for education. There are numerous benefits from increased digitalisation for all ages and Ireland is increasingly at the forefront of exploring, utilising and promoting the digital world.

However, the positive benefits of the internet, while exceptionally important, are not the focus of this Report. Due to the immensely broad nature of this topic, this Report focuses only a number of key areas of digital safety. The aim of the Committee in taking on the topic of 'Cyber Security' was to explore how children and young people can be active participants online, and benefit from the positives the internet has to offer, while ensuring they are protected. The challenges in terms of providing children and young adults with that protection relates to the fact that, when they are using the internet they are engaging in a world with few boundaries, regulations, laws or certainties. The Committee wishes to ensure that child protection is paramount when they are provided with the opportunity to explore the vast digital universe that awaits them.

The Committee notes that this issue crosses many policy areas and acknowledges the work done cross-departmentally on the topic. In addition, the Committee commends this Report to the other Oireachtas Committees who have a particular interest in this area including Communications, Climate Action and Environment, Justice and Equality, and Education and Skills.

In the course of the preparation of this Report, the Committee met with a large number of relevant stakeholders to elicit their views over many months of extensive engagements dating back as far as February 2017. Many of the contributions given before the Committee were eye-opening, and they were important in highlighting the complexities of this topic, and the realities and challenges which children and young adults currently face online.

All of the opening statements and the transcripts of the public meetings of the Joint Committee at which various organisations and individuals gave evidence can be accessed on the Committee's website via the links provided in this Report. In addition many other individuals and organisations corresponded with the Committee on this issue or provided written submissions which the Committee considered as part of their engagement on the subject.

As Chair of the Joint Committee, I would like to express my gratitude to Committee Members for their input to this valuable Report. On behalf of the Joint Committee, I wish to express my gratitude to the organisations and individuals who came before the Joint Committee to give evidence or who provided written submissions or correspondence to aid the Committee in its consideration of this important topic.

The Joint Committee gained valuable insights from all those who had an input into the preparation of the Report and is grateful for their time. I would also like to thank the staff of the Committee Secretariat for the work involved in producing this Report.

There are 18 recommendations set out in the Report. The Oireachtas must act in a timely manner to address the issues raised in this Committee Report and to give effect to its recommendations. The Joint Committee is fully committed to monitoring the impact of the recommendations and intends to revisit the issue regularly for updates from the relevant Government Ministers, state bodies and other agencies on the progress of their responses to this Report.

_____

Alan Farrell T.D.

Chairman

29 March 2018

MEMBERSHIP – JOINT COMMITTEE ON CHILDREN AND YOUTH AFFAIRS

Deputies

			
Lisa Chambers T.D. (FF)	**Alan Farrell T.D. (FG) Chair**	**Kathleen Funchion T.D. (SF)**	**Denise Mitchell T.D. (SF)**
			
Tom Neville T.D. (FG)	**Anne Rabbitte T.D. (FF)**	**Seán Sherlock T.D. (Lab)**	

Senators

			
Lorraine Clifford-Lee (FF)	**Máire Devine (SF)**	**Joan Freeman (Ind)**	**Catherine Noone (FG)**

1 RECOMMENDATIONS

Recommendation 1
The Joint Committee recommends that the remaining recommendations as set out in the Report of the Internet Content Governance Advisory Group of 2014 should be implemented without delay.
Recommendation 2
The Joint Committee recommends that an Office of a Digital Safety Commissioner should be established and that it should have particular regard to ensuring that Children and Young People, who are some of the most vulnerable online users, are protected. This Office should be provided with sufficient resources and personnel to ensure that it can perform its functions adequately.
Recommendation 3
The Joint Committee recommends that an Advisory Task Force on the protection of Children and Young People online should be established.
Recommendation 4
The Joint Committee recommends that a National Strategy on Children's Cyber Safety, which outlines the Government's plans to address and resource the issues around Cyber Safety, should be introduced by Government. The Strategy should also take account of new developments that may accrue from this Report.
Recommendation 5
The Joint Committee recommends that the Government should launch a National Communications and Public Awareness campaign on Cyber Safety that is directed at Children and Young people, and, by extension, parents.
Recommendation 6
The Joint Committee recommends that both primary and post-primary schools should encourage and accommodate peer-to-peer workshops on Cyber Safety in schools.
Recommendation 7
The Joint Committee recommends that both primary and post-primary schools should appoint teachers as "Digital Safety Ambassadors" and that these teachers should be provided with supports and training so that students have an appropriate person to approach when issues arise in this area.

Recommendation 8
The Joint Committee recommends that both primary and post-primary schools and local libraries should be encouraged and supported to host parent's education and awareness evenings on Cyber Safety. The Joint Committee believes that presentations should be given by Children and Young People themselves in this regard.
Recommendation 9
The Joint Committee recommends that the Government advance the establishment of a Cyber Safety Programme in both primary and post-primary schools.
Recommendation 10
The Joint Committee recommends that Cyber Safety education should be formalised on both the primary school curriculum and the post-primary school curriculum.
Recommendation 11
The Joint Committee recommends that Cyber Safety education should form a mandatory part of both primary and post-primary teacher training courses.
Recommendation 12
The Joint Committee recommends that Children and Young people are made aware of the "right to be forgotten" as part of the proposed National Communications and Public Awareness campaign on Cyber Safety.
Recommendation 13
The Joint Committee recommends that the Joint Committee on Justice and Equality should have due regard to both child protection concerns and children's rights in the context of its Committee Stage consideration of the *Data Protection Bill 2018*, with particular emphasis on the "'Digital Age of Consent'".
Recommendation 14
The Joint Committee recommends that Social Media Platforms do more to strengthen their safety policies with a view to protecting their users. This could be done in consultation with the proposed Office of the Digital Safety Commissioner.
Recommendation 15
The Joint Committee recommends that Section 10 of the *Non-Fatal Offences Against the Person Act 1997* should be repealed and replaced with a new offence of harassment which expressly applies to harassment by all forms of communication including through digital and online communications, as per the Law Reform Commission's *Report on Harmful Communications and Digital Safety*.

Recommendation 16
The Joint Committee recommends that a specific stalking offence, separate from the related offence of harassment, should be introduced, as per the Law Reform Commission's *Report on Harmful Communications and Digital Safety.*
Recommendation 17
The Joint Committee recommends that Section 13 of the *Post Office (Amendment) Act 1951* should be repealed and replaced with a provision which would make the distribution of threatening, false, indecent or obscene messages, whether that message is to a person or about a person, an offence, as per the Law Reform Commission's *Report on Harmful Communications and Digital Safety.* This provision should also apply to all forms of communication, including any online communication.
Recommendation 18
The Joint Committee recommends the enactment of offences relating to the distribution of intimate images without the consent of the person depicted, as per the Law Reform Commission's *Report on Harmful Communications and Digital Safety.*

2 INTRODUCTION

The Irish Society for the Prevention of Cruelty to Children (ISPCC) made a submission to the Joint Committee on Children and Youth Affairs in February 2017. As part of this submission, the ISPCC indicated to the Committee that it had performed a case review of its work relating to cyber issues and how these issues affected the children, young people and families with which the ISPCC had worked with over the period from January 2015 - June 2016. This review helped to identify eight main themes relating to concerns with regard to children's safety online:

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; and
8. Lack of Knowledge and Skills.[1]

The Joint Committee also received submissions on this topic from the National Parents Council – Primary (NPCp) and the National Parents Council – Post Primary (NPCpp). In their respective submissions, both the NPCp and the NPCpp illustrated the findings of surveys conducted with their respective members in October 2017.

In summarising the findings of the answers to the question: "*What are the main concerns that you have when your children are online?*" as contained within its survey, conducted in October 2017 and to which 1,745 members responded, the NPCp stated that:

> *Accessing inappropriate content was the greatest concert shown by parents with 88% of parents selecting this option. Cyber-bullying is a major concern for parents with 73% highlighting this issue. Sexual exploitation was noted by 68% of respondents and 66% of parents are concerned with their children possibly giving out personal details. Many parents, 64%, are concerned with the amount of time their children spend online.*[2]

The NPCpp, in its survey which was undertaken in October 2017 and to which 297 parents responded, asked respondents to rank their main concerns from 1-6, with 6 being the greatest concern, with regard to their children's safety online. The main concerns in this

[1] ISPCC, *Briefing on Children and Cyber Safety*, 22 February 2017, pp. 3-4.
[2] National Parents Council Primary, *Submission to the Joint Committee on Children and Youth Affairs on Cyber Security for Children and Young Adults*, 23 October 2017, pp. 5-6.

regard were that children could become the victims of online grooming (26.6%), followed by children seeing sexually/violently explicit images online (15.82%) and that children might become isolated from others by spending too much time online (15.15%).[3]

CyberSafe Ireland's *Annual Report 2017* states that amongst children between the ages of 8-13:[4]

- 3% do not use the internet at all;
- 25% use the internet for 0-1 hours per day;
- 32% use the internet for 1-2 hours per day;
- 24% use the internet for 2-4 hours per day; and
- 16% use the internet for 4+ hours per day.[5]

Furthermore, a "Net Children Go Mobile" report conducted in 2014 found that 8% of Irish children between the ages of 9-16 use the internet daily while "out and about", while 46% of Irish children between the ages of 9-16 use the internet "when in their own bedroom".[6]

2.1 TRENDS

Based on the evidence presented above, the Joint Committee had concerns over the following conclusions that could be drawn from this evidence and its impacts:

- The issues that children have to deal with online are wide-ranging. However, both parents and children have indicated to the Committee that there a number issues that arise which they are most concerned about, namely:
    - That children will be the victims of cyber-bullying; that children will access inappropriate material online; and that children will become isolated by virtue of the fact that they are spending more time online.
- When compared to figures from 2016, an increasing percentage of children between the ages of 8-13 are using the internet for between 2-4 hours per day. This figure was 17% in 2016[7] while the figure is 24% for 2017.[8]
- As of 2014, almost half (46%) of Irish children between the ages of 9-16 were using the internet in their own bedrooms on a daily basis. These statistics indicate that a significant number of users between the ages of 9-16 use the internet in an unsupervised environment on a daily basis. This is broadly comparable with figures

[3] National Parents Council Post-Primary, Submission to the Joint Committee on Children and Youth Affairs on Cyber Security for Children and Young Adults, 20 October 2017, p.5.
[4] Representative sample of 4,893 children aged between 8 and 13 years of age.
[5] CyberSafeIreland, *Annual Report 2017*, p. 11.
[6] Net Children, Go Mobile: *Final Report*, 2014, p. 5.
[7] CyberSafeIreland, *Annual Report 2016*, p. 9.
[8] CyberSafeIreland, *Annual Report 2017*, p. 11.

from 2011 which suggested that 37% of children between the ages of 9-16 used the internet in a private space on a daily basis.[9]

- The issues and concerns that children, young people and families have with regard to children's safety online are wide-ranging. However, it is important to stress that the internet has many benefits for children also. Many stakeholders, including Professor Brian O'Neill and the Psychological Society of Ireland, emphasised this point. Similarly, the ISPCC noted in its briefing provided to the Joint Committee:

> *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.*[10]

Ultimately, the Joint Committee concluded, on the basis of the above and on the basis of all materials/submission received by it, that the area of Cyber Safety for Children and Youth Affairs warrants in-depth scrutiny of the issues which are preventing children and young people from experiencing the digital world as a safe environment.

This Report will illustrate the various viewpoints of the relevant stakeholders, after which the Joint Committee will make its recommendations.

[9] O'Neill, B., Grehan, S., & Ólafsson, K. *Risks and safety for children on the internet: the Ireland report*. LSE, London, 2011, p. 7.
[10] ISPCC, *Briefing on Children and Cyber Safety*, 22 February 2017, p. 3.

3 CURRENT POLICY CONTEXT

At present, the Office for Internet Safety (OIS), which is under the aegis of the Department of Justice and Equality, has lead responsibility for internet safety in Ireland. The OIS works closely with those in the industry, such as Internet Service Providers (ISPs) who are represented by the Internet Service Providers Association of Ireland (ISPAI), to ensure that those involved in this area are committed to the self-regulatory framework which is in place.

The ISPAI developed the Code of Practice and Ethics for Internet Service Providers, as envisioned by one of the main recommendations contained in the *First Report of the Working Group on Illegal and Harmful use of the Internet*,[11] and requires, inter alia, that ISPs:

- Ensure that they do not enclose content which is illegal, misleading, likely to incite violence or cruelty, racial hatred, prejudice or discrimination and, even if it is not illegal, is still considered inappropriate or calculated to cause distress, anxiety, inconvenience to others;
- Have Acceptable Usage Policies (AUPs) in place that ensure that customers are aware that they cannot use ISPs' service to create, host, transmit material which is unlawful/libellous/abusive/offensive/vulgar/obscene/ calculated to cause unreasonable offence. The AUPs must include "harmful material" clauses, as opposed to confining the Code to illegal material;
- Endeavour to have a working relationship with Hotline.ie (the national facility which allows for Internet Users to report suspected illegal content) by ensuring that: they provide a point of contact for interactions with Hotline.ie, comply with take-down notices as issued by Hotline.ie/An Garda Síochána and retain copies of removed material if requested to do so by Hotline.ie/An Garda Síochána;
- Facilitate an environment where end-users are empowered and ensure that Hotline.ie is utilised to provide information on methods to protect end-users.[12]

The Office for Internet Safety also provides resources on its website for the benefit of both children and parents, and these are as follows:

- A guide to cyber bullying;
- A parents' guide to social networking websites;
- A parents' guide to filtering technologies;
- A parents' guide to new media technologies. [13]

[11] First Report of the Working Group on Illegal and Harmful use of the Internet, 1999.
[12] http://www.ispai.ie/code-of-practice/key-features/
[13] http://www.internetsafety.ie/en/is/pages/oisbooklets

Furthermore, the Department of Education and Skills co-funds Webwise, the Irish Internet Safety Awareness Centre, along with funding from the European Union's Connecting Europe Facility. Webwise promotes the autonomous, effective, and safer use of the internet by young people through a sustained information and awareness strategy targeting parents, teachers, and children themselves with consistent and relevant messages.[14] For instance, Webwise is involved in the promotion of Safer Internet Day, an EU wide initiative to promote a safer internet for all users, especially young people.[15] This took place on 06 February 2018.

In late 2013, an independent, expert Internet Content Governance Advisory Group (ICGAG) was established to report to the then Minister for Communications, Energy and Natural Resources on a range of issues related to online content following a number of incidents. ICGAG's Report was brought before Cabinet and published in June 2014.[16]

ICGAG's Report contained 30 recommendations centred on institutional, legislative and governance reform, and in October 2017 the Joint Committee on Children and Youth Affairs wrote to the Department of Communications, Climate Action and Environment requesting an update on the progress made in implementing these recommendations. The Department, in its response, informed the Committee that:

> *A number of the Report's recommendations have been or are in the process of being implemented, most notably in the area of Education and in the awareness-raising activities of the Office of Internet Safety.*[17]

The Minister for Communications, Climate Action and Environment, Mr. Denis Naughten, T.D. informed the Joint Committee on Children and Youth Affairs at its meeting on 21 February 2018 that approximately 50% of the recommendations contained with the ICGAG Report are being progressed at present.[18]

The Law Reform Commission (LRC) also published its Report on Harmful Communications and Digital Safety in September 2016. The Report contains 32 recommendations of its own, and a draft *Harmful Communications and Digital Safety Bill*, designed to give effect to these changes, accompanies the Report.

The LRC's Report has attracted significant political attention in the meantime. The Joint Committee on Children and Youth Affairs met with the LRC to discuss its Report in October 2017. A Bill based partly on the recommendations of the LRC recently passed second stage

[14] https://www.webwise.ie/welcome-to-webwise/us/
[15] http://www.saferinternetday.ie/
[16] Department of Communications, Energy and Natural Resources, *Report of the Internet Content Governance Advisory Group*, May 2014.
[17] Received in correspondence by the Joint Committee on Children and Youth Affairs from the Minister for Communications, Climate Action and Environment on 13 November 2017.
[18] Joint Committee on Children and Youth Affairs, Debate: 21 February 2018.

in the Dáil and has been referred to the Committee on Justice and Equality for Committee stage consideration of the Bill.[19]

A Bill with the purpose of establishing an office of a Digital Safety Commissioner is also before the Dáil at present.[20]

As can be seen from the evidence above, the area of internet safety is regulated and governed by a variety of actors. In this regard, the Joint Committee believes that there should be a clearer regulatory framework and governance structure in place so as to ensure that children and young people are adequately protected in this space. The following sections of this report will consist of recommendations on how to establish an adequate framework based on the evidence received from stakeholders and other relevant literature.

Recommendation 1
The Joint Committee recommends that the remaining recommendations as set out in the Report of the Internet Content Governance Advisory Group of 2014 should be implemented without delay.

[19] Harassment, Harmful Communications and Related Offences Bill 2017 [PMB], Sponsored by Mr. Brendan Howlin, T.D.
[20] Digital Safety Commissioner Bill 2017 [PMB], Sponsored by Mr. Donnchadh Ó Laoghaire, T.D.

4 EVIDENCE FROM COMMITTEE MEETINGS

4.1 INTRODUCTION

In this section of the report, there will be an analysis of the pertinent themes that arose during the Joint Committee's engagements on this topic; while there will also be a consideration of the other materials that the Joint Committee has become aware as a result of its consideration of this topic.

Following this, the Joint Committee will provide its recommendations in this regard.

4.2 STAKEHOLDER ENGAGEMENT

The Joint Committee held eight days of hearings during the period from February 2017 – February 2018 to engage with relevant stakeholders to discuss "Cyber Security for Children and Young Adults." Table 1 below identifies all stakeholders who made presentations to the Joint Committee, the date of their presentations and the session during which they made their presentation. Table 2 below provides details relating to submissions that were received by the Joint Committee on this topic.

4.2.1 TABLE 1 - STAKEHOLDERS

	Session 1	Session 2
22 February 2017	• Ms. Grainia Long, Chief Executive, **Irish society for the Prevention of Cruelty (ISPCC)**. • Ms. Caroline O'Sullivan, Director of Services, **ISPCC.** • Ms. Cliodhna O'Neill, Director of Policy and Communications, **ISPCC.**	

27 September 2017	• Mr. Simon Grehan Project Officer, Professional Development Service for Teachers (PDST), **Webwise.** • Ms. Jane McGarrigle Project Officer, Professional Development Service for Teachers (PDST), **Webwise.** • Mr. Tony Weir, Senior Inspector, Department of Education and Skills, **Webwise.** • Ms. Ana Niculescu, Manager, **Hotline.ie.**	
18 October 2017	• Dr. Geoffrey Shannon, **Special Rapporteur on Child Protection**. • Professor Brian O'Neill, Director of Research, Enterprise & Innovation Services, Dublin Institute of Technology (DIT) and **Past Chairperson of the Internet Content Governance Advisory Group**.	• Mr. Justice John Quirke, President, **Law Reform Commission**. • Mr. Ray Byrne, Commissioner, **Law Reform Commission**. • Professor Donncha O'Connell, Commissioner, **Law Reform Commission**. • Mr. Ciaran Burke, Director of Research, **Law Reform Commission**.
25 October 2017	• Mr. John O'Driscoll, Assistant Commissioner, Special Crime Operations, **An Garda Síochána**. • Mr. Declan Daly, Detective Superintendent, Garda National Protective Services Bureau (GNPSB), **An Garda Síochána**. • Mr. Michael Gubbins, Detective Superintendent, Garda National Cyber Crime Bureau (GNCCB), **An Garda Síochána.**	• Ms. Siobhan McCabe, Assistant Principal Officer, **Office for Internet Safety**. • Ms. Eileen Leahy, Principal Officer, **Office for Internet Safety**. • Ms. Alex Cooney, Chief Executive Officer, **CyberSafe Ireland**. • Ms. Cliona Curley, Programme Director, **CyberSafe Ireland**. • Ms. Maggie Brennan, Scientific Adviser, **CyberSafe Ireland**.

06 December 2017	• Ms. Niamh Sweeney, Head of Public Policy, **Facebook Ireland**. • Ms. Siobhán Cummiskey, Head of Content Policy, **Facebook Ireland.** Ms. Julie de Bailliencourt, Head of Safety for Europe the Middle East and Africa, **Facebook**.	
07 February 2018	• Ms. Lauren Reynolds, **Newbridge College.** • Ms. Muireann Whelan, **Newbridge College.** • Ms. Serena Devereux, **Newbridge College.** • Ms. Isabel Seacy, **Newbridge College.** • Ms. Tara Trevaskis Hoskin, **Wicklow Comhairle na nÓg.** • Ms. Jade O'Hagan, **Wicklow Comhairle na nÓg.** • Ms. Jody Whelan, **Clare Comhairle na nÓg.** • Mr. Fearghal Burke, **Clare Comhairle na nÓg.**	
13 February 2018	• Dr. Mary Aiken, Adjunct Associate Professor at UCD Geary Institute for Public Policy, and **Academic Advisor to the European Cyber Crime Centre at Europol.** • Professor Barry O'Sullivan, Director, **Insight Centre for Data Analytics, Department of Computer Science, UCC**.	

21 February 2018	• Professor Brian O'Neill, Chair, **Internet Content Governance Advisory Group.** • Mr. Ronan Lupton, Barrister-at-Law, **Internet Content Governance Advisory Group.** • Ms. Áine Lynch, CEO of the National Parents Council Primary, **Internet Content Governance Advisory Group.** • Professor Joe Carthy, College Principal and Dean of Science at University College Dublin, **Internet Content Governance Advisory Group.**	• Dr. Katherine Zappone T.D., **Minister for Children and Youth Affairs**. • Mr. Denis Naughten T.D., **Minister for Communications, Climate Action and Environment**. • Mr. Charlie Flanagan T.D., **Minister for Justice and Equality**. • Mr. Richard Bruton T.D., **Minister for Education and Skills**.

4.2.2 TABLE 2 - SUBMISSIONS

Organisation	Title	Date Received
National Parents Council – Post-Primary	Written Submission to the Joint Committee on Children and Youth Affairs on the topic of Cyber Security for Children and Young Adults	20 October 2017
National Parents Council - Primary	Submission to the Joint Committee on Children and Youth Affairs on Cyber Security for Children and Young Adults	23 October 2017
The Irish Society for the Prevention of Cruelty to Children	Update to the Joint Oireachtas Committee on Children and Youth Affairs on the ISPCC's Stance on Children's Cyber Safety	01 December 2017
The Irish Society for the Prevention of Cruelty to Children	Consultation Event Report	01 December 2017
Snapchat	Written evidence submitted by Snap Inc.	29 January 2018
Instagram	Instagram's Approach to Online Safety	08 February 2018
Psychological Society of Ireland	Submission to the Oireachtas Joint Committee on Children and Youth Affairs	20 February 2018

4.3 ESTABLISHMENT OF THE OFFICE OF THE DIGITAL SAFETY COMMISSIONER

In 2016, the Law Reform Commission (LRC), as part of its 4th Programme of Law Reform, published its *Report on Harmful Communications and Digital Safety*. In its Report, the LRC recommends, inter alia, that an Office of a Digital Safety Commissioner should be established in Ireland and should be based on the model that is in place in Australia, and to a lesser extent, the model that is place in New Zealand.[21]

The LRC recommends that the general functions of this Office should be:

a) to promote digital safety for all persons;
b) to support and encourage the implementation of measures to improve digital safety;
c) to ensure the oversight and regulation of a timely and efficient procedure for the take down, that is, removal, by digital service undertakings, of harmful digital communications (the "take down procedure");
d) to ensure that the take down procedure is made available to all affected individual persons by digital service undertakings free of charge;
e) to consult widely in the development of the code of practice;
f) to support the preparation and publication by the Ombudsman for Children of guidance material, including guidance material for schools, relevant to digital safety of children and to harmful digital communications;
g) to coordinate the activities of Government Departments and other public bodies and authorities relating to digital safety;
h) to collect, analyse, interpret and disseminate information relating to digital safety;
i) to support, encourage, conduct and evaluate research about digital safety; and
j) to publish (whether on the internet or otherwise) reports and papers relating to digital safety.[22]

The Joint Committee notes that the possible establishment of an Office of a Digital Safety Commissioner was a common theme that arose consistently during its engagements with various stakeholders and unanimously calls for its establishment.

[21] The Law Reform Commission, *Report on Harmful Communications and Digital Safety*, 2016, pp. 141-145
[22] The Law Reform Commission, *Report on Harmful Communications and Digital Safety*, 2016, *p*p. 157-158

4.3.1 IRISH SOCIETY FOR THE PREVENTION OF CRUELTY TO CHILDREN

During its first engagement on this topic on 22 February 2017, the Joint Committee invited the Irish Society for the Prevention of Cruelty to Children (ISPCC) to discuss Cyber Security for Children and Young Adults.

The ISPCC informed the Joint Committee that it had chosen Cyber Safety for children as one of its current priorities. The ISPCC informed the Joint Committee that the work done in this area by the LRC would be particularly useful for the Joint Committee's investigation of this topic and that the real change in this area, which it believes is necessary to ensure that children and young people are protected, could be achieved through the establishment of an Office of a Digital Safety Commissioner as proposed by the LRC.

In echoing the sentiments of the LRC with regard to an Office of a Digital Safety Commissioner, the ISPCC informed the Joint Committee that it believes that the Office should have three core functions. According to the ISPCC:

> *First, it should co-ordinate all the education work that is in place. There has been a proliferation of organisations doing work in this area, including ours. That is great but a co-ordinating organisation is needed. We also need to make sure there are standards for educating parents and young people in this area…*
>
> *…Second, the office should set standards for industry. We need to be clear that industry needs to play a role. Companies need to step up to the plate to make technology available to children and young people. The office should put a set of guiding principles in place that industry would have to follow. It could then take action. Individuals could contact the commissioner if they wanted information deleted online. The right to have information removed would be placed with the office. If the industry body, ISP, telecommunications provider and so on did not follow the request, action could be taken. It would be a useful office.*
>
> *Third, the office should have an important role in investigating individual cases. That would formalise much of the law in this area and regulate a regulatory policy.*[23]

[23] Joint Committee on Children and Youth Affairs, Debate: 22 February 2017.

4.3.2 DR. GEOFFREY SHANNON, SPECIAL RAPPORTEUR ON CHILD PROTECTION

During the engagement of the Joint Committee on Children and Youth Affairs on 18 October 2017, Dr. Geoffrey Shannon, Special Rapporteur on Child Protection, fully endorsed the recommendations as set out in the LRC's Report.

Dr. Shannon was particularly concerned with regard to having effective mechanisms in place whereby an aggrieved party would be in a position to have "harmful" content removed from the internet if they so wished. Dr. Shannon stated:

> *The proposed Office of the Digital Safety Commissioner of Ireland should oversee an effective and efficient take down procedure in a timely manner, regulating for a system of take down orders in respect of harmful cybercommunications made in respect of both adults and children. I would also add that in the terms of the role of the Digital Safety Commissioner and take down procedures there should be a requirement on the Digital Safety Commissioner to take down material within a specified period of time. It is an issue that is not expressly referenced in the report of the Law Reform Commission, but it is one that I believe should be adopted.*
>
> …
>
> *My vision for the future is that the digital safety commissioner will take the lead. We need somebody to take the lead on this issue. There is a real opportunity associated with establishing an office designated to deal with this issue. It would be a society-wide approach rather than a sectoral approach. My vision is that the digital safety commissioner will liaise with the Data Protection Commissioner and all the other bodies.*[24]

Dr. Shannon, in the *10th Report of the Special Rapporteur on Child Protection*, further endorses the recommendation of the LRC with regard to establishing an Office of a Digital Safety Commissioner. In this Report, Dr. Shannon states:

> *The Law Reform Commission has proposed the establishment of a new statutory oversight system with a dual role of promoting digital safety and ensuring an efficient take down procedure for harmful digital communications. The proposed Office of the Digital Safety Commissioner of Ireland would therefore oversee an "effective and efficient" take down procedure in a timely manner, regulating for a system of take down orders in respect of harmful cyber communications made in respect of both adults and children. It is recommended therefore that consideration be given by the government to Chapter 3 of the Commission's*

[24] Joint Committee on Children and Youth Affairs, Debate: 18 October 2017.

Report forthwith, to enable progress to be made in this regard and to ensure that steps are taken to establish an Office of the Digital Safety Commissioner. It is further recommended herein that the Office of the Digital Safety Commissioner be subject to strict timelines within which to act on complaints received and take such further steps as might be necessitated.[25]

4.3.3 PROFESSOR BRIAN O'NEILL, DIRECTOR OF RESEARCH, ENTERPRISE AND INNOVATION SERVICES, DUBLIN INSTITUTE OF TECHNOLOGY AND MEMBERS OF THE INTERNET CONTENT GOVERNANCE ADVISORY GROUP

During the engagement of the Joint Committee on Children and Youth Affairs on 18 October 2017, the Joint Committee engaged with Professor Brian O'Neill, Director of Research, Enterprise and Innovation Services, Dublin Institute of Technology on the topic. Professor O'Neill was also the Chairperson of the Internet Content Governance Advisory Group (ICGAG). Members of this Group appeared before the Committee on the topic of Cyber Security for Children and Young Adults on 21 February 2018.

Professor O'Neill, along with Members of the ICGAG: Mr Ronan Lupton, Barrister-at-Law, Áine Lynch, CEO of the National Parents Council (primary), Professor Joe Carthy, College Principal and Dean of Science at University College Dublin, provided details of their work with ICGAG to the Joint Committee and explained how the Group's final report drew on available evidence to assess the adequacy of Ireland's governance arrangements on online content and Internet safety and that the Group's recommendations emanated from this work.

Professor O'Neill also informed the Committee that the work of ICGAG coincided with the work of the Law Reform Commission in this area and that ICGAG consequently made limited comment on the legislative framework in deference to the work of the Law Reform Commission. ICGAG did, however, recommend that the role of the Office for Internet Safety "should be reconfigured to deal exclusively with issues of law enforcement and illegal online content."[26]

In this regard, Professor O'Neill acknowledged that ICGAG's recommendation with regard to the Office for Internet Safety complemented the LRC's recommendation in relation to the establishment of an Office of a Digital Safety Commissioner. Professor O'Neill stated:

The recommendations have been submitted to Government for consideration and I believe they were positively received but we await further implementation.

---

[25] Dr. Geoffrey Shannon, *Tenth Report of the Special Rapporteur on Child Protection*, 2017, p. 29.
[26] Department of Communications, Energy and Natural Resources, *Report of the Internet Content Governance Advisory Group*, May 2014, p. 8

I believe it is a resource which complements the work of the Law Reform Commission and its recommendation for the establishment of a digital safety commissioner. The two in fact are quite complementary and stand as an important statement awaiting further Government response.[27]

4.3.4 THE LAW REFORM COMMISSION

During the engagement of the Joint Committee on Children and Youth Affairs on 18 October 2017 the Committee heard from representatives of the LRC. The LRC informed the Joint Committee about the work that it undertook so as to inform its *Report on Harmful Communications and Digital Safety* and also provided more details on the LRC's recommendations contained therein. The LRC stated the following in relation to the proposed Office of the Digital Safety Commissioner:

We have considered and proposed a system of statutory oversight in the form of a digital safety commissioner, with a range of remedies open to that office and a strong focus on the need for a statutory code of practice.

…

On the topic of education and oversight, we propose the establishment of an office of digital safety commissioner, like those already in existence in Australia and New Zealand. If legislated for, this office will promote digital safety and will also have an important educational role in promoting positive digital citizenship among children and young people. We state very explicitly in the report that the digital safety commissioner should work with the Office of the Ombudsman for Children and liaise with all education partners to develop guidance material for young people in schools, including guidance on encouraging mediation and restorative processes, especially for issues for which the criminal law is not suitable.

On the issue of a code of practice on take-down procedure, what we have proposed in the draft Bill and in our report is that the digital safety commissioner should publish a statutory code of practice on digital safety, setting out nationally agreed standards on the details of an efficient take-down procedure.

…

The type of procedure that we envisage for a take-down is that individuals who feel aggrieved by a harmful communication would initially apply directly to social media sites themselves. This would encourage social media hosts to have robust

[27] Joint Committee on Children and Youth Affairs, Debate: 18 October 2017.

mechanisms for taking down harmful communications to avoid engagement with the more formal process. If the site did not comply with such a request, and in so doing did not comply with the code of practice, the individual could appeal to the digital safety commissioner who could then direct that site to comply. The digital safety commissioner would be empowered statutorily to enforce the code. If the site did not comply with such a direction from the digital safety commissioner, the latter could then apply to the Circuit Court for a court order.[28]

The Joint Committee fully endorses the proposal that the Digital Safety Commissioner would publish a statutory code of practice of digital safety. This is important as it would put what is now a self regulated system on a statutory footing. This is also significant as it would be enforceable.

4.3.5 CYBERSAFE IRELAND

During its engagement on this topic on 25 October 2017, the Joint Committee heard from representatives of CyberSafe Ireland. CyberSafe Ireland is a not-for-profit organisation that works to empower children, parents and teachers to navigate the online world in a safe and responsible manner.

CyberSafe Ireland informed the Joint Committee that is in favour of establishing an Office of a Digital Safety Commissioner. However, CyberSafe Ireland also believe that that Office should not operate in isolation and should receive its direction from an advisory body. CyberSafe Ireland stated:

The Government must lead the way in tackling this issue by showing clear leadership, by creating a national strategy and a task force on online safety for children, and by appointing a digital safety commissioner and resourcing his or her office appropriately.

…

Regarding who would sit on the task force, many of the stakeholders have already been named, such as the telecommunications industry, representatives of academia and representatives from the charitable sector, which is particularly the case in Ireland because so many of our preventative responses rely on that third sector at present. Obviously, there would be representation from the appropriate Departments. I believe a cross-departmental body would be preferable. The role in respect of the commissioner would have to be advisory.

[28] Joint Committee on Children and Youth Affairs, Debate: 18 October 2017.

There would have to be some independent advisory body that is advising the commissioner rather than sitting within the office of the commissioner. There must be independence because the issues … are complex, social, nuanced and dynamic. They change and therefore the relative roles of the stakeholders in this task force will change over time.[29]

4.3.6 PROFESSOR BARRY O'SULLIVAN AND DR. MARY AIKEN

During the engagement of the Joint Committee on Children and Youth Affairs on 13 February 2018, Professor Barry O'Sullivan and Dr. Mary Aiken informed the Joint Committee that they are in favour of the establishment of an Office for Digital Safety Commissioner. Professor O'Sullivan stated:

The Government must formalise the role, office, and statutory powers of the digital safety commissioner, which we strongly welcome. One specific task that could be assigned to this office is the development of a robust system for age verification online. Self-verification does not work. A child simply saying he or she is 13 or 16 is not adequate. One does not enter bars on the basis that one says one is 22 if one is not. Ireland could lead in the area of online age verification. We believe that robust age verification online is one of the most critical requirements to deliver on child and youth security in cyber contexts.[30]

The Joint Committee agrees that self-verification of age online is not a robust system and endorse this suggestion that the Digital Safety Commissioner should be tasked with investigating how a more accurate system could be developed. The Joint Committee also had concerns about this issue from its interaction with the social media platforms Facebook, Instagram and Snapchat and how they verify that their users are of the age where they are able to set up an account. Therefore, the Joint Committee considers that a robust system of age verification is necessary to ensure that children and young people of an appropriate age are using these platforms.

[29] Joint Committee on Children and Youth Affairs, Debate: 25 October 2017.
[30] Joint Committee on Children and Youth Affairs, Debate: 13 February 2018.

4.3.7 RECOMMENDATIONS

On the basis of the evidence presented above, the Joint Committee has a number of observations to make, following which it will make its recommendation(s).

The Joint Committee recommends that an Office of a Digital Safety Commissioner should be established and that it should have particular regard to ensuring that Children and Young People, who are some of the most vulnerable people in this space, are protected. This Office should be provided with sufficient resources and personnel to ensure that it can perform its functions adequately.

With particular regard to resourcing and personnel, the Joint Committee notes that the Office for Internet Safety, which has lead responsibility for internet safety in Ireland, is vastly under-resourced, and the Joint Committee does not wish to see similar resourcing issues affecting the scope, work and effectiveness of the proposed Office of the Digital Safety Commissioner.

At a minimum, the Office of the Digital Safety Commissioner (ODSC) should:

- Coordinate the activities of Government Departments and other public bodies and authorities relating to digital safety;
- Collect, analyse, interpret and disseminate information relating to digital safety;
- Rationalise, where possible, any existing section within relevant Government Departments in order to ensure no duplication arises following its creation.
- Support, encourage, conduct and evaluate research about digital safety. In particular, the Joint Committee believes that research should be carried out in relation to the long term effects of internet use on:
    - Children and Young People's development;
    - Children and Young People's mental health; and
    - Children and Young People's abilities to develop relationships.
- In respect of its research function, carry out research in the area of age verification with a view to developing a robust age verification system.
- Publish a statutory code of practice on digital safety that would replace the current self-regulatory code that is in place.
- Oversee an effective and efficient take down procedure which would form part of the new code of practice on digital safety, within a specified time period, in respect of harmful cybercommunications made in respect of both adults and children. The Joint Committee envisages that an aggrieved party, in the first instance, would

apply to the web site in question to have the harmful material removed. In the event that the web site did not comply with such a request, and in so doing did not comply with the new code of practice, the individual could appeal to the Digital Safety Commissioner who could then direct that site to comply. The Digital Safety Commissioner would be empowered statutorily to enforce the code. If the web site in question did not comply with such a direction from the Digital Safety Commissioner, then he/she could apply to the Circuit Court for a court order.

Recommendation 2
The Joint Committee recommends that an Office of a Digital Safety Commissioner should be established and that it should have particular regard to ensuring that Children and Young People, who are some of the most vulnerable online users, are protected. This Office should be provided with sufficient resources and personnel to ensure that it can perform its functions adequately.

The Joint Committee recommends that an advisory task force on the protection of Children and Young People on the Internet should be established. This task force should sit across the four relevant Departments in this space, i.e. the Department of Communications, Climate Action and Environment, the Department of Justice and Equality, the Department of Education and Skills and the Department of Children and Youth Affairs.

Its membership should also consist of members from the telecommunications industry, the academic sector, the charitable sector and social media, while children and young people themselves should also be consulted. It should be the responsibility of this task force to provide independent advice and guidance to the Office of the Digital Safety Commissioner, particularly in relation to matters as they pertain to children and young people.

Recommendation 3
The Joint Committee recommends that an Advisory Task Force on the protection of Children and Young People online should be established.

4.4 EDUCATION AND AWARENESS

In 2014, the ICGAG, in its *Report of the Internet Content Governance Advisory Group*, was cognisant of the important role that education can play in this sphere. The Report states the following:

> *The reliance on soft law and self-regulatory approaches as the primary means of dealing with bullying and harassment online has created an ever more important need to develop levels of digital literacy and awareness among users. If, as is claimed, the range of existing measures is sufficient: that legislative provision for both criminal and civil prosecution in relation to the most serious kinds of abuses is adequate; that industry processing and response to reports of abuse is effective; and that there is sufficient legal protection for industry providers in handling content, then a priority for policy has to be a major emphasis on awareness-raising and user education.*[31]

The Joint Committee notes that the need for increased levels of education and awareness was a common theme that arose consistently during its engagements with various stakeholders. The Joint Committee concurs with the views of many stakeholders that education and awareness are the most important areas to be tackled. Empowering parents, teachers and children through education as to appropriate online behaviour is more valuable and effective in the long term than any absolute bans or extreme limitations on young people's access to the Internet.

4.4.1 IRISH SOCIETY FOR THE PREVENTION OF CRUELTY TO CHILDREN

The ISPCC made a submission to the Joint Committee on Children and Youth Affairs in advance of its meeting on 22 February 2017. As part of this submission, the ISPCC advocated for the development of a National Strategy on Children's Cyber Safety. The ISPCC proposed various potential components of this strategy, and one particular component related to education for children and young people in this space. The ISPCC stated:

> *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*

[31] The Internet Content Governance Advisory Group, *Report of the Internet Content Governance Advisory Group*, 2014, p. 44.

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.[32]

At the meeting of the Joint Committee on 22 February 2017, the ISPCC reiterated its call for increased levels of education in this regard. Ms. Grania Long, Chief Executive Office stated:

I cannot stress enough the importance of formal and informal education in solving this problem. All of the members have mentioned in their comments that education is required for children, young people and parents. I will start with children and young people. To be blunt, our education curriculum does not prepare people for the outside world. We are frankly naive as a society if we think that what we teach children about sex and sexual behaviour is enough to equip them. The sooner we recognise that and it is reflected in our curriculum the better for children and child safety. The national strategy needs to be owned by Government and rolled out by four key Departments. The Department of Education and Skills would play a key role.

…

I would prefer the matter formalised within the education system. Every time we move it out to other organisations it becomes disparate, whether the schools can afford same and whether the school considers it to be a priority. It is left to either the principal or the board of governors to make it a priority. We need to make cybersafety a national priority and consistently available to children. My feeling is the more formal this is the better.[33]

4.4.2 WEBWISE

Webwise is the Irish Internet Safety Awareness Centre and is co-funded by the European Union and the Department of Education and Skills. Webwise is part of the Professional Development Service for Teachers (PDST) Technology in Education, which promotes and supports the integration of Information and Communications Technology (ICT) in teaching and learning in first and second level schools.

Webwise appeared before the Committee on 27 September 2017, with Hotline.ie, in order to inform the Joint Committee of its work. Webwise strives to promote autonomous, effective, and safer use of the internet by young people through a sustained information

[32] ISPCC, *Briefing on Children and Cyber Safety*, 22 February 2017, p. 19.
[33] Joint Committee on Children and Youth Affairs, Debate: 22 February 2017.

and awareness strategy targeting parents, teachers and children themselves with consistent and relevant messages. Webwise develops and disseminates resources that help teachers integrate internet safety into teaching and learning in their schools. Webwise also provides information, advice, and tools to parents to support their engagement in their children's online lives. Webwise Youth Advisory Panel develops youth oriented awareness raising resources and campaigns that address topics such as cyber bullying.

The Webwise 2017 Parenting Survey,[34] which was a collaborative effort between Webwise, the Irish Internet Safety Awareness Centre, and the National Parents Council Primary (NPC), asked parents questions regarding attitudes to online risks, safety and digital parenting issues for children aged between 0-18.

Arising from this survey Webwise believe that parents need more information and advice targeted to the age and needs of their children in order to help them in supporting their children's online use.

The Joint Committee has heard from a number of stakeholders that parents do not feel adequately equipped to deal with the issues arising from cyber safety with their children. While there are a number of valuable organisations producing resources in this space, the Joint Committee has heard that many parents are not even aware they exist. As such the Committee believes that the proposed Digital Safety Commissioner could coordinate and collaborate with groups, including Webwise and the Office of Internet Safety, to ensure that all parents have access to these publications, possibly through distribution through the schools' network.

4.4.3 DR. GEOFFREY SHANNON, SPECIAL RAPPORTEUR ON CHILD PROTECTION

During the engagement of the Joint Committee on Children and Youth Affairs on 18 October 2017 Dr. Geoffrey Shannon, Special Rapporteur on Child Protection urged the Joint Committee to look beyond solely considering potential changes to the legal framework and to place an emphasis on education also. Dr. Shannon said:

> *I emphasise that many parents, carers and teachers are ill-equipped to advise and protect their children from risks online. Education and awareness raising around the risks and opportunities and rights of children engaging online should begin very early in primary school and well before the age of digital consent in order that children are prepared and parents and teachers are in a position to*

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

advise and support them. This should be part of the primary school curriculum.[35]

4.4.4 PROFESSOR BRIAN O'NEILL, DIRECTOR OF RESEARCH, ENTERPRISE AND INNOVATION SERVICES, DUBLIN INSTITUTE OF TECHNOLOGY

During the engagement of the Joint Committee on Children and Youth Affairs on 18 October 2017 Professor Brian O'Neill referred to a number of documents and initiatives that have a bearing on education and awareness-raising in this sphere.

In particular, Professor O'Neill made reference to the European Strategy to make the internet a better place for children. This Strategy requires the following of Members States:

Member States should

- *step up the implementation of strategies to include teaching online safety in school curricula by 2013.*
- *reinforce informal education about online safety and provide for 'online safety' policies in schools and adequate teacher training.*
- *support public-private partnerships to reach the above goals.*[36]

Professor O'Neill, in describing this Strategy and the work he is doing in respect of the Strategy, stated the following:

The Commission enjoined Member States to step up their efforts in developing and supporting digital skills education in schools and requested industry to enhance measures around new areas of content such as user generated content and guidance to parents to support them in their role. That work is ongoing.

I am currently leading a study which is a bench marking or comparative assessment of how individual member states have implemented this against the communication which was in 2012. It informs European thinking in supporting better Internet experiences for young people while strengthening or enhancing protection measures to ensure there is sufficient good quality content, and better support available to young people to emphasise their positive dimensions.[37]

The Joint Committee notes Professor O'Neill's involvement in the comparative assessment of what Members States have implemented when compared to what was set out in the Strategy and looks forward to seeing how Ireland fares in this regard.

[35] Joint Committee on Children and Youth Affairs, Debate: 18 October 2017.
[36] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: European Strategy for a Better Internet for Children, COM(2012) 196 final, 02 May 2012.
[37] Joint Committee on Children and Youth Affairs, Debate: 18 October 2017.

Professor O'Neill proceeded to describe the situation with regard to Internet Safety as part of the relevant school curricula in Ireland. Professor O'Neil stated:

> *There already is some good representation of Internet safety issues in the school curriculum. Part of the difficulty, however, is the ability or otherwise of schools to address the issue comprehensively and consistently. The social, personal and health education programme offers many opportunities and curriculum points for discussing children's use of technology. We must acknowledge that digital interaction is part and parcel of how children communicate, learn and access entertainment. It is important that teachers have sufficient resources and training available to them to make the best use of technology in the context of a world that is rapidly evolving. Children's usage of new technologies will proceed apace. Having opportunities within the curriculum to emphasise consistently across all subject areas the importance of effective and responsible use of online or connected technologies is crucial.*[38]

The Joint Committee supports the suggestion to have online safety made a mandatory part of the curriculum in primary and post-primary schools. The Joint Committee also supports the suggestion that it form part of the curriculum for teacher training for both primary and post primary schools to ensure teachers are fully equipped to deal with the complex subject matter.

4.4.5 CYBERSAFE IRELAND

During the engagement of the Joint Committee on Children and Youth Affairs on 25 October 2017 CyberSafe Ireland informed the Joint Committee that appropriate levels of education in this sphere is key in terms of preventing unwanted behaviour from occurring online. CyberSafe Ireland stated:

> *We need prevention. We strongly believe that the most effective response is prevention through education. We must equip our young Internet users with the skills and knowledge that they need to navigate the online world safely, responsibly and in ways that are respectful of others. This provision cannot be offered unsystematically, as it is now, to those children who are lucky enough to live in a location where an online safety expert is available. This provision must be made available to all children in every corner of the country, wherever a child may be online. Digital literacy that encompasses online safety education will need to become the fourth pillar of our education system, alongside reading, writing and arithmetic.*

[38] Joint Committee on Children and Youth Affairs, Debate: 18 October 2017.

…

> *We must invest in education. We must ensure that every child benefits from a good education on online safety, digital rights, citizenship and well-being and that, when things go wrong, the child at the centre will be effectively protected. We need to be doing so much more to respond comprehensively to this issue. Problems of online safety are becoming increasingly urgent for children and parents around the country. They have the potential to impact on the future of every online child in Ireland.*[39]

CyberSafe Ireland also referred to the *Internet Safety Strategy – Green paper* which was recently published by the Secretary of State for Digital, Culture, Media and Sport in the United Kingdom (UK). It is worth noting, however, that the measures contained therein apply to England alone, as education is a devolved area within the UK.

This Green Paper has an entire strand dedicated to the support of children, and also details how parents and carers can be supported to give children the knowledge and confidence they need in this regard.

The Green Paper acknowledges that while all primary school children must be taught Relationships Education and all secondary school children must be taught Relationships and Sex Education (RSE) in England following the introduction of the *Children and Social Work Act 2017*,[40] it also acknowledges that other compulsory subjects need to be considered.

The Green Paper states the following in relation to these other compulsory subjects:

> *The Department for Education will support schools to ensure that content is pitched at the right level for each school year and builds knowledge as children grow up. Engagement and consultation will help us to get the detail right, but we expect it will start with the basics, including building friendships online in the early years of primary school, through to cyberbullying and contact advice; and then online pornography and sexting education at age appropriate points as children get older.*[41]

The Joint Committee would welcome proposals of this nature in an Irish context, but more detail would need to be provided as to what these proposals would entail in the context of the relevant curricula in Ireland.

[39] Joint Committee on Children and Youth Affairs, Debate: 25 October 2017.
[40] https://www.legislation.gov.uk/ukpga/2017/16/part/1/chapter/4
[41] HM Government, Department for Digital, Culture, Media and Sport, *Internet Safety Strategy – Green paper* , 2017, p. 26.

4.4.6 NEWBRIDGE COLLEGE

During the engagement of the Joint Committee on Children and Youth Affairs on 07 February 2018 representatives of Newbridge College stressed to the Committee that raising levels of education and awareness in this sphere is of utmost importance.

Students of Newbridge College stated the following in particular reference to the practice of "sexting":

> *Not only is sexting dangerous, it can also have serious possible legal consequences. Very few teenagers are aware of the legalities surrounding nude images, which can also be classified as child exploitation material. The Child Trafficking and Pornography Act 1998 makes no allowance or distinction regarding underage sexting. Child pornography incorporates a person under 17 years of age engaging in an explicit sexual activity or visual representation. Even the case of a suggestive provocative image that may suggest an explicit sexual representation of a part of the body may still come within the definition of child pornography ... I believe this issue is getting out of control and becoming a popular trend due to the lack of education and information provided to young people. We can help prevent and tackle this by raising awareness and being taught the dangers of sexting in school as part of the social, personal and health education, SPHE, curriculum or the relationships and sexuality education, RSE, module.*[42]

In a more general sense, students from Newbridge College also had the following to say in relation to education and awareness-raising:

> *Many of these problems can be easily prevented. The Internet is not a truly bad and dangerous place and, when used in a safe and responsible way, like many things, can be positive and beneficial. How do we tackle these issues? While there will always be negative and dangerous sources online, the right guidelines on children and young people, implemented with the assistance of teachers and parents, can help us young people remain safer on the web. Raising awareness is key. We need to get these issues talked about. There is much schools and parents can do to help. Safer Internet Day was yesterday, 6 February [2018], with 100,000 teachers and students throughout the country taking part in activities relating to how to be safe when online.*
>
> *Teachers addressing these issues through a range of subjects can help educate young people who are otherwise the most vulnerable to the dangers they may encounter online. Information evenings in schools or communities should be in*

[42] Joint Committee on Children and Youth Affairs, Debate: 07 February 2018.

place to inform parents and get them talking about the importance of safety online too.[43]

4.4.7 CLARE COMHAIRLE NA NÓG

During the engagement of the Joint Committee on Children and Youth Affairs on 07 February 2018, representatives of Clare Comhairle na nÓg informed the Committee about the work that it has done in this sphere.

Clare Comhairle na nÓg informed the Joint Committee that it became apparent following the Comhairle AGM in 2014 that Cyber-Safety was a priority topic for its members and associates. As a result, Cyber-Safety became part of the Clare Comhairle's work plans in 2015, 2016 and 2017. In 2015 and 2016, the Comhairle made a short film which included aspects of inappropriate sharing online and it also ran a consultation which examined attitudes to oversharing online.

In 2016 and 2017, Clare Comhairle na nÓg was involved in an Erasmus exchange with its equivalent in Iceland, the Samfés committee. Each group delivered workshops to the other on areas of common interest, such as positive mental health and cyber-safety. The Clare Comhairle informed the Committee that the young people from Samfés had developed and run a sexting peer education workshop in 2016 and that they had translated it into English so that the Clare Comhairle could make use of it. The Clare Comhairle has now formatted this sexting workshop so that it can be used in an Irish context.

The Clare Comhairle also described separate work that it has done in this area. In response to young people looking for some direction and education in this rapidly changing environment, the Clare Comhairle approached a global computer security software company which had developed a cyber-safety programme as part of its corporate social responsibility project. The programme was piloted with 49 young people at the Clare Comhairle AGM in 2015 and the results were fed back to relevant company. Clare Youth Service decided to deliver this programme with funding from the Clare local development company, and during 2016 and 2017, 752 young people took part in the programme in secondary schools across Clare.

The Clare Comhairle informed the Committee that ten of its members have now received teacher training in this programme, and so the Comhairle is now in a position to deliver this programme.

[43] Joint Committee on Children and Youth Affairs, Debate: 07 February 2018.

4.4.8 WICKLOW COMHAIRLE NA NÓG

During the engagement of the Joint Committee and Children and Youth Affairs on 07 February 2018 Wicklow Comhairle na nÓg described the work that it is has done in this area to the Committee.

Wicklow Comhairle na nÓg informed the Committee that its work in this area began with what it calls the Great Wicklow Youth Survey. This survey was completed by over 1,000 young people between the ages of 12-18 in County Wicklow. From an analysis of the results, the Wicklow Comhairle informed the Committee that cyberbullying was shown to be one of the most important issues, along with mental health and youth homelessness.

As a means of delving deeper into the issue of cyberbullying, the Wicklow Comhairle conducted a survey online where respondents could make submissions. More than 220 young people responded to the survey.

The Wicklow Comhairle then hosted workshops around the county to discuss the results of the survey with various stakeholders. The Wicklow Comhairle conducted walk-in debates where people gave their opinions on the results of the survey. The overwhelming feedback indicated that the Wicklow Comhairle should develop a charter which speaks to all of the relevant people within the picture of cyberbullying.

The Wicklow Comhairle has since created its charter, and it is directed at those who are bullied, those who are bullies, bystanders, those who are in authority and to all young people in general.

The members of the Wicklow Comhairle informed the Committee that it is their intention to share the charter within Wicklow and beyond, if there is interest.

The Joint Committee notes and compliments the efforts of the young people in both Clare and Wicklow Comhairle na nÓg for the work that they have done in this area. However, the Committee also believes that the very fact that this type of work is being undertaken by organisations such as Comhairle na nÓg further highlights that there is a need for a more formalised structure in this regard to be put in place, and that this structure should be formed in consultation with youth organisations such as Comhairle na nÓg so as to ensure that the voices of children and young people are taken into account.[44]

[44] Joint Committee on Children and Youth Affairs, Debate: 07 February 2018.

4.4.9 RECOMMENDATIONS

On the basis of the evidence presented above, the Joint Committee has a number of observations to make, following which it will make its recommendation(s).

The Joint Committee recommends that a National Strategy on Children's Cyber Safety, which outlines the Government's plans to address and resource the issues around Cyber Safety, should be introduced by Government. The Strategy should also take account of new developments that may accrue from this Report.

Responsibility for this Strategy should sit with the four key Departments in this space, i.e. the Department of Communications, Climate Action and Environment, the Department of Justice and Equality, the Department of Education and Skills and the Department of Children and Youth Affairs.

Ultimately, this Strategy should be developed, coordinated, implemented and reviewed by the Government Department which is assigned lead responsibility for this area.

Recommendation 4
The Joint Committee recommends that a National Strategy on Children's Cyber Safety, which outlines the Government's plans to address and resource the issues around Cyber Safety, should be introduced by Government. The Strategy should also take account of new developments that may accrue from this Report.

The Joint Committee recommends that the Government should launch a communications and public awareness campaign on Cyber Safety that is directed at children and young people and, by extension, parents.

The key focus of this Campaign should be to provide support and education for children and young people, and their parents. The Strategy should be formulated in such a way as to highlight the potential risks that come with using the Internet and to also highlight what one can do if adversely affected by content on the Internet. The Strategy should also be formulated in such a way as to highlight the numerous benefits that using the Internet can bring and to also highlight how one can take advantage of these benefits in a safe and responsible manner.

Recommendation 5
The Joint Committee recommends that the Government should launch a National Communications and Public Awareness campaign on Cyber Safety that is directed at Children and Young people, and, by extension, parents.

Recommendation 6
The Joint Committee recommends that both primary and post-primary schools should encourage and accommodate peer-to-peer workshops on Cyber Safety in schools.

Recommendation 7
The Joint Committee recommends that both primary and post-primary schools should appoint teachers as "Digital Safety Ambassadors" and that these teachers should be provided with supports and training so that students have an appropriate person to approach when issues arise in this area.

Recommendation 8
The Joint Committee recommends that both primary and post-primary schools and local libraries should be encouraged and supported to host parent's education and awareness evenings on Cyber Safety. The Joint Committee believes that presentations should be given by Children and Young People themselves in this regard.

The Joint Committee notes the important work and positive contribution which Programmes, like the Green-Schools Programme, have made to raising awareness and encouraging children to be active participants when it comes to environmental matters. A similar Programme regarding Cyber Safety would provide a useful vehicle for encouraging Children and Young People to become involved in this area.

Recommendation 9
The Joint Committee recommends that the Government advance the establishment of a Cyber Safety Programme in both primary and post-primary schools.

The Joint Committee recommends that Cyber Safety education should be formalised on both the primary school curriculum and the post-primary school curriculum.

At present, Cyber Safety education is offered in an unsystematic and disparate fashion, particularly in primary schools, as the level of education which is provided is often dictated by the resources available to each school.

The current primary school curriculum was also published in 1999 and so may not take account of technologies that have developed in the meantime.

Again, the focus in this regard should be to empower children and young people on the positives of the Internet, while also educating them on the potential dangers with a view to ultimately building online resilience.

Adequate resources should be made available to schools to ensure that children and young people receive education in this regard and to ensure that teachers are in a position to provide this education. In addition Cyber Safety should form part of teacher training for both primary and post primary levels to ensure teachers themselves feel adequately knowledgeable to deal with this subject matter in schools.

Recommendation 10
The Joint Committee recommends that Cyber Safety education should be formalised on both the primary school curriculum and the post-primary school curriculum.

Recommendation 11
The Joint Committee recommends that Cyber Safety education should form a mandatory part of both primary and post-primary teacher training courses.

4.5 PROTECTION AND PREVENTION

In terms of specific protective and preventative measures outside of those already mentioned in this Report, the Joint Committee on Children and Youth Affairs decided that for the purposes of its consideration of this topic that it would focus on the efforts that social media platforms are making in this sphere, the statutory right to be forgotten and the 'Digital Age of Consent'.

At the outset of this section of the report, the Joint Committee would like to recognise the excellent work that is being done in this area by both Hotline.ie and An Garda Síochána. These witnesses met with the Joint Committee on 27 September 2017 and 25 October 2017 respectively.

These witnesses outlined the work that they do and the Joint Committee is very impressed at what they have achieved, often with limited resources.

However, this report is focused on identifying gaps in the current framework and, as such, the evidence provided by these witnesses has not been included in detail in the final report as they discussed the programmes already in place in this space which provide a vital part of the mechanisms currently in situ to protect children online.

The Joint Committee recommends that these programmes continue to be adequately funded and resourced to deal with the scale and pace of change in the issues that arise for children and young people online. The Joint Committee endorses the work currently being undertaken by both An Garda Síochána and Hotline in particular.

4.5.1 STATUTORY RIGHT TO BE FORGOTTEN AND 'DIGITAL AGE OF CONSENT'

The Joint Committee notes that the need for recognition of the statutory right to be forgotten and a determination on the 'Digital Age of Consent' are themes which arose sporadically during its engagements with various stakeholders and from submissions received by the Joint Committee.

It is important to note that the 'Digital Age of Consent' was not the focus of the Joint Committee's engagement on the topic of Cyber Security as it forms part of the *Data Protection Bill 2018* which will come under the remit of the Committee on Justice and Equality. However, as some stakeholders mentioned it in their engagement with the Committee, a brief outline of some of the views of key stakeholders is given here and the Joint Committee recommends that the Committee on Justice and Equality consider fully children's rights, as well as child protection concerns, when they are debating the Bill.

4.5.1.1 DR. GEOFFREY SHANNON, SPECIAL RAPPORTEUR ON CHILD PROTECTION

Dr. Geoffrey Shannon, in the 9th Report of the Special Rapporteur on Child Protection, called for a formal acknowledgment of the importance of the right to be forgotten on behalf of Irish authorities, as per Article 17 of the prospective General Data Protection Regulation.[45] In this Report, Dr. Shannon states:

> *The relevance for children of the 'right to be forgotten' should be acknowledged, children should be educated about the matter, and it should be understood that the age at which an individual posts information online should be considered a very important factor in decisions about whether to remove an individual's personal information from sites.*[46]

Dr. Shannon also reiterated his call for a formal acknowledgement of the right to be forgotten during the meeting of the Joint Committee on Children and Youth Affairs on 18 October 2017.

During the engagement of the Joint Committee on Justice and Equality on 05 July 2017, Dr. Shannon called for the 'Digital Age of Consent' to be set at 13 years of age. Dr. Shannon said:

> *It appears, therefore, that no determination on this critical issue has been made by the legislature at this point in time. I believe that Ireland should take the opportunity now to designate the lowest permissible age - namely 13 - as the age of digital consent for this jurisdiction. This lower 'Digital Age of Consent' has also been recommended by children's organisations such as the Children's Rights Alliance. Ahead of this meeting with the committee I took the opportunity last week to discuss the issue with the Ombudsman for Children, who supports my view that the age of digital consent should be set at 13 years of age. A variety of competing children's rights and practical realities support the argument that the appropriate age, having regard to the permissible age range delineated by the GDPR, should be the lowest age possible.*[47]

The Joint Committee notes the views of both the Ombudsman for Children and the Children's Rights Alliance with regard to the 'Digital Age of Consent'.

[45] Article 17, *General Data Protection Regulation*, 27 April 2016.
[46] Dr. Geoffrey Shannon, *Ninth Report of the Special Rapporteur on Child Protection*, 2016, p. 24.
[47] Joint Committee on Justice and Equality, Debate: 05 July 2017.

4.5.1.2 IRISH SOCIETY FOR THE PREVENTION OF CRUELTY TO CHILDREN

The ISPCC made a submission to the Joint Committee on Children and Youth Affairs in advance of its meeting on 22 February 2017. As part of this submission, the ISPCC indicated that it had responded to the consultation hosted by the Department of Justice and Equality's on the 'Digital Age of Consent', and explicitly called for Dr. Geoffrey Shannon's comments on the right to be forgotten to be taken into consideration. The ISPCC stated:

> *The ISPCC notes the recommendations by Dr. Geoffrey Shannon on the right of children to be forgotten on the internet in the Ninth Report of the Special Rapporteur on Child Protection. The ISPCC recommends that the Department consult on and consider carefully how this right will be achieved in the consultation on this issue.*[48]

Again, as part of this same submission, the ISPCC indicated that it had responded to the consultation hosted by the Department of Justice and Equality's on the 'Digital Age of Consent'. There, the ISPCC also called for the 'Digital Age of Consent' to be set at 13 years of age. The ISPCC stated:

> *The ISPCC recommends that national legislation be introduced to set the age limit at 13 years for Ireland where services provided are commercial.*
>
> *Our three key points are as follows:*
>
> 1. *The ISPCC disagrees in principle with the European Commission's inclusion in this directive of the introduction of an age at which parental consent should be sought for children to access digital services. There are several reasons for our position in this regard.*
>
>   *First, the UN Convention on the Rights of the Child does not place age limits on children's access to services. The age of a child does not necessarily reflect maturity and the setting of an arbitrary age limit to access these services is not appropriate. We are not aware of any comprehensive research that would support the setting of a requirement for parental consent at any particular age.*

[48] ISPCC *Submission to the Department of Justice and Equality*'s consultation process on the statutory "age of digital consent", December 2016, p. 2.

Second, requiring services to receive the consent of a parent in order for a child to access them is not a guarantee of protection from commercial exploitation.

Third, the requirement to obtain parental consent could inhibit the access of children to services which are beneficial to them.

2. *Where services are beneficial to a child and are provided on a non-commercial basis there should be no requirement for parental consent at any age. The definition of 'preventative or counselling services offered directly to a child' as outlined in Recital 38 must be interpreted broadly so as to ensure the widest possible availability of such services to children without any barriers being placed on their access.*

3. *Where services provided are commercial, the setting of an age limit should be done at the youngest age – in this case the age 13 permitted under the directive.*[49]

4.5.1.3 THE JOINT COMMITTEE ON JUSTICE AND EQUALITY

The Joint Committee on Children and Youth Affairs notes that in a pre-legislative scrutiny report of the General Scheme of the Data Protection Bill 2017 published in November 2017 that the Joint Committee on Justice and Equality recommended that the 'Digital Age of Consent' is set at 13 years of age. The Joint Committee on Justice and Equality stated:

> *The Committee recommends that the 'Digital Age of Consent' be set at 13 years of age. The Committee also recommends that this age of consent be reviewed at appropriate intervals to ensure it remains suitable as technology evolves.*[50]

4.5.1.4 SPUNOUT.IE

Spunout.ie, Ireland's youth information website created by young people, for young people, wrote to the Joint Committee on Children and Youth Affairs on 12 February 2018 to iterate its strong support for retaining and formalising the age of digital consent at 13 years of age. Spunout.ie said:

---

[49] ISPCC Submission to the Department of Justice and Equality's consultation process on the statutory "age of digital consent", December 2016, pp. 5-6.
[50] Joint Committee on Justice and Equality, Report on pre-legislative scrutiny of the General Scheme of the Data Protection Bill 2017, November 2017, p. 34.

SpunOut.ie wishes to iterate our strong support for retaining and formalising the current effective age of digital consent at 13.

We believe this is the only way to honour the rights to expression and information set out in the UN Convention on the Rights of the Child, and that the issues facing young people and parents can best be tackled through increased digital education for parents and young people, parental involvement and industry enforcement rather than arbitrary and unenforceable age restrictions on internet use.[51]

4.5.1.5 PROFESSOR BARRY O'SULLIVAN AND DR. MARY AIKEN

Professor Barry O'Sullivan and Dr. Mary Aiken made a joint submission to the Joint Committee on Children and Youth Affairs in advance of its meeting on 13 February 2018. As part of this submission, Professor O'Sullivan and Dr. Aiken iterated their support for setting the 'Digital Age of Consent' at 16 years of age. Professor O'Sullivan and Dr. Aiken stated:

Given the substantial risks to the safety, security and wellbeing of children and young people online, Ireland needs to put in place a policy framework and an associated educational programme that ensures that our children are sufficiently aware and responsible to understand and exercise their digital rights by the time they reach the 'Digital Age of Consent'. In the absence of a rigorous basis for any specific age at this point, a prudent approach would be to set the 'Digital Age of Consent' in Ireland at 16.

We would like to state unequivocally our opposition to the Irish Government's current position to set the 'Digital Age of Consent' in Ireland at 13 years.[52]

Professor O'Sullivan and Dr. Aiken reiterated their support for setting the 'Digital Age of Consent' at 16 years of age at the meeting of the Joint Committee on Children and Youth Affairs on 13 February 2018.[53]

4.5.2 SOCIAL MEDIA PLATFORMS

The Joint Committee invited Facebook, Instagram and Snapchat to attend meetings on the topic of Cyber Security for Children and Young Adults. The Joint Committee notes that Facebook was the only platform to respond in the positive, while Snapchat and Instagram sent submissions in place of attending.

[51] Received in correspondence by the Joint Committee on Children and Youth Affairs on 12 February 2018.
[52] Professor Barry O'Sullivan, Dr. Mary Aiken, Meeting of the Joint Committee on Children and Youth Affairs, Opening Statement: 13 February 2018.
[53] Joint Committee on Children and Youth Affairs, Debate: 13 February 2018.

4.5.2.1 FACEBOOK

At the meeting of the Joint Committee on Children and Youth Affairs on 06 December 2017 Facebook described how it removes malicious content from its platform. Facebook said:

> *Our team receives tens of millions of reports every week from all over the world. We prioritise the most serious issues first. Many of the reports related to suicide, credible threats, child safety or bullying are reviewed ahead of any other topics. We work hard to ensure that those reports are reviewed by our team as quickly as possible. The vast majority of reports are reviewed within 24 hours and evaluated against our community standards. Our team of experts include native speakers of more than 50 languages working 24-7 throughout the globe. The team is close to 7,500 people, several hundred of whom are located in our Dublin headquarters.*
>
> *If reported content is found to be against our community standards, it is immediately removed. We also close the loop with the person who reported the content to let him or her know what action we have taken. People who engage in abusive behaviour on Facebook face varying consequences, ranging from a warning to losing their accounts permanently. In the most severe cases, for example, where child exploitation is involved, such people can be referred to law enforcement. Our help centre includes a range of additional contact forms where people can report copyright violations, privacy rights violations, defamation and more.*[54]

4.5.2.2 SNAPCHAT

The Joint Committee on Children and Youth Affairs notes that Snapchat was invited to attend a Committee meeting in a letter dated 18 January 2018 and that it declined on 23 January 2018.

Snapchat sent a submission to the Joint Committee on 29 January and this can be accessed on the Committee's website.[55]

4.5.2.3 INSTAGRAM

The Joint Committee on Children and Youth Affairs notes that Instagram was invited to attend a Committee meeting in a letter dated 18 January 2018 and that it declined on 25 January 2018.

[54] Joint Committee on Children and Youth Affairs, Debate: 06 December 2017.
[55] Joint Committee on Children and Youth Affairs, Submission: 29 January 2018.

Instagram sent a submission to the Joint Committee on 08 February 2018 and this can be accessed on the Committee's Website.[56]

4.5.3 RECOMMENDATIONS

On the basis of the evidence presented above, the Joint Committee has a number of observations to make, following which it will make its recommendations.

The Joint Committee recommends that Children and Young people are made aware of the "right to be forgotten" as part of the proposed National Communications and Public Awareness campaign on Cyber Safety.

The Joint Committee believes that targeted initiatives will be beneficial in ensuring that Children and Young People are aware of their "right to be forgotten", as per Article 17 of the General Data Protection Regulation, as well as making them aware of the limitations to this right.

Recommendation 12
The Joint Committee recommends that Children and Young people are made aware of the "right to be forgotten" as part of the proposed National Communications and Public Awareness campaign on Cyber Safety.

Recommendation 13
The Joint Committee recommends that the Joint Committee on Justice and Equality should have due regard to both child protection concerns and children's rights in the context of its Committee Stage consideration of the *Data Protection Bill 2018*, with particular emphasis on the "'Digital Age of Consent'".

Recommendation 14
The Joint Committee recommends that Social Media Platforms do more to strengthen their safety policies with a view to protecting their users. This could be done in consultation with the proposed Office of the Digital Safety Commissioner.

[56] Joint Committee on Children and Youth Affairs , Submission: 20 February 2018.

4.5 LEGAL FRAMEWORK

The Law Reform Commission, in its *Report on Harmful Communications and Digital Safety* recommended that the law in relation to cyber safety should be reformed. In particular, the Law Reform Commission recommends that the following changes occur:

- The repeal of Section 10 of the *Non-Fatal Offences Against the Person Act 1997* to be replaced with an offence of harassment modelled on section 10 and that includes two additional provisions: (a) that the harassment offence should expressly apply to harassment by any means of communication, including through digital and online communications; and (b) that it should deal with indirect forms of communication, such as setting up fake online social media profiles.
- That an offence of stalking separate from the related offence of harassment be enacted.
- That Section 13 of the *Post Office (Amendment) Act 1951* be repealed and replaced with an offence of distributing a threatening, false, indecent or obscene message by any means of communication and with the intent to cause alarm, distress of harm or being reckless as to this.
- The enactment of an indictable offence of distributing an intimate image without the consent of the person depicted in the image, or threatening to do so, and with the intent to cause alarm, distress of harm or being reckless as to this. The enactment of a summary, strict liability offence of taking or distributing an intimate image of another person without the other person's consent.[57]

The Joint Committee notes that the need to amend legislation, particularly as it relates to criminal activity in this sphere, was a common theme that arose consistently during its engagements with various stakeholders.

4.5.1 AMENDMENT TO THE OFFENCE OF HARASSMENT

In relation to the possible repeal and replacement of Section 10 of the *Non-Fatal Offences Against the Person Act 1997* with a new offence of harassment, the Law Reform Commission states:

> *The Commission considers that amending the harassment offence to include a specific reference to harassment by digital or online means would offer important clarification as to the scope of the offence, similar to the specific mention of harassment by telephone which is already included in section 10 of the 1997 Act. This clarification could lead to an increase in reporting of this type*

[57] Adapted from: Law Reform Commission, *Report on Harmful Communications and Digital Safety*, pp. 155-156.

of harassment. Expressly identifying harassment by digital or online means in the legislation as a particular form of the wider offence of harassment would also underline society's recognition of its seriousness and the need to prevent and punish it…

…The reference in section 10 to "telephone" without any mention of other forms of electronic communication makes the section appear outdated. Thus, including a reference to harassment by digital or online communication would clarify and modernise the wording of the harassment offence. It would also correctly label the conduct that is covered by the offence and ensure that harassment by digital or online means is not a hidden form of harassment as section 10 of the 1997 Act currently suggests.

The Commission thus recommends that section 10 of the Non-Fatal Offences Against the Person Act 1997 be repealed and replaced with a harassment offence which expressly applies to harassment by all forms of communication including through digital and online communications such as through a social media site or other internet medium. The Commission recommends that this amendment be made by including a definition of "communication" in the legislation which would extend to any form of communication including by letter, telephone (including SMS text message) or digital or online communication such as through a social media site or other internet medium.[58]

The Law Reform Commission also suggests that the offence of harassment should be expanded to include communications with third parties. The Law Reform Commission states:

By expanding the harassment offence to include communications with a third person rather than just the target of the harassment, an important gap in the law of harassment would be filled.

Currently, indirect communications such as posting content on public websites or sending harmful communications to third parties connected to the victim do not appear to be covered by section 10 in most cases. This has been confirmed during the consultative process leading to this Report. Although this Report also proposes an offence designed to deal with indirect victim-shaming behaviour (so-called "revenge porn"), which some consultees have suggested could obviate the need for a reference to indirect harassment, the expansion of the harassment offence to include indirect activity is nonetheless warranted because

[58] Law Reform Commission, *Report on Harmful Communications and Digital Safety*, 2016, p. 55

not all indirect behaviour is related to the victim-shaming behaviour. Moreover, in certain cases that type of behaviour may be part of a pattern of persistent behaviour where charging the perpetrator with harassment would be appropriate.[59]

4.5.1.1 IRISH SOCIETY FOR THE PREVENTION OF CRUELTY TO CHILDREN

During the engagement of the Joint Committee on Children and Youth Affairs on 22 February 2017, the ISPCC informed the Committee that it strongly agrees that new offences need to be introduced to reflect the current online world. The ISPCC said:

> *We spent a great deal of time examining the LRC report and I urge members to read it. It is an exceptional piece work, which gives a substantial overview of digital safety law, where the gaps are and how they can be filled. We strongly agree with the creation of new offences that reflect our online world. Harassment online is a different from offline harassment. It works differently and it is more pervasive…*
>
> *..the LRC has said that in creating new offences, children should not be criminalised in that way. The offences should be created to detect and prosecute adults but we should behave responsibly in taking prosecutions against a child. That would only be done in exceptional circumstances at the discretion of the DPP.*[60]

4.5.1.2 DR. GEOFFREY SHANNON

During the engagement of the Joint Committee on Children and Youth Affairs on 18 October 2017, Dr. Shannon, in supporting the suggested amendments to the criminal law as it relates to harassment as set out by the Law Reform Commission, said the following:

> *In Ireland, the law in force at present only deals with harassment to a limited extent and has yet to be updated to take into account the potential for online abuse. Section 10 of the Non-Fatal Offences Against the Person Act 1997 creates the offence of harassment in criminal law. While section 10 already criminalises online or digital harassment as it refers to harassment "by any means", online and digital harassment is under-reported and under-prosecuted in Ireland. This suggests that section 10 of the 1997 Act in its current form is not sufficient to deal with these types of behaviour. For example, the existing reference in section 10 to the use of the telephone alone in outlining the offence*

[59] Law Reform Commission, *Report on Harmful Communications and Digital Safety*, 2016, pp. 60-61
[60] Joint Committee on Children and Youth Affairs, Debate: 22 February 2017.

of harassment, without any reference to the Internet, makes the current offence appear archaic and outdated.

The definition of harassment should be broadened. Any new definition should criminalise what is known as "indirect harassment". Currently, the offender must persistently follow, watch, pester, beset or communicate with the victim. The offence does not include communications to third parties about the victim, such as posting content on public websites or sending emails to persons connected with the victim, but not directly to him or her. I recommend therefore that not only should section 10 be amended to encompass online and digital communications, the definition should be further developed to allow prosecutions for indirect harassment to fall within same. Having an overall broader offence of harassment on the Irish criminal Statute Book would be preferable, thereby encompassing new forms of behaviour that have arisen through the development of digital technology and which merit criminalisation.[61]

4.5.2 INTRODUCTION OF A SPECIFIC STALKING OFFENCE

In relation to the possible introduction of a specific stalking offence, the Law Reform Commission states:

Firstly, specifically naming stalking as an offence appears to have had a significant practical effect, with the number of prosecutions for stalking activity increasing in both Scotland and England and Wales since they introduced specific stalking offences.

Secondly, identifying stalking as a specific crime carries particular importance for victims of stalking because of the "hidden" nature of the crime as well as its more serious nature compared to harassment. This has been acknowledged by the English Independent Parliamentary Inquiry into Stalking Reform stating, that "[n]aming the crime appears to increase public protection from stalking and the confidence of victims". Thus, by specifically naming stalking in legislation, rather than including it within the broad-ranging offence of harassment, the different and more insidious character of the crime is underlined.

The Commission therefore recommends that a stalking offence, separate from the related offence of harassment, should be introduced. The Commission considers that the essential ingredients of the stalking offence should be the same as the proposed, amended, harassment offence, so that the offence would be committed where a person "stalks" another person by persistently following,

[61] Joint Committee on Children and Youth Affairs, Debate: 18 October 2017.

watching, pestering or besetting another person or by persistently communicating by any means of communication with the other person or by persistently communicating with a third person by any means of communication about the other person.

For the purposes of this offence, a person would stalk another person where he or she, by his or her acts intentionally or recklessly, seriously interferes with the other person's peace and privacy and causes alarm, distress or harm to the other person and his or her acts are such that a reasonable person would realise that the acts would seriously interfere with the other person's peace and privacy and cause alarm, distress or harm to the other person. Thus, the stalking offence would differ from the harassment offence by requiring the intentional or reckless acts of the perpetrator to interfere seriously with the victim's peace and privacy and cause him or her alarm, distress or harm, as opposed to the harassment offence which makes these alternative requirements.[62]

4.5.2.1 IRISH SOCIETY FOR THE PREVENTION OF CRUELTY TO CHILDREN

During the engagement of the Joint Committee on Children and Youth Affairs on 22 February 2017, the ISPCC informed the Committee that it agrees that a new stalking offence needs to be introduced. The ISPCC said:

A distinction needs to be made between technology and use of the Internet and social media, but we also need to make a distinction between what is or should be illegal behaviour online and what is harmful behaviour. Illegal behaviour is simpler to understand and define. For example, the Law Reform Commission has stated that online stalking needs to be prescribed as an offence in law. That would make it easier to detect and prosecute. We agree with that recommendation. Online harassment also needs to be a prosecutable offence.

Cyberbullying is a form of harmful behaviour. Severe and malicious bullying that becomes harassment then becomes a form of illegal behaviour, but we need to understand the two separately. If we do not, we are at risk of criminalising children and young people who often undertake actions online without understanding the consequences.[63]

[62] Law Reform Commission, *Report on Harmful Communications and Digital Safety*, 2016, pp. 67-68
[63] Joint Committee on Children and Youth Affairs, Debate: 22 February 2017.

4.5.2.2 DR. GEOFFREY SHANNON

During the engagement of the Joint Committee on Children and Youth Affairs on 18 October 2017, Dr. Shannon echoed the sentiments of the Law Reform Commission with regard to creating a specific stalking offence. Dr. Shannon said:

> *In light of the loopholes in existing criminal legislation to which I referred, action has been proposed by the Minister for Justice and Equality. At the final Cabinet meeting of December 2016, the then Minister received the approval of the Cabinet to draft the non-fatal offences (amendment) Bill, now named the harmful communications and digital safety Bill 2017. I note that no further progress has been made in respect of the publication of this legislation and I suggest that it receive priority. The Bill will legislate to put stalking, including cyberstalking and revenge pornography, on the criminal Statute Book and provide for the creation of new criminal offences, including criminalising the act of intentionally posting intimate images of a person online without his or her consent.*[64]

4.5.3 AMENDMENT TO THE OFFENCE OF DISTRIBUTING THREATENING, FALSE, INDECENT OR OBSCENE MESSAGES

In relation to the possible repeal and replacement of Section 13 of the *Post Office (Amendment) Act 1951* with a new offence, the Law Reform Commission states:

> *Thus, the Commission recommends that section 13 be repealed and replaced with a new offence designed to apply to all forms of communication including messages distributed online through social media, and that this should include not only messages to a person but also about a person. This new offence would be committed where a person intentionally or recklessly for the purpose of causing alarm, distress or harm, by any means of communication distributes or publishes a threatening, false, indecent or obscene message to or about another person or distributes or publishes such a message persistently. This is broadly based on the factors in section 13 of the 1951 Act, but the wording has been aligned with the "harm" test in section 10 of the Non-Fatal Offences Against the Person Act 1997.*
>
> *The new offence of distributing a threatening, false, indecent or obscene message reflects section 13 of the 1951 Act in that one act is sufficient for the offence to be committed. The offence also reflects section 13 of the 1951 Act by*

[64] Joint Committee on Children and Youth Affairs, Debate: 18 October 2017.

being capable of applying to persistent acts, and can thus be compared with the restated harassment offence and the new stalking offence.[65]

4.5.3.1 DR. GEOFFREY SHANNON, SPECIAL RAPPORTEUR ON CHILD PROTECTION

In a submission sent to the Joint Committee on Health and Children in advance of its meeting on 19 November 2013, Dr. Shannon informed the Committee that he believed that a new offence needed to be created in this regard. Dr. Shannon said:

> *Existing laws regarding harassment can be used to incorporate cyber-bullying. For example, a review of the Post Office (Amendment) Acts should be undertaken with a view to incorporating emerging means of cyber-bullying. Prosecutions have been brought under section 13(1) of the Post Office (Amendment) Act, 1951. That Act refers to messages sent by telephone and while it specifically includes text messages, it does not include any reference to email or other internet messages. An offence relating to this form of communication would be welcomed.*[66]

Dr. Shannon, in his sixth report in his capacity as Special Rapporteur on Child Protection, again called for the law in this area to be amended. Dr. Shannon said:

> *Existing laws regarding harassment can be used to incorporate cyber-bullying incidents. A review of the Post Office (Amendment) Acts should be undertaken with a view to incorporating emerging means of cyber-bullying.*[67]

4.5.3.2 THE INTERNET CONTENT GOVERNANCE ADVISORY GROUP

The Internet Content Governance Advisory Group's Report, which was published in May 2014, also recommended that the legislation in this area should be amended. The Report stated:

> *We recommend that the Communications Regulation (Amendment) Act 2007 be amended to include 'electronic communications' within the definition of measures dealing with the 'sending of messages which are grossly offensive, indecent, obscene or menacing'.*[68]

[65] Law Reform Commission, *Report on Harmful Communications and Digital Safety*, 2016, p. 101
[66] Dr. Geoffrey Shannon, Meeting of the Joint Committee on Health and Children, Opening Statement: 19 November 2013.
[67] Dr. Geoffrey Shannon, *Sixth Report of the Special Rapporteur on Child Protection*, 2013, p. 96.
[68] *Report of the Internet Content Governance Advisory Group*, May 2014, p. 9.

4.5.4 THE ENACTMENT OF OFFENCES RELATING TO THE DISTRIBUTION OF INTIMATE IMAGES WITHOUT THE CONSENT OF THE PERSON DEPICTED

In relation to the possible enactment of offences relating to the distribution of intimate images without the consent of the person depicted therein, the Law Reform Commission states:

> *The Commission recommends the enactment of an indictable offence of distributing an intimate image without the consent of the person depicted in the image, or threatening to do so, and with the intent to cause alarm, distress of harm or being reckless as to this.*
>
> *The Commission recommends the enactment of a summary, strict liability offence of taking or distributing an intimate image of another person without the other person's consent.*
>
> *The Commission recommends that the definition of "consent" applicable to the intimate images offences should be that a person agrees by choice and that the person has the freedom and capacity to make that choice.*[69]

4.5.5 RECOMMENDATIONS

On the basis of the evidence presented above, the Joint Committee makes the following recommendations:

Recommendation 15
The Joint Committee recommends that Section 10 of the *Non-Fatal Offences Against the Person Act 1997* should be repealed and replaced with a new offence of harassment which expressly applies to harassment by all forms of communication including through digital and online communications, as per the Law Reform Commission's *Report on Harmful Communications and Digital Safety*.

Recommendation 16
The Joint Committee recommends that a specific stalking offence, separate from the related offence of harassment, should be introduced, as per the Law Reform Commission's *Report on Harmful Communications and Digital Safety.*

[69] Law Reform Commission, *Report on Harmful Communications and Digital Safety*, 2016, p. 105.

Recommendation 17
The Joint Committee recommends that Section 13 of the *Post Office (Amendment) Act 1951* should be repealed and replaced with a provision which would make the distribution of threatening, false, indecent or obscene messages, whether that message is to a person or about a person, an offence, as per the Law Reform Commission's *Report on Harmful Communications and Digital Safety.* This provision should also apply to all forms of communication, including any online communication.

Recommendation 18
The Joint Committee recommends the enactment of offences relating to the distribution of intimate images without the consent of the person depicted, as per the Law Reform Commission's *Report on Harmful Communications and Digital Safety.*

APPENDIX 1: TERMS OF REFERENCE

COMMITTEE ON CHILDREN AND YOUTH AFFAIRS

TERMS OF REFERENCE

a. Functions of the Committee – derived from Standing Orders [DSO 84A; SSO 70A]

(1) The Select Committee shall consider and report to the Dáil on—

(a) such aspects of the expenditure, administration and policy of a Government Department or Departments and associated public bodies as the Committee may select, and

(b) European Union matters within the remit of the relevant Department or Departments.

(2) The Select Committee appointed pursuant to this Standing Order may be joined with a Select Committee appointed by Seanad Éireann for the purposes of the functions set out in this Standing Order, other than at paragraph (3), and to report thereon to both Houses of the Oireachtas.

(3) Without prejudice to the generality of paragraph (1), the Select Committee appointed pursuant to this Standing Order shall consider, in respect of the relevant Department or Departments, such—

(a) Bills,

(b) proposals contained in any motion, including any motion within the meaning of Standing Order 187,

(c) Estimates for Public Services, and

(d) other matters as shall be referred to the Select Committee by the Dáil, and

(e) Annual Output Statements including performance, efficiency and effectiveness in the use of public monies, and

(f) such Value for Money and Policy Reviews as the Select Committee may select.

(4) The Joint Committee may consider the following matters in respect of the relevant Department or Departments and associated public bodies:

(a) matters of policy and governance for which the Minister is officially responsible,

(b) public affairs administered by the Department,

(c) policy issues arising from Value for Money and Policy Reviews conducted or commissioned by the Department,

(d) Government policy and governance in respect of bodies under the aegis of the Department,

(e) policy and governance issues concerning bodies which are partly or wholly funded by the State or which are established or appointed by a member of the Government or the Oireachtas,

(f) the general scheme or draft heads of any Bill,

(g) any post-enactment report laid before either House or both Houses by a member of the Government or Minister of State on any Bill enacted by the Houses of the Oireachtas,

(h) statutory instruments, including those laid or laid in draft before either House or both Houses and those made under the European Communities Acts 1972 to 2009,

(i) strategy statements laid before either or both Houses of the Oireachtas pursuant to the Public Service Management Act 1997,

(j) annual reports or annual reports and accounts, required by law, and laid before either or both Houses of the Oireachtas, of the Department or bodies referred to in subparagraphs (d) and (e) and the overall performance and operational results, statements of strategy and corporate plans of such bodies, and

(k) such other matters as may be referred to it by the Dáil from time to time.

(5) Without prejudice to the generality of paragraph (1), the Joint Committee appointed pursuant to this Standing Order shall consider, in respect of the relevant Department or Departments—

(a) EU draft legislative acts standing referred to the Select Committee under Standing Order 114, including the compliance of such acts with the principle of subsidiarity,

(b) other proposals for EU legislation and related policy issues, including programmes and guidelines prepared by the European Commission as a basis

of possible legislative action,

(c) non-legislative documents published by any EU institution in relation to EU policy matters, and

(6) matters listed for consideration on the agenda for meetings of the relevant EU Council of Ministers and the outcome of such meetings.The Chairman of the Joint Committee appointed pursuant to this Standing Order, who shall be a member of Dáil Éireann, shall also be the Chairman of the Select Committee.

(7) The following may attend meetings of the Select or Joint Committee appointed pursuant to this Standing Order, for the purposes of the functions set out in paragraph (5) and may take part in proceedings without having a right to vote or to move motions and amendments:

(a) Members of the European Parliament elected from constituencies in Ireland, including Northern Ireland,

(b) Members of the Irish delegation to the Parliamentary Assembly of the Council of Europe, and

(c) at the invitation of the Committee, other Members of the European Parliament.

b. Scope and Context of Activities of Committees (as derived from Standing Orders) [DSO 84; SSO 70]

(1) The Joint Committee may only consider such matters, engage in such activities, exercise such powers and discharge such functions as are specifically authorised under its orders of reference and under Standing Orders.

(2) Such matters, activities, powers and functions shall be relevant to, and shall arise only in the context of, the preparation of a report to the Dáil and/or Seanad.

(3) The Joint Committee shall not consider any matter which is being considered, or of which notice has been given of a proposal to consider, by the Committee of Public Accounts pursuant to Standing Order 186 and/or the Comptroller and Auditor General (Amendment) Act 1993.

(4) The Joint Committee shall refrain from inquiring into in public session or publishing confidential information regarding any matter if so requested, for stated reasons given in writing, by—

(a) a member of the Government or a Minister of State, or

(b) the principal office-holder of a body under the aegis of a Department or which is partly or wholly funded by the State or established or appointed by a member of the Government or by the Oireachtas:

Provided that the Chairman may appeal any such request made to the Ceann Comhairle / Cathaoirleach whose decision shall be final.

(5) It shall be an instruction to all Select Committees to which Bills are referred that they shall ensure that not more than two Select Committees shall meet to consider a Bill on any given day, unless the Dáil, after due notice given by the Chairman of the Select Committee, waives this instruction on motion made by the Taoiseach pursuant to Dáil Standing Order

28. The Chairmen of Select Committees shall have responsibility for compliance with this instruction.

APPENDIX 2: COMMITTEE MEMBERSHIP

Joint Committee on Children and Youth Affairs

Deputies:

Lisa Chambers (FF)

Alan Farrell (FG) [Chairman]

Kathleen Funchion (SF)

Denise Mitchell (SF)

Tom Neville (FG)

Sean Sherlock (LAB)

Anne Rabbitte (FF)

Senators:

Lorraine Clifford-Lee (FF)

Máire Devine (SF)

Joan Freeman (Ind)

Catherine Noone (FG)

Notes:

1. Deputies nominated by the Dáil Committee of Selection and appointed by Order of the Dáil of 16 June 2016.
2. Senators nominated by the Seanad Committee of Selection and appointed by Order of the Seanad on 21 July 2016.
3. Deputy Catherine Martin discharged and Deputy Kathleen Funchion appointed to serve in her stead by the Fifth Report of the Dáil Committee of Selection as agreed by Dáil Éireann on 4 October 2016.
4. Deputy Josepha Madigan discharged and Deputy Tom Neville appointed to serve in her stead by the Sixth Report of the Dáil Committee of Selection as agreed by Dáil Éireann 15 November 2016.
5. Deputy Jim Daly discharged and Deputy Alan Farrell appointed to serve in his stead by the Tenth Report of the Dáil Committee of Selection as agreed by Dáil Éireann 11 July 2017.
6. Deputy Donnchadh Ó Laoghaire discharged and Deputy Denise Mitchell appointed

by the Twelfth Report of the Dáil Committee of Selection as agreed by Dáil Éireann 03 October 2017.

7. Deputy Jan O'Sullivan discharged and Deputy Sean Sherlock appointed by the Twelfth Report of the Dáil Committee of Selection as agreed by Dáil Éireann 03 October 2017.

APPENDIX 3: GLOSSARY OF TERMS

AUP	Acceptable Usage Policy
ICGAG	The Internet Content Governance Advisory Group
ICT	Internet and Communications Technology
ISP	Internet Service Provider
ISPAI	Internet Service Providers Association of Ireland
ISPCC	The Irish Society for the Prevention of Cruelty to Children
LRC	The Law Reform Commission
NPCp	The National Parents Council – Primary
NPCpp	The National Parents Council – Post-Primary
ODSC	The Office of the Digital Safety Commissioner
OIS	The Office of Internet Safety
PDST	Professional Development Service for Teachers
RSE	Relationships and Sexuality Education
SPHE	Social, Personal and Health Education