Rialtas na hÉireann
Government of Ireland

Action Plan

For Online Safety 2018-2019

gov.ie/besafeonline

Action Plan

For Online Safety 2018-2019

Table of Contents

TAOISEACH:

“Government action alone will not and cannot remove all risks from the internet.

Individuals, parents, educators, industry and law enforcement all have roles to play in making the internet a safer place.

As the internet affects all aspects of our lives, the only approach that will truly be effective is one that involves all stakeholders playing their part.”

MINISTER FOR COMMUNICATIONS, CLIMATE ACTION AND ENVIRONMENT:

“We all know that the internet is a tool that brings enormous benefits, but there are risks and dangers that combine anonymity and distance too easily.
Given the range of different material, no one single action is going to “fix the internet”.

MINISTER FOR CHILDREN AND YOUTH AFFAIRS:

“I believe the issue of safety for children engaging in online activity presents a very serious challenge… Of course, the internet is not age-bound. The risks and dangers apply to people of all ages. But children are particularly vulnerable and they need greater protection.”

MINISTER FOR JUSTICE AND EQUALITY:

“Robust legislation is in place to tackle the evil crime of online child exploitation and I will continue to work to ensure our laws protect vulnerable children. An Garda Síochána is successfully targeting those perpetrating vile child pornography offences. My message to these criminals is that they will be targeted by law enforcement and they will face the full rigours of the law.”

MINISTER FOR EDUCATION AND SKILLS:

“New technology is revolutionising our world bringing with it fantastic opportunities but also challenges. We have an important role in equipping our citizens, in particular our children, with skills to negotiate life in a fast changing 21st century and working together raise awareness to the benefits of new technology while safeguarding our children online.”

Executive Summary - Key Objectives and Actions

Importance of Online Safety

While the State has a role to play in ensuring the public's safety, the State does not have all the answers.

Government cannot act alone in relation to online safety. Individuals, parents, educators, industry and law enforcement all have roles to play in making the internet a safer place.

The global nature of the internet also means that one country acting alone cannot tackle all of the risks. We need to work in collaboration with other countries facing similar challenges at EU and international level.

This is the Government's first Action Plan for Online Safety. The key objective of this action plan is to set out and implement actions, over a short 18 month period, that are achievable and which will have the greatest impact on Online Safety for everyone in Ireland.

We know more work will be required and further actions must be taken in the years following implementation of this plan.

This plan provides a strong step forward in addressing Online Safety. It demonstrates the whole of Government approach that is being taken, which is particularly important for an issue that spans so many different Departments, and deals with such a wide range of concerns.

The Action Plan is centred on five goals:

- **Goal 1**: Online Safety for All
- **Goal 2**: Better Supports
- **Goal 3**: Stronger Protections
- **Goal 4**: Influencing Policy
- **Goal 5**: Building our Understanding

Summary of Actions

The Action Plan sets out 25 specific actions to be progressed over the coming 18 months:

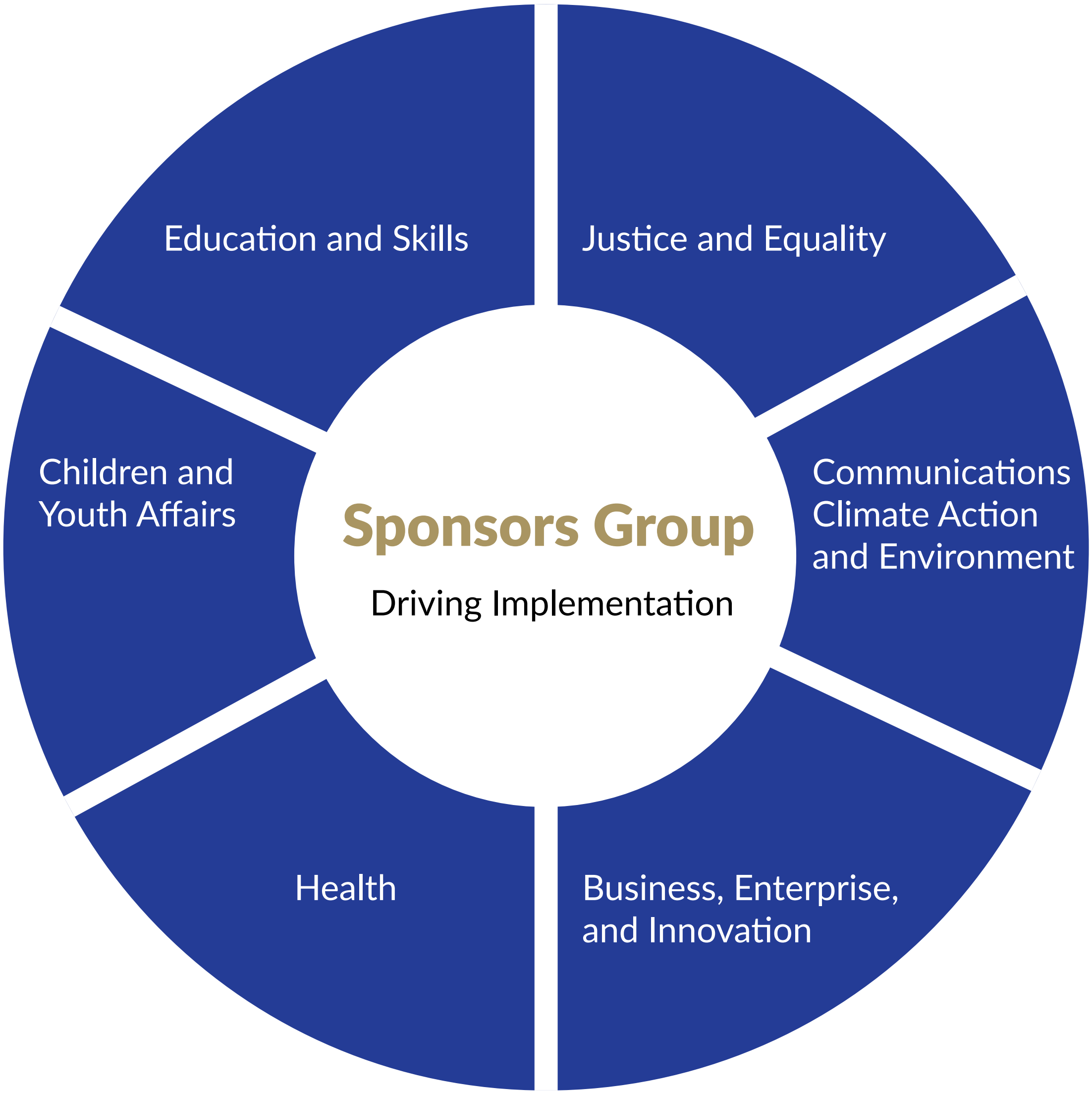
1. Create a single online access point on gov.ie through which all available Online Safety resources can be accessed
2. Review, consolidate and augment resources to support Online Safety
3. Equip teachers to embed digital awareness and digital citizenship in their practice
4. Encourage non users of the internet to develop computer and online skills through community based classes
5. Support enhanced curriculum development
6. Foster collaboration with parents
7. Support student participation in safer internet day activities and peer-to-peer initiatives
8. Develop online and telephone signposting tools and explore the provision of remote online supports for mental health
9. Develop awareness training to build resilience and peer support
10. In line with the EU better internet for kids strategy, we will promote best practice standards for quality content for children
11. Legislate for new criminal offences with the support of the Oireachtas
12. Ensure that Online Safety is specifically accounted for in statutory child safeguarding statements
13. Strengthen links and processes with industry for removing illegal and harmful material
14. Work with online platforms based in Ireland to advance Online Safety measures
15. Work with industry to develop a practical guide for online platforms and interactive services to support best practice in Online Safety in design
16. Work with EU and international partners to actively promote Online Safety
17. Revise the regulatory framework for on demand audio visual media services
18. Work with the Joint Oireachtas Committee in relation to the Digital Safety Commissioner Bill 2017
19. Publish an annual safer internet report
20. Establish a new National Advisory Council for Online Safety
21. Support the implementation of the Action Plan through consultation with Children and Young People
22. Ensure that offline and on-line responsibilities are aligned with effective whole of government coordination
23. Ensure political oversight of the implementation of this plan
24. Refocus the Office for Internet Safety
25. Ensure appropriate funding and resourcing targeted at Online Safety initiatives is in place

Expert Stakeholder input and advice

National Advisory Council for Online Safety

- Providing advice to Government on Online Safety policy issues
- Identify emerging issues
- Review national and international research
- Chaired by Minister of State
- Comprising expert stakeholders, including representatives of industry, academia, voluntary sector, children/young people, and parents

Whole of Government approach to implementation


Education and Skills
Justice and Equality
Children and Youth Affairs
Sponsors Group
Driving Implementation
Communications Climate Action and Environment
Health
Business, Enterprise, and Innovation

Introduction

Positive Impact of Online Engagement

It is now almost impossible to imagine a world without the internet or to imagine a future where the internet has less of a role in our lives than it does today.

It is important to acknowledge the positive effect the internet has on society. We can be connected with loved ones in an instant, no matter where they are in the world; businesses can access markets far greater than could be achieved through traditional means at far less cost; and students have a wealth of information and resources at their fingertips.

The Internet operates in a very dynamic environment in terms of speed of change and degree of innovation. Importantly, many of the issues arising are, by definition, new, international and common to many countries. It is challenging for Governments to be ahead of the curve in terms of responding to Online Safety challenges. Indeed, there are limits to what Ireland, or indeed any country, can achieve on its own.

Online Risks

There is wide variety in the types of content that give rise to concern. At one end of the spectrum there is serious criminal intent, such as child sexual abuse material or grooming of minors, and on the other there is the non criminal but nonetheless harmful content such as cyber bullying or websites that encourage or provide misinformation in relation to suicide or eating disorders.

Similarly, those responsible vary from criminals to ordinary users. Indeed, children can upload and disseminate content that is harmful or even illegal, in many cases unwittingly. The game changer in the use of the internet is the ubiquitous use of smart phones by all ages, but especially children and young people. We are only in the early stages of understanding how smartphone usage affects how and when we consume content and its impact.

Providing an effective response to Online Safety issues requires collaboration between many players including, among others, Government, parents, teachers, children, the EU and online platforms. An effective response also requires a joined up approach by Government Departments and Agencies which has not always been apparent to date. In essence, framing a response to Online Safety concerns involves acknowledging how online content is used and the dynamic and innovative nature of developing and using content including unfortunately, illegal and inappropriate content.

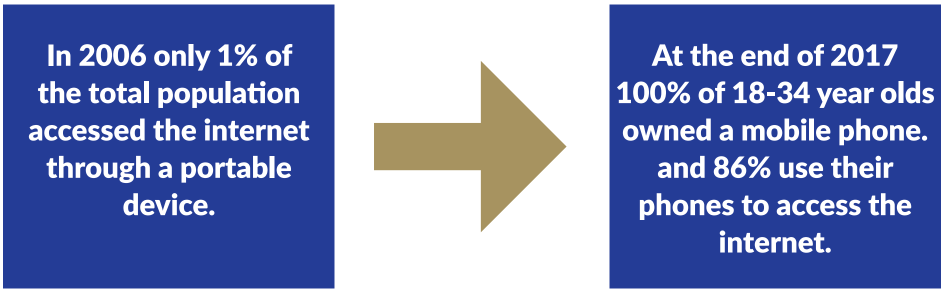
Adopting an overly prescriptive approach could mean that our response is out of sync with how content is evolving. Therefore, in order to be effective in meeting the needs of users, our response needs to encompass:

- Education, information and awareness raising
- EU and International law making

- Engaging with a diverse range of stakeholders

Our Online Safety content needs to be developed in a user friendly way so that it can be accessed and used in the same way as people engage with online content in their daily lives.

Internet and Smart Phone Usage in Numbers[1]



In 2006 only 1% of the total population accessed the internet through a portable device.

At the end of 2017 100% of 18-34 year olds owned a mobile phone. and 86% use their phones to access the internet.

The CSO estimates that in 2017[2]

- 81% of individuals used the internet in the previous 3 months
- 95% of individuals in the 16-29 years age group used the internet within the last 3 months, compared with 48% of individuals in the 60-74 years age category
- 96% of Students used the internet within the previous 3 months
- Close to nine and over of every ten households with dependent children used the internet within the last 3 months
- Seven out of every ten internet users used the internet every day
- Of the 16-29 years age category, 92% accessed the internet every day
- Mobile phones or smart phones were used to access the internet away from home or work by 87% of individuals in 2017, either via the mobile phone network and/or via the wireless network

[1] Internet and Smart Phone Usage in Numbers: https://www.comreg.ie/comreg-publishes-results-2017-ireland-communicates-survey/

[2] The CSO estimates that in 2017: https://www.cso.ie/en/releasesandpublications/er/isshh/informationsocietystatistics-households2017/

The Net Children Go Mobile Survey from 2015

found that **40%** of Irish

9-16 year olds

owned a smartphone, and that the smartphone was the device most used by this age group to access the internet.

This has undoubtedly increased in the intervening period.

A survey conducted by the National Anti Bullying

Research and Resource Centre in 2016 found

that over **50%** of children aged

6-8 years old have access

to a computer with internet

..over **25%** have access to the internet

on their own portable device

Open Policy Debate on Online Safety

This Action Plan was informed by the recent Open Policy Debate on Online Safety, which was hosted by the Minister for Communications, Climate Action and Environment in March 2018. The purpose of the Open Policy Debate was to raise awareness amongst participants of the activities being undertaken by Government, by the European Commission, by industry and by NGOs; and to get the views of participants on the issues they viewed as most important in this realm. A wide range of stakeholders were invited to this event, including a number of teenagers and young people, to contribute their views as to how best to promote safety online.

The discussions highlighted that participants main concerns were in the areas of education and awareness raising; cooperation and collaboration; structures; and legislation. This Action Plan addresses each of these themes, with clear, actionable, time-bound measures. The issues that emerged as being of particular concern included that no single person or organisation can sort these issues out on their own and that there is a need for strong partnerships and a more structured approach to the issue of Online Safety.

There was also a concern amongst participants in relation to the speed at which some online platforms take down offensive material and a view that industry could do more to protect users' data.

While a Digital Safety Commissioner was discussed, the emphasis of this discussion was on the proposed coordination and education aspects of the role, rather than that of regulation. It was acknowledged that some issues relating to potential regulation need to be addressed first at international level if they are to be meaningfully tackled.

Participants also expressed the view that it is important that children benefit from the positive aspects of the internet and rather than attempt to stop them using it we must instil in them the knowledge and tools to help keep them safe online.

Communication and education were also highlighted as being of particular importance. It was also noted that many people were unaware of the vast array of resources already available and a single point of access for all this information would be very helpful.
The actions outlined in this plan take steps towards addressing the issues raised by the participants of the Open Policy Debate.

Need for a Collaborative Approach

The range of risks found online requires our response to be nuanced and to take account of those differences. Law enforcement, legislation and regulation are important elements in addressing online risks - but they are only a part of our response.

This is the Government's first Action Plan on Online Safety which sets out in a coherent plan the actions that are being undertaken across Government Departments and agencies to protect children and adults in their online engagement.

The plan details the range of actions that will be progressed over the next 18 months.

To achieve what is outlined in this plan all relevant Government Departments will work together and with a range of stakeholders including industry, parents and children. Delineation of policy responsibility between Government Departments in relation to online issues operates on the basis that if a Department is responsible for a policy area offline, then it is responsible for the policy area online as well. As a result, a wide range of Government Departments have responsibility for the many strands of policy that are relevant to Online Safety. The Departments of - Communications, Climate Action and Environment; Justice and Equality; Education and Skills; Children and Youth Affairs; Health; and Business Enterprise and Innovation all have a policy role in relation to Online Safety.

In formulating this plan the Government considered a number of significant reports published in recent years, including the report of the Internet Content Governance Advisory Group (ICGAG) report[3], the Law Reform Commission's Report on Harmful Communications and Digital Safety[4], and more recently the Joint Oireachtas Committee on Children and Youth Affairs Report on Cyber Security for Children and Young Adults[5].

Ongoing Stakeholder Engagement

While Government has an important role, it alone cannot effectively address Online Safety issues. Industry, educators, parents, and children and young people must all play their part. That is why the Government is establishing a new National Advisory Council on Online Safety to ensure expert stakeholder input and advice. Membership of the Council will be broad based, and will be refreshed regularly to ensure the widest possible range of stakeholders can participate on the Council.

The Government is committed to regular and ongoing engagement with stakeholders, to providing appropriate information and supports to all users of the internet, and to fostering a positive digital citizenship for all.

Government will continue to work closely at international level, both through the European Union and globally, on coordinated initiatives that will make the internet a safer place.

[3] Internet Content Governance Advisory Group (ICGAG) report: https://www.dccae.gov.ie/en-ie/communications/publications/Documents/70/InternetContentGovernanceAdvisoryGroupReport.pdf

[4] Law Reform Commission's Report on Harmful Communications and Digital Safety : http://www.lawreform.ie/_fileupload/Final%20Report%20on%20Harmful%20Communications%20and%20Digital%20Safety%2021%20Sept%20PM.pdf

[5] Joint Oireachtas Committee on Children and Youth Affairs Report on Cyber Security for Children and Young Adults: https://data.oireachtas.ie/ie/oireachtas/committee/dail/32/joint_committee_on_children_and_youth_affairs/reports/2018/2018-03-29_report-on-cyber-security-for-children-and-young-adults_en.pdf

Goal 1:

Online Safety for All

Key Objective of Goal 1

Develop a single online access point where all advice, information and other resources for children and young people; parents and guardians; teachers; and the wider public can be accessed in a single place.

A concept that is central to Online Safety is that of digital citizenship, which focuses on themes of respect, education, and protection.

Children and young adults are generally considered to be able to use technology effectively and easily.

However, it is equally important to encourage and support children and adults alike to become digital citizens. A digital citizen acts appropriately and ethically in an online environment. They must be able to interact with others in a respectful, kind, open minded and responsible manner and act ethically at all times.

To be digitally literate one must be able to navigate, evaluate, and share and create content using all forms of digital devices, for example, smartphones, laptops and computers. Critical thinking, social, cultural, collaborative and technical skills are some of the skills that contribute to digital literacy.

The availability of high quality and up to date resources are vital to ensuring that anyone who interacts with the online environment can educate themselves and others on how to be a digital citizen.

Single Portal for all information and resources

A great many resources are currently available to children, parents, teachers and the general population about how to stay safe online. However, it is not always easy for people to find the information they are looking for, or indeed to know that the information exists in the first instance. Creating awareness of the existing supports was a recurring theme with participants of the Open Policy Debate on Online Safety, as was the desire for one “go-to” place for people to access all information and resources on the subject.

A single portal that is clearly signposted, linking to easy to understand materials, will make accessing the desired information and guidance easy and will empower people to become informed about their rights, responsibilities and the structure and supports in place should they need them.

Resources for children and young people

Usage of digital technologies is high among children. We must be able to allow children to enjoy and benefit from what the internet has to offer. We must also acknowledge that a determined child will find a way to go online with or without parental approval or supervision.

Those lacking sufficient levels of maturity and understanding may be particularly vulnerable to risks in the online digital environment. 44% of secondary school age children and 23% of primary school age children say they use the internet at home in their bedroom. While most children are aware of the importance of privacy settings 24% of secondary school age children don't use privacy settings, and 36% of primary school age children do not know how to keep their account private.[1]

> **The National Anti Bullying Research and Resource Centre Report on Cyberbullying in Ireland found that 29% of 13/14 year olds operate the computer without a parental filter**

We must ensure that our children are equipped with the knowledge and skills to avoid harm and, if harm comes their way, to feel that they can tell a parent or guardian.

A large number of resources on the safe use of the internet are already available to children and young people through a number of online platforms. These include articles and short videos and can cover topics to do with online platform policies, staying safe while online gaming, the effect of online platforms on our mental health, cyberbullying, and posts about the latest apps.

The Department of Children and Youth Affairs provides funding to three national youth organisations which provide online safety resources for the youth sector. The National Youth Council of Ireland provides the Web Safety in Youth Work Resource, SpunOut has developed an Online Safety hub which provides guidelines for young people on Online Safety and Youth Work Ireland, in conjunction with McAfee Security, has developed a digital safety programme which highlights the risks associated with online activity.

GDPR, which came into effect from 25 May 2018, grants significant data protection rights to all people in the European Union, but will provide particular protections to children. Article 8 of the GDPR imposes an obligation on providers of online goods and services offered to children to seek to obtain the consent or authorisation of a child's parent or guardian where the child is, in the case of Ireland, under the age of 16.

Webwise.ie, jointly funded by the Department of Education and Skills and the European Union, is another organisation that provides online safety information and resources targeting schools, teachers, parents and students.

[1] ISPCC, 2011. NCC Report: Children and the Internet. https://www.ispcc.ie/file/4/12_0/NCC+report+-+Children+and+the+Internet.pdf

Empowering Parents and Guardians

While primary responsibility for keeping children safe lies with parents and guardians, be that in the physical or the digital world, Government must ensure that the best possible resources and supports are available for them. This will empower parents and guardians to manage the range of safety settings across a variety of platforms; and to talk to their children about the risks they may face online and what they can do to avoid them. A recent survey conducted by the National Anti Bullying Research and Resource Centre, aiming to look at parents own knowledge and usage of the internet, found that only 8% of respondents believed a teacher or authorities should have the main responsibility for preventing dangers online.[2]

In an acknowledgment of the parent or guardians' vital role, in 2017, Webwise launched an online Parenting Hub to support forging the link between home and school. This Hub provides parents with practical advice and information to help address their concerns about the various issues facing their children on line. The new hub features expert advice from Child, Adolescent and Family Psychotherapists and offers useful conversation starters and tips on managing Online Safety in the home. It features advice on issues such as Chatstep, Snapmap, live streaming, sexting, social networking tips/online gaming; and cyberbullying.

Acknowledging that the popularity of apps and social networking sites can change quite rapidly Webwise continue to provide updated and relevant advice and supports for parents and guardians on the responsible use of the internet by their children.

Bridging the Digital Divide

The digital divide is the term used to describe the gap that exists between those who readily have access to the internet and those who do not, this is quite often older people and those living in more remote areas of the country.

The public library system, for example, helps to bridge the digital divide by developing digital learning centres, supporting non-users in introduction to and use of digital technology and offering STEAM (Science, Technology, Engineering, Arts and Maths) and coding workshops. It plays an increasingly important supporting role, showcasing new digital technologies and providing access to interactive digital technology and learning opportunities.

There is a growing practice within public libraries to extend the range and scope of activities and services supporting communities, repurposing libraries for creative activity and informal learning and ensuring that the public can become comfortable and confident with technology. Public libraries are developing creative community spaces leveraging technology to provide more personalised experiences for library users and their customized ways of learning. Examples of activities and services include- computer, internet, tablet and smart phone classes; digital touch-typing, reading and spelling courses

[2] O'Higgins, J and McGuire, L, 2016. Cyberbullying in Ireland: A Survey of Parents Internet Usage and Knowledge. ABC, National Anti Bullying Research and Resource Centre, Dublin City University

for children; and coding clubs.

The new public library strategy *Our Public Libraries 2022 – Inspiring, Connecting and Empowering Communities*, launched in June 2018, has a focus on targeted outreach initiatives for hard to reach individuals and groups in marginalised and disadvantaged communities as well as supporting accessibility, promoting learning and lifelong learning and digital technology use.

Digital learning centres in libraries can provide an environment for the community to come together to learn, work and create in an interactive, collaborative way. Equipped with the latest technologies, they can provide a space for users to experiment and innovate with 3D design, printing, web and graphic design, computer coding, circuit making and game design. Digital learning centres also offer a space for less confident users in the community to try out technology, explore its functions and become comfortable in its use.

Goal 1 - Online Safety for All

Actions	Constituent elements	Responsible Departments	Timeline
1. We will create a single online access point on gov.ie through which all available online safety resources can be accessed	1.1 We will create a single online access point on gov.ie signposting information on online safety and through which all available resources can be accessed targeted appropriately for different users – and updated regularly in light of emerging trends 1.2 Roll out a single brand associated with the new online platform 1.3 National communications campaign directed at all users, with key messages targeted at specific user groups. Including children and young people; parents and guardians	All departments through Sponsors Group	Q4 2018
2. We will review, consolidate and augment resources to support online safety	2.1 Develop Webwise - Youth Hub, in consultation with the youth panellists, and linked to the single online platform, which will act as a central point for representing the student voice in online safety. Features will include information on new and trending apps and advice on safe online communication. Safety and privacy; and data rights/ right to access/right to be forgotten	D/ES D/CYA D/JE	Q2 2019
	2.2 Review, consolidate resources and content for parents and guardians and address gaps including helping to: Develop resources for parents of pre-school age children Develop guidance on appropriate amounts of 'screentime' for each age group	D/ES D/CYA	Q4 2018
	2.3 Review and consolidate resources and content for teachers	D/ES	Q4 2018
	2.4 Continue to forge the link between home and school through the ongoing review and update of supports for parents through the Webwise parenting hub	D/ES	Q4 2018
3. Equip teachers to embed digital awareness and digital citizenship in their practice	3.1 Highlight the need for online safety and raise the awareness for webwise amongst teachers.	D/ES	Q3 2018
	3.2 Engage with the Teaching Council to identify opportunities to integrate enhanced digital literacy in droichead, the induction framework for new teachers, and cosán, the national framework for teachers training	D/ES	01 2019
	3.3 Make a discrete online safety module available to primary and post primary teachers to support their continued professional development	D/ES	Q3 2019
4. We will encourage non users of the internet to develop computer and online skills through community based classes	4.1 Through our public libraries 2018-2022 we will develop digital learning centres in suitable libraries, and provide users with access to training in the latest technologies helping people to stay safe online	D/RCD	Q4 2019

Goal 2:

Better Supports

Key Objectives of Goal 2

- Improved digital citizenship through schools
- Improved online links to mental health supports and services

The Role of Schools in Online Safety

The safety and welfare of children is a complex and challenging concern for policy makers, Government, parents and society in general. Internet and Online Safety presents a particular challenge and schools have a significant contribution to make. However, Online Safety does not lie solely within a schools remit. Key messages on Online Safety must be embedded across the whole of Government policy.

The overall operation of the individual school is the responsibility of its Board of Management which includes representatives of the wider community including parents. It is a matter for each Board to ensure that it has appropriate policies in place to safeguard the overall safety and wellbeing of students. All schools are required to have a range of policies in place including policies on the safe and ethical use of technologies, anti-bullying and a code of behaviour. The Board is also responsible for ensuring that the curriculum meets the academic as well as developmental needs of its students.

The Department of Education and Skills supports schools through the prescription of school curriculum that supports overall student learning and in particular, supports the development by students of the skills and competencies necessary to negotiate living in the 21st century which includes being safe using online technologies. There are extensive training and curricular supports and resources available to assist schools in the development of policies and practices on the safe use of the internet and on the prevention of bullying and harassment using the internet.

The *Digital Strategy for Schools 2015-2020* links with other Departments and agencies and outlines a vision for the use of digital technologies in teaching and learning. There are specific actions in the Strategy that relate to the promotion of the safe and ethical use of technology in schools.

Supporting Teachers

Student wellbeing and safety are an integral part of teacher education programmes covering initial teacher education through to induction and career long continuing professional development.

Online Safety is a concern for all teachers and all teachers should be aware of the importance of Online Safety and that it should feature in classroom activity as part of teaching and learning. The Department of Education and Skills, through the Professional Development Service for Teachers and its Technology in Education team, has a dedicated team to support teachers and schools on the safe and ethical use of technologies for teaching, learning and assessment.

Online Safety Education will be a key component of Summer Courses, term time, face –to-face and online CPD provision which will be delivered by the PDST (Technology in Education) Team in 2018 and 2019.

In addition, the Teaching Council, in its review of the standards for Initial Teacher Education (ITE), will have a particular focus on the need to support student teachers as responsible digital citizens, including fostering a deeper understanding of the ethical creation, use and dissemination of information.

A *Digital Learning Framework* for primary and post primary, developed by the Department of Education and Skills, is a key support for schools for the embedding of digital technologies in teaching and learning.

In implementing the *Digital Learning Framework*, schools and teachers are given a structure which will allow them to identify where they are on the journey towards embedding digital technologies in teaching, learning and assessment, and enable them to progress in that journey. The implementation of the Framework is being trialled across 30 primary and 20 post primary schools and the outcome of this trial will inform the national roll out of the Framework in September 2018.

Online Safety Programme for Primary and Post Primary

Both Primary and Post Primary Schools currently provide formalised education on Online Safety. The Department of Education and Skills provides for Online Safety through a range of programmes, including the formal curriculum content, teacher professional development, strategies around wellbeing, bullying and the use of innovative materials. This approach is considered preferable to that of a stand-alone programme.

The curriculum provides students with the opportunity to develop the skills and competence to learn about themselves, to take care of themselves and others and to make informed decisions about their health, personal lives and social development.

The National Council for Curriculum Assessment (NCCA) conducted a consultation on the future structure and content of the primary school curriculum. The findings from this consultation will be used to map the direction for future work on the redevelopment of the primary school curriculum and matters relating to Online Safety and digital literacy will be considered as part of this.

Stay Safe, a mandatory personal safety skills programme in primary school includes specific lessons on meeting and responding to strangers online including through gaming, cyberbullying, how to stop/block/tell, effects of cyberbullying, rules for Online Safety, setting profiles to private and preventing online grooming.

Social Personal Health Education (SPHE) which is mandatory subject at primary level and up to junior cycle in post-primary schools includes a module on Relationship and Sexuality Education (RSE). SPHE is taught in an age appropriate holistic manner and deals with respectful communication, friendships, relationships, personal safety and influences and decisions.

In May 2018, the Minister for Education and Skills published a circular requiring All schools to consult parents, teachers and students on the use of smart phones and tablet devices in schools. The Minister also reiterated his commitment that the use of smart phones in schools will be included as an item requiring consultation under the Education (Parent and Student Charter) Bill 2016, a new law which will require every school to consult with parents and students on key issues and publish and operate a Parent and Student Charter in line with national statutory guidelines.

Webwise Initiative

Webwise is the Professional Development Services for Teachers (PDST) Technology in Education Online Safety initiative.

It is part of the wider *Safer Internet Ireland Project* which is co-ordinated by the Office for Internet Safety, an executive office of the Department of Justice and Equality. The Safer Internet Ireland Project is a consortium of industry, education, child welfare and government partners that act as a Safer Internet Centre in Ireland providing awareness, hotline and helpline functions. It develops national initiatives promoting the safer use of electronic media and enhances protection of the vulnerable, particularly children, against the risks associated with use of the internet.

Webwise promotes the autonomous, effective, and safer use of the internet by young people through a sustained information and awareness strategy targeting school principals, teachers, parents and children with consistent and relevant messages.

The PDST Technology in Education Team develops and disseminates resources that help teachers integrate internet safety into teaching and learning in their schools. With the help of the Webwise Youth Advisory Panel it also develop student/youth oriented awareness raising resources and campaigns that address topics such as social networking, sexting, and cyber bullying.

Webwise.ie was re-developed in 2017. In October 2017, ahead of the redevelopment, Webwise surveyed website users –principals, teachers, parents, and Department support services - on ways to improve the website. Following this consultation the website was fully redeveloped to ensure the user experience was optimised for all of the target audiences.

In the next phase of redevelopment Webwise will establish a Youth Hub, which will act as a central point for representing the student voice in Online Safety. Webwise will consult with young people on the development of the Hub which will feature peer created articles and information on new and trending apps.

Involving Parents in Review of School Policies on Safe and Responsible Internet Usage

All schools are advised to have an Acceptable Use Policy (AUP) in place, An AUP policy is a document which addresses all rights, privileges, responsibilities and sanctions associated with internet use in schools. It is usually drawn up by teachers and management in consultation with parents and students and incorporated into the school's overall ICT policy. Ideally every school will devise an AUP before it is involved in any use of the internet and will seek Board of Management endorsement.

An AUP can deal with many topics like setting out guidelines for the proper use of internet searches, downloads, browsing, the use of email, phones, tablets and online games.

All schools are also required to have in place a code of behaviour, an anti-bullying policy and policies relating to the safe and ethical use of digital technologies. All schools are also obliged to comply with Child Protection legislation, which includes internet safety, and have a Child Safeguarding Statement in place.

A school wide approach to digital safety, rather than designating specific members of the teaching staff as ambassadors, is advisable.

Safer Internet Day

Safer Internet Day is an EU wide initiative to promote a safer internet for all users, especially young people and is celebrated in February each year. It is promoted in Ireland by Webwise, developed by the Professional Development Service for Teachers (PDST) and other participants, and aims to educate and raise awareness about protecting children online, so that they can responsibly enjoy the benefits of the Internet, without compromising their safety and privacy. Over 102,000 students celebrated Safer Internet Day across Ireland in 2018

Peer to Peer Workshops

An important aspect of anti-bullying prevention and Online Safety in schools is the active involvement of students in building a positive school climate.

The Department of Education and Skills supports the use of a range of pedagogical approaches that encourage students to be self-reflective and autonomous in the learning process. This includes the use of peer learning and teaching by students where appropriate, under the guidance and supervision of teachers.

Due to the range of sensitive issues that could come up during any workshop on Online Safety any peer-to-peer workshops, potentially delivered by students, would have to be within the context of the schools own policy on the delivery of the SPHE curriculum and RSE programme with due regard to the School's Child Protection Procedures and its Child Safeguarding Statement.

A limited peer led programme, the Safer Internet Day Ambassador Programme, is facilitated under Webwise.ie to promote Safer Internet Day. As a part of Safer Internet Day 2018, Webwise encouraged and supported post-primary students to address the issue of cyberbullying and Online Safety by leading awareness raising campaigns in their clubs, schools, and communities. Ambassadors receive free online and offline training from the Webwise team and members of ISSU (Irish Second-Level Students Union) develop teamwork and communication skills and learn about leadership.

Mental Health Supports

Many studies have been conducted on the impact technology and the internet can have on our mental health. Witnessing harmful content online; experiencing an unpleasant interaction over social media or through an app; or merely spending too much time inactive and staring at a computer screen are just a few of the risks the internet can pose to our mental health. However, it also provides an opportunity to help people. A policy report on suicide prevention, published by Bristol University in 2016, found that while the internet is often used by people who self harm and/or attempt suicide the internet is also used as a forum for seeking help.[1]

> **A clinical sample conducted by the University of Bristol found that 8% of patients who presented to hospital following a suicide attempt had used the internet in connection with their attempt**

The National Youth Mental Health Task Force concluded that use of digital technologies

[1] Biddle et al., 2016, Priorities for suicide prevention: balancing the risks and opportunities of internet use. Bristol-University, Policy Bristol

can play an important role in the delivery of mental health supports to children and young people. Innovative, digital technologies are well placed to support children and young people when and where they need it.

Work in this area is further informed by good practice guidelines for the safe delivery of online mental health information and support commissioned by the National Office for Suicide Prevention in 2015.

Several initiatives in the Department of Health focus on improving digital literacy and availing of digital supports that build mental resilience and education. Healthy Ireland engages with various Government Departments and supports their work to create awareness and training about cyber bullying.

Goal 2 - Better Supports

Actions	Constituent elements	Responsible Departments	Timeline
5. Curriculum Development	5.1 Publish a digital media literacy interactive resource for primary level 5.2 Online safety will be a key component of the national seminars planned for the dissemination of the digital learning frame work for schools which will commence from Q4 2018	D/ES D/ES	Q1 2019 Q4 2018
6. Collaboration with parents	6.1 Schools will be required to consult with parents, students, and teachers on if and how smart phones and other tablet devices should be used in schools 6.2 Provide funding to the national parents council for the provision of 65 training sessions on anti-bullying, including cyberbullying 6.3 Develop and publish a resource on Webwise.ie for use by primary and post-primary schools to deliver internet safety awareness evenings to parents.	D/ES D/ES D/ES	Q2 2018 Q4 2018 Q3 2018
7. Support student participation in safer internet day activities and peer-to-peer initiatives	7.1 Support safer internet day 2019, including by: • Promoting the safer internet day ambassador programme • Increasing participation in the programme by a minimum of 20% • Targeting over 110,000 students for safer internet day 2019; and • Launching a safer internet day awards programme.	D/ES	01 2019
8. We will develop online and telephone signposting tools and explore the provision of remote online supports for mental health.	8.1 Develop an online signposting tools for mental health supports 8.2 Support the establishment of a single point of telephone contact for HSE mental health services information. 8.3 Explore the provision of additional online supports for people with mental health concerns and will; • Examine the feasibility of hosting online therapeutic interventions; • Create a pilot mental health hub in a primary care centre to provide remote online counselling services. 8.4 Develop advertising and media strategies for a digital health support suite.	D/Health D/Health D/Health D/Health	Q3 2018 Q3 2018 Q4 2018 Q1 2019
9. Develop awareness training to build resilience and peer support	9.1 Develop website content that will focus on resilience building and peer support training.	D/Health D/CYA	Q4 2018
10. In line with the EU better internet for kids strategy, we will promote best practice standards for quality content for children	10.1 Consider ways to promote positive online content for children.	Sponsors Group	Q1 2019

Goal 3:

Stronger Protections

Key Objectives of Goal 3

- Legislate for new criminal offences
- Build up means of capturing and responding to harmful and illegal content
- Improved industry responses

Access to the internet is now available through a wide range of devices, including tablets, smart phones, and games consoles. No longer is internet access restricted to use of the family computer.

Risks that can be encountered include the patently illegal such as predatory behaviour, online grooming, and child exploitation; hate speech and illegal content, the dissemination of child sexual abuse material and fraudulent practices.

> **A survey conducted by the ISPCC and completed by 18,116 children and young people found that 16% (over 2,000) of young people had met up with someone from online.[1]**

However, risks also include the impact on children, young people and vulnerable adults of access to harmful content, for example pornography; the inappropriate portrayal of suicide; misinformation on diet and eating disorders; cyber bullying; and mental health impacts of harmful online activity.

These risks prove more challenging to address, and requires a multi-stakeholder approach including the whole of Government through the new Sponsors Group, NGOs, Industry, and others. It also requires an EU wide approach involving collaboration of member states and a wider global approach

Legislation and Regulation

Address criminality and gaps in current legislation

A serious challenge in addressing Online Safety is ensuring an up to date legal framework is in place that will be fit for purpose in the medium to long term, in an area that is developing and progressing at such speed. We must recognise that it is not possible to legislate in a manner that predicts the evolution of technology and consumer behaviour, but there are certain steps that can be taken.

The Law Reform Commission (LRC) undertook a review of the law on cyber-crime affecting personal safety, privacy and reputation and in September 2016, it published its report on Harmful Communications and Digital Safety.

[1] ISPCC, 2011. NCC Report: Children and the Internet. https://www.ispcc.ie/file/4/12_0/NCC+report+-+Children+and+the+Internet.pdf

The Report acknowledges that the revolution in telecoms and digital media has brought enormous positive benefits, allowing people to participate in a civic society and in public discourse. However, this freedom brings with it new and emerging challenges, including the use of the internet as a medium to cause significant harm to others.

The Report recognises that both criminal law and civil remedies are important in tackling this issue and includes proposals for reforming the criminal law on harmful communications and addressing gaps in the current legislation

The Law Reform Commission's Report makes recommendations on creating a number of new criminal offences that relate to - harassment online or through digital communication; stalking; the non-consensual distribution of intimate images with intent to cause harm; and the taking and distribution of intimate images without consent. It also recommends that the existing offence of sending threatening or indecent messages should be extended to apply to all online communications.

Legislation to address these recommendations was in development in the Department of Justice and Equality. However, the Government has accepted a Labour Party Private Member's Bill aimed at progressing these issues, along broadly similar lines to the legislation that was in the course of being drafted. The Harassment, Harmful Communications and Related Offences Bill completed second stage in the Dáil in January 2018 and was not opposed by Government. The Minister for Justice and Equality will work with the Labour Party to ensure that this Bill is enacted.

Online Child Sexual Abuse Material and Child Sexual Exploitation

A number of measures exist that combat sexual abuse and sexual exploitation of children and child sexual abuse material including legislation, operations carried out by An Garda Síochána and actions supported by industry.

The primary legislation is the Child Trafficking and Pornography Act 1998, which provided for offences relating to the possession, distribution and production of child abuse material. The legislation was further strengthened by the Criminal Law (Human Trafficking) Act 2008 and the Criminal Justice (Withholding of Information on Offences against Children and Vulnerable Persons) Act 2012.

The Criminal Law (Sexual Offences) Act 2017 made provision for the offence of child grooming. It introduced new offences targeting, in particular, the use of information and communication technology to facilitate the sexual exploitation of a child and those controlling or directing the activities of a child for the purposes of prostitution or pornography. The Act also introduced additional grooming offences, such as causing children to watch sexual activity, as well as strengthening existing offences targeting those who would travel to meet a child for the purpose of sexually exploiting that child and creates new offences of exposure and offensive conduct of a sexual nature.

A valuable resource is Hotline.ie, an anonymous facility for Internet users to report suspected illegal content, particularly Child Sexual Abuse Material, accidentally encountered online. Information is received through the line in a secure and confidential way. It is run and funded by the Internet Service Providers Association of Ireland (ISPAI) and is co-financed by the European Union's Connecting Europe Facility.

The hotline works closely with the ISPs and Gardaí in relation to "a Notice and Takedown" of illegal content and it is overseen and compliance monitored by the Department of Justice and Equality. The member companies of the ISPAI agree to operate the Notice and Takedown procedure.

'Operation Ketch' is an ongoing operation targeting those in possession and involved in the distribution of Child Exploitation Material (child sexual abuse material) either through online platforms or via File Sharing Networks. Assistance was received by the Online Child Exploitation Unit from the Federal Bureau of Investigation (FBI) and National Centre for Missing and Exploited Children (NCMEC) in the USA, and the National Child Exploitation Coordination Centre (NCECC) in Canada in the targeting of suspects.

The objective of the operation was to identify Child Protection concerns at each address and engage with Túsla; to identify, target and search persons suspected of distributing online Child Exploitation Material; and to send out a message to other persons who are distributing this material that An Garda Síochána will actively identify and pursue them.

Garda Inspectorate Report "Responding to Child Sexual Abuse - A Follow-Up Review"

The Garda Inspectorate Report *"Responding to Child Sexual Abuse - A Follow-Up Review"* directly relates to a previous Inspectorate report on the investigation of child sexual abuse published in 2012. Since the initial report there has been a considerable increase in the risk to child safety posed by the internet and online platforms.

Child sexual abuse is one of the most serious types of crime for the Garda Síochána to deal with and this report is a comprehensive examination of Garda Síochána practices and procedures in handling this important issue. In this regard, Chapter 4 of the Inspectorate's Report deals exclusively with issues of Online Child Sexual Abuse (CSA) and Child Sexual Exploitation (CSE). Several actions are recommended for An Garda Síochána and partner agencies in terms of its assessment and operational response to the threat of online CSA and CSE.

Processes are in place at the Garda National Protective Services Bureau to monitor, investigate and detect online abuse. Procedures are also in place in the Online Child Exploitation (OnCE) Unit to, inter alia, investigate and co-ordinate cases relating to the possession, distribution and production of child pornography, and to proactively investigate intelligence concerning paedophiles and their use of technology and the online targeting of suspects for the production, distribution and possession of child abuse images on the internet. The development of Standard Operating Procedures relating to these processes and procedures is under consideration by the Garda Síochána.

The Government has established an independently-chaired, inter-agency Implementation Group to appraise and develop a whole of Government response to the Inspectorate Report.

Child Safeguarding Statement

The Children First Act 2015 is predicated on the clear principle that child protection issues are the responsibility of all organisations and Departments in their respective sectors, and that they must be embedded in the policy considerations of all Departments.

The Children First Act 2015 was enacted in November 2015, and commenced on a phased basis, with all provisions commenced by 11 December 2017. The Act sets out a range of obligations for individuals and organisations in relation to child protection. This includes mandated reporting of child abuse and the publication of Child Safeguarding Statements by providers of relevant services.

Garda Síochána and Industry Collaboration

Hotline

A valuable resource is Hotline.ie, an anonymous facility for Internet users to report suspected illegal content, particularly Child Sexual Abuse Material, accidentally encountered online. Information is received through the line in a secure and confidential way. It is run and funded by the Internet Service Providers Association of Ireland (ISPAI) and is co-financed by the European Union's Connecting Europe Facility.

The hotline works closely with the ISPs and Gardaí in relation to "a Notice and Takedown" of illegal content and it is overseen and compliance monitored by the Department of Justice and Equality. The member companies of the ISPAI agree to operate the Notice and Takedown procedure.

Memorandum of Understanding with Internet Service Providers

The Garda blocking initiative was launched in November 2014. Under the terms of a Memorandum of Understanding (MOU), a large internet service provider (ISP) company has agreed to block access to child abuse material on its network in accordance with a list provided by An Garda Síochána. If a user accesses child sexual abuse material, whether deliberately or mistakenly, access will be blocked and an advisory message will be displayed outlining the reasons why.

An Garda Síochána is actively engaged with a number of Internet Service Providers (ISPs) on them putting in place a similar MOU. Such discussions can take time because each ISP has unique and significant technical and resource issues to resolve before putting blocking in place on their system.

Improved Industry Responses

Role of Industry

Ireland is home to offices of some of the biggest technology companies in the world including Apple, Facebook, Twitter, LinkedIn, and Oath (formerly Yahoo!). A great deal of work is already being done by these and many other companies, to keep people safe online.

All the major online platforms provide tools and resources for all users to assist them in staying safe while using their platforms, including tools for the reporting of inappropriate content and advanced privacy settings.

In addition, Facebook and Google contribute to addressing illegal content by providing the US National Center for Missing and Exploited Children with information that is then passed on to An Garda Síochána.

While collaboration exists between An Garda Síochána and industry on illegal content, industry may need to go further in relation to harmful content.

Recently, there have been increased concerns regarding the wellbeing and safety effects of online platforms and internet use in general. Inappropriate media reporting and online platforms use was identified as a risk factor in Connecting for Life - Ireland's National Strategy to Reduce Suicide 2015-2020. The internet is now a leading source of information about suicide and contains readily accessible sites that can be inappropriate in their portrayal of suicide. Internet sites and online platforms have been implicated in both inciting and facilitating suicidal behaviour.

There is concern amongst users as to what action is taken by companies when harmful or illegal content is reported. There is a need to 'close the loop' and inform users of outcomes. Steps are being taken already in this area - Google and YouTube, for example, are introducing transparency reports in relation to what happens to flagged material.

Recent events and the introduction of GDPR have also made users more aware of how their personal data is stored and used and their data protection rights. There is provision in the GDPR for a right to access and a right to be forgotten. Furthermore Section 33 of the Data Protection Act 2018 provides for a specific "right-to-be-forgotten" for children. This section strengthens the rights of children to erasure of any data collected during the provision to them of information society services. Data controllers, for example online platforms, are required to provide users with a copy of their processed personal data upon request and users can request the erasure of personal data concerning him or her.

Voluntary Codes of Practice

Currently in Ireland the members of the Internet Service Providers Association of Ireland – which includes leading internet service providers - operate under a self-regulatory format in relation to illegal content on the Internet.

The ISPAI Code of Practice and Ethics outlines the self-regulatory environment to which the ISPAI members have committed themselves. The Department of Justice and Equality has primary oversight responsibility in respect to reviewing and ensuring the appropriate operation of the Code and the wider self-regulatory system. Currently there are 23 internet service providers signed up to the code. It is estimated by the ISPAI that between them, they represent 90% of the market.

A voluntary Code of Conduct was agreed by the European Commission with leading internet companies to combat the spread of illegal hate speech on their services so they can remove or disable access to such content. The third evaluation of the Code of Conduct carried out by NGOs and public bodies shows that IT companies removed on average 70% of illegal hate speech notified to them.

Structured engagement with Online Platforms

It is clear from the recent evaluation of the voluntary Code of Conduct on Illegal Online Hate Speech that self-regulation can be successful. The positive developments made by some companies in relation to greater transparency also shows that the online platforms listen to their users and are willing to change practices.

The technology and how we engage with it is constantly evolving. It is therefore paramount that we work together with industry to find ways to constantly improve and strengthen safety for all users.

Safety must be built into the design of any new app; learning and best practice needs to be shared with smaller, less well resourced companies; and improvements on transparency need to be made.

Goal 3 - Stronger Protections			
Actions	**Constituent elements**	**Responsible Departments**	**Timeline**
11. We will legislate for new criminal offences with the support of the Oireachtas	11.1 We will assist with Private Members legislation for new criminal offences of harassment online or through digital communication; stalking; the non-consensual distribution of intimate images with intent to cause harm; and the taking and distribution of intimate images without consent as recommended by the law reform commission in its report on harmful communications and digital safety.	D/JE	Q2 2019
12. We will ensure that on-line safety is specifically accounted for in statutory child safeguarding statements	12.1 We will include a specific reference to the need to consider online safety in the template for the completion of the child safeguarding statement; and	D/CYA	Q3 2018
	12.2 We will amend the Children First guidance to include a specific reference to the need to consider online safety in the context of completing the child safeguarding statement	D/CYA	Q2 2019
13. We will strengthen links and processes with industry for removing illegal and harmful material	13.1 We will review with the Internet Service Providers Association of Ireland the Code of Practice and Ethics for their internet service provider member companies with a view to enhancing measures to support improved cooperation between hotline.ie and industry for taking down child abuse and other illegal material.	D/JE	Q1 2019
	13.2 Increase ISP sign up to the code of practice and ethics from 90% to 95% of the market	D/JE	Q3 2019
	13.3 We will engage with providers to extend the Garda blocking initiative to those providers with the largest share of the market	D/JE	Q2 2019
	13.4 The inter-agency implementation group will undertake and complete its appraisal of the Garda Inspectorate's recommendations in its report "responding to child sexual abuse - a follow-up review" with particular reference to those concerning online child sexual abuse and child sexual exploitation	D/JE	Q2 2019
	13.5 We will explore the feasibility of proactively engaging in searches for images and videos of child sexual abuse material online	D/JE	Q2 2019
14. We will work with online platforms based in Ireland to advance online safety measures	14.1 We will establish a process of structured engagement by Departments with online platforms, including to: • Improve and update child online safety mechanisms; and • Encourage platforms to monitor where, when and how children might encounter potentially harmful advertising messages; • Encourage best practice in reporting around self harm behaviour.	D/CCAE D/BEI D/HEALTH D/ES D/JE D/CYA	Q3 2018
	14.2 We will work with industry to publish regular transparency reports in relation to illegal and harmful content	D/CCAE D/JE	Q1 2019
15. We will work with industry to develop a practical guide for online platforms and interactive services to support best practice in online safety in design	15.1 We will work with industry to produce a practical guide for online platforms and interactive services, similar to that produced by UKCCIS, to encourage a standardised approach to best practice in online safety at all stages of design, development and roll out.	D/CCAE	Q4 2018

Goal 4:

Influencing Policy

Key Objectives of Goal 4

- Work with the European Union and International Partners in respect of improved policy, legislation and regulation
- Develop national regulatory and policy responses
- Strengthen national protective measures

While Government can enact legislation on Online Safety, and indeed is doing so, the reality is that many companies will not be subject to these laws if they are not based in Ireland.

Online Safety is a transnational concern and we must work together with our counterparts both in the European Union and globally to advance certain aspects of improving Online Safety.

European Union

A great deal of progress has been made at European Union level in the area of Online Safety. Measures have been taken in recent years to tackle illegal hate speech and counter terrorism online; and to ensure a safer, better internet for children.

In Ireland, actions relating to the European Strategy for a Better Internet for Children, which aim to provide children with the digital skills and tools needed to fully and safely benefit from being online, have been addressed in a number of separate national policies including Better Outcomes, Brighter Futures and the Action Plan on Bullying.

In 2016, the European Commission agreed a voluntary Code of Conduct with the leading internet companies to combat the spread of illegal hate speech online in Europe.

The Ministerial level EU Internet Forum, launched in 2015, brings together EU Member States, Europol, EU experts and key internet companies to progress joint efforts with the private sector to reduce the online accessibility of terrorism-related material and to better develop counter narratives to combat violent radicalisation.

The interaction at EU level with the internet companies has taken place on the basis of partnership. Significant work has been done by the tech companies, especially with the establishment by Facebook, Google and Twitter of the 'Database of Hashes' to digitally identify known terrorist content with a view to improving takedown and reducing further dissemination. The companies also provide updates to the Forum on their ongoing work in developing automated means of identifying and blocking terrorist content.

The European Commission has indicated its intention to monitor the progress made by the online platforms in the months ahead and to assess whether additional measures are needed, to ensure the swift and proactive detection and removal of illegal content online, including possible legislative measures. This is an issue that Ireland will explore further with our fellow EU members.

The E-Commerce Directive 2000 provides a framework for electronic commerce that provides legal certainty for business and consumers alike. It establishes harmonised rules on issues such as the transparency and information requirements for online and intermediary service providers.

The proper functioning of the Internal Market in electronic commerce is ensured by the Internal Market clause. This means that information society services, for example online platforms, are, in principle, subject to the law of the Member State in which they are established. In turn, the Member State in which the information society service is received cannot restrict incoming services.

Over the past number of years, the main E-Commerce involvement has been in relation to the liability exemptions of intermediaries otherwise known as Internet Service Providers. Articles 12-14 in the Directive provide defences to Internet Service Providers (ISPs) who transmit digital content by electronic means, i.e. the Internet. Article 13 of the Directive concerns the concept of a ‘safe harbour’ relating to the legal responsibility of ISPs for illegal content and the issue of notices of such and the take down of such material. ISPs are generally considered to be ‘mere conduits’ with a voluntary code existing as to when they become aware of such illegal content.

The present liability regime for ISPs, as set out in the Directive, was designed at a time when online platforms did not have the characteristics and scale they have today. The harmonisation of the exemption of certain types of online platforms from liability for illegal content and activities, in respect of which they have neither control nor knowledge, now necessitates the consideration of whether further action at EU level may be appropriate. Legislation requiring companies to take down content when directed would be ineffective at this time, as this requirement would not be enforceable in relation to companies based outside of Ireland.

On 28 September 2017 the European Commission adopted a Communication with guidance on the responsibilities of online service providers in respect of illegal content online. The Recommendation on measures to effectively tackle illegal content online, published on 1 March 2018, further outlines approaches that can be progressed.

At the end of April the European Commission published a Communication on “Tackling online disinformation: a European approach” which sets out the views of the Commission on the challenges associated with disinformation online. The Communication outlines the key overarching principles and objectives which should guide actions to raise public awareness about disinformation and tackle the phenomenon effectively, as well as the specific measures which the Commission intends to take in this regard.

The Communication was developed taking into account extensive consultations with the public and stakeholders, including a High-Level Expert Group which reported on 12 March 2018. The Commission also launched a broad public consultation process, comprising online questionnaires that received 2,986 replies, structured dialogues with relevant stakeholders, and a Eurobarometer opinion poll covering all 28 Member States.

Regulation of on-demand services

The EU's Audiovisual Media Services Directive (AVMSD) governs EU-wide coordination of national legislation on all audiovisual media; both traditional TV broadcasts and on-demand services. The AVMSD is currently being revised and it is likely that Member States will have two years in which to implement the revised Directive from Q4 2018.

Two parts of the revision are of particular relevance to Online Safety. The first part will require the Department to formalise the position of On-Demand regulation in Ireland. The second and most significant aspect of the revision from an Online Safety perspective is the extension of the scope of the Directive to include video-sharing platform services (VSPS), and to introduce, by co-regulation, targeted and limited obligations on VSPS, including specified measures to protect minors from potentially harmful content and all audiences from hate speech.

In effect, this will mean that a National Regulatory Authority will be required to examine and deem adequate the measures which a VSPS has in place to protect minors from potentially harmful content.

The definition of what is and isn't a VSPS is still unclear, but as an example – services such as YouTube, and aspects of Facebook's service are likely to fall within the scope of the Directive. These measures will only apply to the video aspects of these services, and not for example the user comments underneath the videos.

The Department of Communications, Climate Action and Environment is currently conducting an initial engagement with key stakeholders, including Google, Facebook, Twitter, Apple and Oath (formerly Yahoo!) in preparation for a formal public consultation period once the final text has been adopted.

Other International Initiatives

The extremely serious issue of child sexual exploitation online is one that no country can tackle on its own. Modern technology allows criminals to move images and videos quickly between jurisdictions, exploiting legal loopholes and providing a sense of anonymity.

The WePROTECT Global Alliance to End Child Sexual Exploitation Online combines two major initiatives: the Global Alliance, led by the U.S. Department of Justice and Equality and the EU Commission and WePROTECT, which was convened by the UK. The two initiatives were merged in 2015 to create a single global initiative dedicated to national and global action to end the sexual exploitation of children online. It gathers the influence, resources and expertise necessary to transform how this crime is dealt with worldwide.

Ireland joined the WePROTECT Global Alliance in 2016. We are one of 70 countries working towards a coordinated national response to online child sexual exploitation with a common set of aims, which include - to identify victims, and ensure they receive necessary support; investigate cases of exploitation; prosecute offenders and ensure their effective management; increase public awareness and empowerment of children and young people to protect themselves online, and; engaging with industry in developing solutions to prevent and tackle child sexual exploitation and abuse online.

Digital Safety Commissioner

Many stakeholders have called for the establishment of a Digital Safety Commissioner.

The Law Reform Commission, in its 2016 Report on Harmful Communications and Digital Safety, recommended that the Office would have two core functions.

- Its first function would be an educational one, whereby it would be responsible for promoting and disseminating information in relation to Online Safety; co-ordinating the activities of Government Departments; conducting research on Online Safety; and developing guidance materials for schools on digital safety.
- Its second function would involve enforcing a system of 'notice and take down' of harmful digital communications by digital service undertakings, including the development of a code of practice on take down procedures.

A Private Members Bill, the Digital Safety Commissioner Bill 2017, introduced to the Dáil in November 2017, has been informed by the Law Reform Commission's report. There are aspects of the Bill which raise jurisdictional and other legal issues and with require greater examination and scrutiny.

While work on the bill is progressing we will continue to implement actions that address many of the same objectives proposed for a Digital Safety Commissioner.

The proposed functions in relation to education are being comprehensively addressed by this Action Plan through the development of the single online access point; the roll out of a national communications campaign; the establishment of the Sponsors Group which will coordinate a whole of Government approach to Online Safety; and the establishment of the National Advisory Council on Online Safety which will examine research in relation to

Online Safety and input to the development of clear and easy to understand Online Safety guidance materials for all internet users.

Recognising that many of the legal and jurisdictional challenges in the online space require EU or international approaches, we will seek to ensure in conjunction with our EU partners that regulatory, technological, and self-regulatory responses, developed in respect of illegal content, are applied where appropriate to harmful content.

It is only through international cooperation and agreement that a Digital Safety Commissioner could be effective in enforcing a system of 'notice and take down'. Progress in this area must be pursued on an EU or international level

Goal 4: Influencing Policy

Actions	Constituent elements	Responsible Departments	Timeline
16. We will work with EU and international partners to actively promote online safety	16.1 Recognising that many of the legal and jurisdictional challenges in the online space require EU or wider international approaches, we will seek to ensure in conjunction with our EU partners, that regulatory, technological and self-regulatory responses developed in respect of illegal content, are applied where appropriate to harmful content	D/JE D/CCAE D/BEI	ONGOING
	16.2 Publish Ireland's 2017/2018 WePROTECT global alliance report and identify gaps and prioritise national efforts to address them.	D/JE	Q1 2019
17. We will revise the regulatory framework for on-demand audio visual media services	17.1 Conduct a public consultation on the implementation in Ireland of the revised audio visual media services directive	D/CCAE	Q4 2019
	17.2 Revise the legislative framework and regulatory oversight structures in line with the directive and public consultation outcomes	D/CCAE	Q3 2020
	17.3 Assign the responsibility for the regulation of on-demand services	D/CCAE	Q4 2019
18. We will work with the Joint Oireachtas Committee in relation to the Digital Safety Commissioner Bill 2017	18.1 We will work with the Joint Oireachtas Committee on Communications, Climate Action and the Environment to explore the issues arising in relation to the Digital Safety Commissioner Bill 2017.	D/JE D/CCAE D/BEI	ONGOING

Goal 5:

Building our Understanding

Key Objectives of Goal 5

- Establish a new National Advisory Council for Online Safety
- Research and publish an annual Safer Internet Report

Establishment of a new National Advisory Council for Online Safety

The Government has to date been guided in its work by the Internet Safety Advisory Committee (ISAC). The ISAC acts as a forum for relevant stakeholders to share experience in the area of Online Safety, and advises on the monitoring and evaluation of the existing self-regulatory framework by Internet Service Providers to ensure a safer internet environment. It also advises on public awareness raising in relation to illegal and harmful content on the internet; and on the current approaches both domestically and internationally in addressing this issue.

The ISAC is comprised of representatives from An Garda Síochána, the Office of the Data Protection Commissioner, industry and academia, and four partner bodies of the Office for Internet Safety in the EU Safer Internet Programme - ISPCC Childline, Professional Development Service for Teachers (Technology in Education), National Parents Council (Primary); and Hotline.ie.

While the Committee has carried out much valuable work since its establishment in 2000, technology and how we use it has evolved greatly in the past two decades. Both the benefits and the risks associated with using the internet are more complex than they were 18 years ago.

Therefore, it is necessary to replace the existing committee with a new National Advisory Council for Online Safety with a broad based membership, as recommended by the Joint Oireachtas Committee on Children and Youth Affairs in its March 2018 report.

The Council will be tasked to

- Provide advice to Government on Online Safety policy issues
- Identify emerging issues where Government intervention may be warranted, including in future iterations of the Government's Action Plan
- Input to the development of clear and easy to understand Online Safety guidance materials for all internet users, including targeted material for children and young people, parents, and older people
- To act as the national stakeholder forum for the purposes of EU funded programmes
- Review national and international research and disseminate key findings to Government, stakeholders, and the wider public
- Provide an annual report for Government on emerging trends and risks and industry's response

The Council will be chaired by a Minister of State. It is envisaged it would meet on a quarterly basis and agree a 12 month work programme at its first meeting, in line with the Action Plan and in collaboration with the Sponsors Group. The work of the Council will be supported by the Department of Communications, Climate Action and Environment.

Involvement of Stakeholders in Working Groups

A key element of the Council's work can be progressed through working groups. The Council may establish working groups to inform specific pieces of work, the membership of which will involve experts and industry representatives relevant to the topic beyond the core membership of the council.

Membership

The Council will have a core membership of up to 20. Membership of the Council will be refreshed every two to three years to involve other persons in the core membership.

Senior officials from each key Department, i.e. Justice and Equality; Communications, Climate Action and Environment; Education and Skills; Health; Business, Enterprise and Innovation; and Children and Youth Affairs may attend Council meetings in an advisory capacity.

Consult with children and young people

Recognising that Online Safety is an issue of particular concern where young people are concerned, it is important that young people have an opportunity to contribute their views and experiences.

The National Strategy on Children and Young People's Participation in Decision-making (2015-2020), commits to the establishment of a Children and Young People's Participation Hub by the Department of Children and Youth Affairs.

The Hub will become the national centre for excellence on children and young people's participation in decision-Making. It will support implementation of the strategy through the provision of information, training and advice for Government departments and agencies and the non-statutory sector.

A number of significant actions have been taken to date in establishing the Hub. An online children's participation database of publications on the theory and practice of children and young people's participation in decision-making has been published. An audit of education and training on children's rights and children and young people's participation in decision-making in all third level, further education and continuing professional development programmes in Ireland has been commissioned. The first training programme on creative methods of seeking the views of children and young people was developed and delivered to adults working in the government, statutory and NGO sectors.

Another valuable platform for engaging and consulting with children and young people are the *Comhairle na nÓgs*. These child and youth councils give children and young people the opportunity to be involved in the development of local services and policies and are established in the 31 local authorities of the country.

A number of Comhairles have undertaken projects looking at Cyber Security and Online Safety including the development of an Online Safety Programme which is being shared across Youth Work Ireland youth services regionally.

Goal 5 - Building our Understanding

Actions	Constituent elements	Responsible Departments	Timeline
19. Publish an annual safer internet report	19.1 To coincide with Safer Internet Day, we will publish an annual safer internet report for Ireland detailing statistics, resources available, and findings from relevant research including relevant summary data from Growing Up in Ireland as it becomes available	D/CCAE D/CYA	Q1 2019
20. Establish a National Advisory Council for Online Safety	20.1 Establish a National Advisory Council for Online Safety • Replace the ISAC with a new national advisory council for online safety • Assign clear Terms of Reference to the new advisory council, including to provide advice to Government on online safety policy issues and to identify emerging issues where Government intervention may be warranted • Membership of the council will be broad based and will include representatives of industry, academia, voluntary sector, children, parents	Government	Q3 2018
21. Support the implementation of the Action Plan through consultation with Children and Young People	21.1 As informed by the Sponsors Group, we will consult with children and young people through Hub na nÓg, Young Voices in Decision Making	D/CYA D/ES	Q1 2019

Making it Happen

Key Objective

- We will ensure political oversight of the implementation of this Action Plan
- We will reconstitute Government structures to support delivery of this Action Plan

Strengthen Structures

Political Oversight

A Cabinet Committee, chaired by the Taoiseach with membership comprising relevant Ministers, will maintain political oversight of the Action Plan and implementation of the actions therein.

Functional responsibility for relevant policy issues remains with the lead Minister/ Department, who will be accountable to the Oireachtas for implementation of assigned actions.

To further support political and public engagement a Minister of State has been tasked by Government of ensuring an effective link between the political system, Government Departments, and external stakeholders.

Establishment of a Sponsors Group to Drive Implementation

A Sponsors Group will be established with membership comprising each of the relevant Departments. Delineation of policy responsibility operates on the basis that if a Department is responsible for a policy area offline then it is responsible for the policy area online as well. Given the broad range of relevant issues it is essential that Departments work closely through the Sponsors Group to: The role of the Group is to:

- Drive implementation of the Action Plan in line with the agreed timelines

- Develop a framework for monitoring and reporting on implementation progress in line with agreed schedule

- Publish biannual progress reports on Action Plan implementation on each Department's Website / Gov.ie

- Ensure a coordinated, whole of Government approach to Online Safety, including working on a collaborative basis, with commitment from each Department, to
    - review, consolidate and augment resources to support on-line safety;

  - develop and maintain a single online point of contact;
  - initiate and roll out a national communications campaign directed at all users, with key messages targeted at specific user groups including children and young people; parents and guardians.

- Assist the work of the National Advisory Council through provision of information, policy papers, and other material as requested.

The Chair of the Group will rotate between key Departments for the lifetime of the Sponsors Group. The Department of Education and Skills will Chair the group for the duration of the Action Plan (2018-2019).

Leadership Roles within the Sponsors Group

- The Department of Education and Skills leads on Schools policy development; Web wise; support for NPC (Primary) helpline

- The Department of Communications, Climate Action, and Environment leads on structured engagement by Departments with online platforms; and review of the Audio Media Visual Services Directive

- The Department of Justice and Equality leads on oversight of hotline.ie; legislative changes to criminal law; liaison with an Garda Síochána on implementation/enforcement issues; and disbursement of EU funding

- The Department of Children and Youth Affairs leads on consultative engagement with children and young people, including through Comhairles; and implementation of Children First.

- The Department of Health leads on the development of online signposting tool for mental health supports; and implementation of Healthy Ireland

- The Department of Business, Enterprise and Innovation leads on oversight of the E-commerce Directive (2000/31/EC); Interdepartmental Committee on the Digital Single Market.

Resourcing of Key Actions

Resources are already being provided by each of the relevant Departments for a range of Online Safety measures.

The new structures that will be established on foot of this action plan, i.e. the National

Advisory Council for Online Safety and the Sponsors Group will need support from the responsible Departments. In addition, some of the actions that require a coordinated approach with responsibility across a number of Departments - consolidation of resources to support Online Safety; development of a single online point of contact; and the rollout of a communications campaign- will also require additional resources.

Implementation of the EU Safer Internet Programme

The EU Safer Internet Programme, a consortium of industry, education, child welfare and government partners, comprise the Safer Internet Centre in Ireland. The project aims to develop national initiatives promoting safer use of the Internet and to enhance protection of the vulnerable, particularly children, against the downside of the Internet.

Currently, the Office for Internet Safety (OIS) acts as the coordinator of the Programme and channels EU funding to four partners:

- ISPCC Childline;
- National Parents Council (Primary);
- Professional Development Service for Teachers (Technology in Education); and
- Hotline.ie.

Each partner retains operational independence and it is responsible for the achievement of specific objectives and related tasks and activities. These bodies respectively focus on providing a helpline for children; helping parents, raising awareness on internet safety in schools, and the provision of a reporting service for illegal content.

Funding for internet safety comes under the Connecting Europe Facility (CEF) budget envelope and attracts grant funding at a rate of 50% with matched funding provided by the relevant project partners. To date Ireland has received €3.4m in funding under this programme. The EU Commission has recently announced a call for proposals for funding for the period 2019-2021.

Refocusing of the existing Office for Internet Safety

The Office for Internet Safety (OIS) has taken lead responsibility for Online Safety in Ireland, particularly but not exclusively as it relates to children and operates on a partnership model with sectoral experts and operators.

Its activities focus on awareness raising and information; coordinating the EU Safer Internet Programme for Ireland; oversight of takedown procedures for Child Sexual Abuse Material; and developing strategic actions to promote the highest possible levels of Online Safety, particularly in relation to combating child sexual abuse material.

The OIS also has an oversight role in relation to Hotline.ie and the Garda blocking initiative. Hotline.ie is the confidential reporting service for illegal content on the internet in Ireland. Specially trained analysts are permitted to view suspected illegal content and if it is deemed probably illegal they refer it on to the Gardaí and to their own member companies, the Internet Service Providers Association of Ireland, for take down. Protocols are also in place for the notification and removal of illegal content where it does not originate in Ireland.

While the OIS performs a very important function in relation to illegal content online, it is not best placed to lead on the broader digital citizenship initiatives, which will now be progressed through the Sponsors Group. The functions of the existing OIS will continue under the remit of the Minister for Justice and Equality incorporated as part of the Department's crime policy function but be refocused to deal exclusively with issues of law enforcement and coordination of EU funding proposals.

Making It Happen

Actions	Constituent elements	Responsible Departments	Timeline
22. We will ensure that off-line and on-line responsibilities are aligned with effective whole of government coordination	22.1 Establish a sponsors group to drive implementation of the Action Plan • Comprising the six key departments which will lead on individual goals/actions • A progress report on implementation of the action plan will be published bi-annually	D/ES D/CYA D/CCAE D/JE D/HEALTH D/BEI	Q3 2018
23. We will ensure political oversight of the implementation of this plan	23.1 Reporting on action plan via a Cabinet Committee chaired by the Taoiseach • A Minister of State will be tasked with ensuring an effective link between the political system, Government Departments, and external stakeholders. • Oversight of Action Plan implementation by a Cabinet Committee chaired by the Taoiseach	SPONSORS GROUP	ONGOING
24. We will reconstitute government and stakeholder structures to support delivery of this action plan	24.1 Establish a National Advisory Council for Online Safety • Replace the ISAC with a new national advisory council for online safety • Assign clear Terms of Reference to the new advisory council, including to provide advice to Government on online safety policy issues and to identify emerging issues where Government intervention may be warranted • Membership of the council will be broad based and will include representatives of industry, academia, voluntary sector, children, parents	GOVERNMENT	Q3 2018
	24.2 The Department of Justice and Equality will retain responsibility for hotline.ie and the criminal aspects on online safety	D/JE	ONGOING
25. We will ensure appropriate funding and resourcing targeted at online safety initiatives is in place	25.1 Ensure appropriate funding and resourcing targeted at online safety initiatives is in place	D/PER SPONSORS GROUP	Q3 2018

www.gov.ie/besafeonline

Rialtas na hÉireann
Government of Ireland