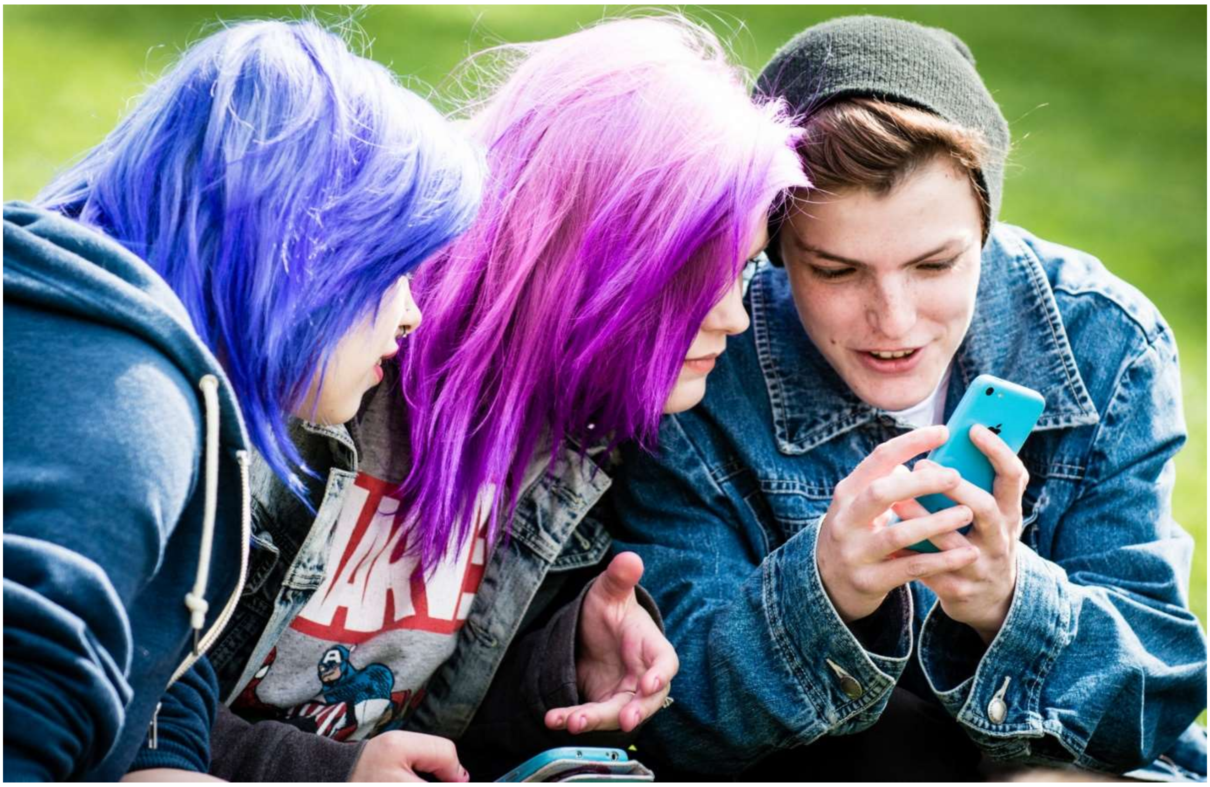


# Keeping children and young people safe: an Online Safety Strategy for Northern Ireland 2020-2025

Northern Ireland Executive

www.northernireland.gov.uk

## Table of contents

# Foreword

**Rt Hon Arlene Foster**
**First Minister**

**Michelle O'Neill**
**deputy First Minister**

**Foreword**

The online world is an integral part of today's society. It is right to embrace it and our children and young people have every right to be part of it and to be empowered to engage with it in a safe, responsible and respectful way.

It has much to offer our children and young people in areas such as education, recreation, social networking and employment. Social media, emailing, texting, shopping, gaming, uploading, downloading and streaming content are all online activities that can be positive experiences. However, this ever-changing and fast-growing environment presents risks to our children and young people. It is unfortunately also used by those who wish to cause them harm and exploit them.

The Online Safety Strategy and its accompanying action plan have been developed with the vision that all children and young people enjoy the educational, social and economic benefits of the online world, and that they are empowered to do this safely, knowledgably and without fear. The strategy takes full cognisance of the rights of children and young people to be part of the online world.

Children are now accessing the online world from a very young age. The risks children and young people face online can differ depending on their age and circumstances. Cyberbullying, sextortion, sexting, grooming, exposure to inappropriate or harmful material are just some of the risks we must address. The harm that can be caused can have a devastating and long-lasting impact on victims, their families and carers.

Through implementation of this strategy and action plan we will create a sustainable online safety infrastructure that enhances and promotes online safety for Northern Ireland, we will educate children and young people, their parents and carers and those who work with them; and we will develop evidence informed quality standards for online safety provision.

Essential to achieving our vision is the meaningful participation of children and young people; parents and carers; schools, colleges and youth organisations; practitioners who work with children and young people; service developers and policy makers; the wider public; internet and technology providers and wider statutory and voluntary services.  There is a responsibility on all of us to help ensure children and young people are safe in the online world.

Online safety of children and young people falls within the remit of all government departments in some capacity.  Executive Ministers are supportive of this strategy.  We are confident that the implementation of this strategy and action plan will assist children and young people to participate in the online world in a positive, safe and responsible way.  We commend it to you.

# Vision and objectives of this Online Safety Strategy

**Our vision is that all children and young people enjoy the educational, social and economic benefits of the online world, and that they are empowered to do this safely, knowledgably and without fear.**

The **overall objectives** of this Online Safety Strategy are to support the development and implementation of a comprehensive cross-government action plan that will improve online safety by:

- Reflecting emerging evidence of good practice in online safety approaches.
- Engaging with existing online safety mechanisms in the UK and beyond, seeking to add value to existing work rather than duplicate.
- Educating and empowering children and young people, and those responsible for their care, to facilitate their informed use of digital technology.
- Educating children and young people on how to manage and respond to harmful online experiences, while ensuring they can access age-appropriate support services, including recovery services, should the need arise.
- Facilitating the meaningful participation of children and young people, parents and carers, and those who support them, in relevant policy and service development.

# The challenge: Why do we need an Online Safety Strategy for Northern Ireland?

## Introduction

The online world is vast and growing daily, providing a wealth of educational and social opportunities for children and young people. Today's generation has been born into a world where the internet is an integral part of everyday life, used for socialising, shopping, gaming and networking, alongside a host of other activities. The lines between the online and offline world are increasingly blurred, with the internet a core component of the way in which young people communicate and interact. In 2018, the Office for National Statistics reported that 100% of households with children across England, Scotland and Wales now have internet access, with estimates suggesting Northern Ireland aligns with this. OFCOM (2019) reports that 83% 12-15 year olds own a smartphone, and 99% go online for an average of 20.5 hours per week.

With increased use has come increased concern, evidenced by emerging research as well as media coverage of incidents of cyber-bullying, grooming and exploitation, feedback from schools involved in the NI Anti-Bullying Forum, practitioners working with children and young people, and from children, young people and parents/carers themselves. There is a particular need to understand the impact that emerging technologies may have, good and bad, and mitigate against any potential risks. The impact of spending time online on the wellbeing of children and young people has been an increasing topic of research in more recent years, with contemporary research considering such issues as; the impact of blue light on sleep patterns, the implications for body image stemming from social media profiles, and even the potential impact on early child development of a technology-focused population (Barnardo's NI, 2018[1]). The Northern Ireland Executive recognises this concern and in January 2015, commissioned the Safeguarding Board for Northern Ireland (SBNI) to develop this Online Safety Strategy for Children and Young People in Northern Ireland. The National Children's Bureau (NCB) undertook this work on behalf of the SBNI.

## What is online safety?

It is important to first clarify the terminology used and provide a definition of what 'online safety' relates to in the context of this strategy. There is no legal or universally recognised definition of

[1] Barnardo's NI (2018) Connections- Parenting infants in a digital world
http://www.barnardos.org.uk/connections-parenting-infants-in-a-digital-world.pdf

'online safety' in the current literature. Indeed, there is much variance around the use of the terms such as online, digital or internet safety, digital safeguarding or citizenship, in everyday discussion. Through the consultation process, it was agreed that 'online safety' should be adopted for the purposes of this strategy; this will ensure the focus is placed on activities and behaviours rather than the device through which they take place. However, it is acknowledged that other terms may be used interchangeably throughout wider literature and practice. The term 'Online world' is broadly equivalent to the term 'Digital Environment' used in the Council of Europe guidelines (CM/Rec (2018)7[2]) to respect, protect and fulfil the rights of the child in the digital environment and which is reflected in the European Network of Ombudspersons for Children (ENOC) Position Statement on "Children's Rights in the Digital Environment" (September 2019[3]).

## Our definition

For the purposes of common understanding, this strategy assumes the following definition:

**Online safety relates to all engagement in the online world.**

**It means supporting and empowering children and young people to engage in online activities in an educated, safe, responsible and respectful way.**

Activities which fall under the remit of online safety include:

- Social and economic activities such as social media, shopping, gaming and downloading or uploading online content.
- e-Communications, including texting, emailing, instant messaging and video chatting.
- Some offline activities on electronic devices, such as gaming or watching downloaded content.

[2] https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

[3] http://enoc.eu/wp-content/uploads/2019/10/ENOC-2019-Statement-on-Childrens-Rights-in-the-Digital-Environment.pdf

Children and young people must be fully equipped to make use of these facilities appropriately, safely and respectfully, particularly when interacting with others.

## What do we know about the online safety needs of children and young people?

The online world has opened up a new level of opportunity for children and young people. This is particularly the case for socialising. 99% of 12-15 year-olds report going online for an average of 20.5 hours per week; during this time, they play games, watch Youtube, stream programmes or interact on social media. 69% of 12-15 year olds have a social media profile, as do 18% of 8-11 year olds, despite the minimum age being set at 12 (OFMCOM, 2018), while the young people we spoke with told us that they communicate via social media constantly throughout the day. Yet the online environment also presents a number of risks. The UK Safer Internet Centre classifies risks as follows:

- **Content:** the child or young person is exposed to harmful material, for example pornography, racist or homophobic abuse, or pro-self-harm/suicide information.
- **Contact:** the child or young person is a victim of adult initiated online activity such as online grooming, harassment, sexual abuse or exploitation, extortion or ideological persuasion (radicalisation).
- **Conduct:** the child or young person is a victim or perpetrator of inappropriate or illegal peer to peer activity such as sexting, cyberbullying or sexual harassment.
- **Commercialism:** the child or young person is exposed to inappropriate commercial advertising, marketing schemes or hidden costs, such as online fraud or scams, in-app purchases, or illegal or age restricted products or services.

There is increased concern at the potential impact that interactions in the online world may have on **mental health and wellbeing**, although there is currently limited and inconclusive evidence in this regard. UKCCIS (2017) report an increase in websites that promote suicidal ideation and self-harm, while the Royal Society for Public Health (2017) notes that spending too much time online can increase anxiety, social isolation, opportunities for bullying, and poor body image, all of which may contribute to poor mental health. Hale and Guan (2015), and Cleland Woods and Scott (2016) also note the potential negative impacts from lack of sleep due to the pressure to communicate via social media late into the night; the as yet unknown impact of constant blue light from screens; and 'Fear of

Missing Out (FOMO) created by the unrealistic representation of life on social media.

> *"It is crucial that the Strategy reflects that the 'online' and 'offline' worlds are absolutely integrated for young people and those issues that arise online do not stop when they disconnect… experiences of cyberbullying can affect school attendance and increase anxiety about going to school." (Consultation respondent)*

More recently, research has focused on the impact of **technology in the early years.** Barnardo's NI (2018)[4] report that parent use of digital devices in the home may negatively impact their parenting. Parents (with a child aged 0-3 in the house) who report high use of digital devices themselves were less likely to feel like a good role model; more likely to have no rules in place to limit their infant's use of digital technology; and more likely to allow their child to access content alone for longer periods of time.

This strategy emphasizes the need to deliver a strong and consistent level of knowledge for all children and young people, their parents and carers, those who support them and those who provide services for them, by developing a core set of online safety messages to help protect them from harm. This is much needed in supporting a consistent approach from training and service providers in Northern Ireland. Yet we know that children and young people face different online risks to their peers, and these risks change constantly depending on their age and circumstances. During the stakeholder engagement process, and review of existing evidence, the following factors were identified as having a potential impact on the types and level of risks faced by a child or young person online.

- Gender
- Age
- Physical or learning disability
- Existing mental health issues
- Sexual orientation
- Experience of care
- Young people attending education other than at school (EOTAS)
- Black and Minority ethnic groups
- Political opinion

**Gender:** Boys and girls face different levels and types of risk online. Livingstone (2017)[5] summarises the literature on gender differences, highlighting that girls are more likely to share or be pressured into sharing sexual images, to experience bullying, sexual harassment or grooming attempts, while boys tend to be concerned about or exposed to violent content. Boys are also more likely to 'be themselves' online, rather than feeling they have to present a certain image, while girls provide more positive reinforcement for one another online. In delivering online safety messaging to children and young people, training organisations must develop gender-appropriate messaging based on the evidence of risks.

**Age:** Children will experience different risks at different ages. Older children are reported as being more likely to have seen something online that was worrying or offensive (29% of 12-15 year olds) than younger children (17% of 8-11 year olds) (OFCOM, 2017[6]). Children are now accessing the online world from a very young age, bringing a new and as yet unknown set of challenges for the early years sector. Regardless of age differences in risks however, we must take a preventative approach. It is important that we don't designate some issues as a risk to a particular age group; rather all children and young people should receive online safety education on the same range of topics, with the message delivered in an age appropriate way.

**Physical or learning disability:** Young people with a disability are significantly more likely to experience bullying and marginalisation (Young Minds, 2016)[7]. The online world can increase confidence and provide access to information, experiences and social interaction that young people feel unable to access face to face (Cerebra, 2012)[8]. However increased confidence may also result in the young person sharing information that they wouldn't do face to face. Children and young people with a disability will therefore require specialised support, and on occasion increased protection, to enable their access to the online world safely and make equal use of the opportunities that it brings.

[5] Livingstone (2017) Children's online activities, risks and safety A literature review by the UKCCIS Evidence Group https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650933/Literature_Review_Final_October_2017.pdf

[6] OFCOM (2017) Children and Parents: Media use and attitudes report. https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf

[7] Young Minds (2016) Resilience for the digital world. http://www.youngminds.org.uk/assets/0002/5852/Resilience_for_the_Digital_World.pdf

[8] Cerebra (2012) Learning disabilities, autism and internet safety: a parent's guide. http://www.parentsprotect.co.uk/files/learning_disabilities_autism_internet_safety_parent_guide.pdf

**Existing mental health issues:** The link between mental health issues and online use is still an area of emerging research. The Chief Medical Officers (2019[9]) published a commentary on screen based activities, and reviewed the evidence base on the impact on children's wellbeing. While they identified no direct causal effect, the document issues guidance for parents and carers which focuses on agreeing boundaries with children around screen time and activities, as well as leading by example in terms of their own screen time.

A youth-led piece of research, supported by NI Youth Forum, Include Youth and Belfast Youth Forum (2018)[10], found that young people feel mental health is negatively impacted by social media. The media has reported an increase in sites dedicated to suicide, self-harm and eating disorders, meaning already vulnerable young people with a mental health disorder who access such sites may therefore face increased risk. While this strategy emphasizes the positive experiences that the online world can provide, it must also acknowledge the risks. Practitioners working with children and young people with a mental health disorder must therefore be aware of these particular risks and targeted messaging should be developed accordingly.

**Sexual orientation:** Young people who identify as LGBTQ+ often turn to the online world as a source of information, support and peer networking while exploring their sexuality. In this regard, the internet is a positive resource and we must continue to facilitate access. However for many such young people, first steps into the dating world are often facilitated by apps and bring increased risk. A report by ChildLine and Stonewall (2014)[11] found that young people identifying as LGBTQ+ are more likely to send explicit images of themselves to people they haven't met, to post them online, or to meet up with someone they met online. Again particular considerations must be made to ensure young people who are LGBTQ+ are protected from risk while having the opportunities to explore the online world.

**Experience of care:** Children and young people who are looked after will have very individual circumstances which may leave them more vulnerable online. The CEOP website[12] identifies specific risks

[9] Davies S.C., Atherton F., Calderwood C., McBride M. United Kingdom Chief Medical Officers' commentary on 'Screen-based activities and children and young people's mental health and psychosocial wellbeing: a systematic map of reviews'. Department of Health and Social Care (2019). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/777026/UK_CMO_commentary_on_screentime_and_social_media_map_of_reviews.pdf

[10] NIYF, Belfast YF & Include Youth (2018) Elephant in the Room http://www.niyf.org/wp-content/uploads/2018/12/ELEPHANT-IN-THE-ROOM-A4-V2_.pdf

[11] https://www.stonewall.org.uk/sites/default/files/staying_safe_online_guide.pdf

[12] CEOP 'Think u know' https://www.thinkuknow.co.uk/parents/articles/Looked-after-children-Specific-risks/

including contact with birth parents or family members, bullying and risk taking behaviours. However again it is important to ensure that Looked after Children have access to the same online opportunities that other children and young people have, and can use them in a safe and secure way.

**Young people attending education other than at school (EOTAS):** While school provides an ideal opportunity for online safety education, we know that not all children and young people attend mainstream school. These young people may have been expelled or become disengaged from mainstream school, have mental or physical health problems, or may have family commitments preventing them from attending school regularly (e.g. young carers). In 2017, 617 children and young people were receiving education via EOTAS provision (DE, 2018)[13]. The focus of this strategy must therefore move beyond school, targeting youth workers, health and social care practitioners, wider education practitioners and importantly parents, carers and the wider family and community, to ensure that the key messages can reach all children and young people.

**Black and minority ethnic groups (BME):** Children and young people from BME groups have been identified as being more vulnerable online (Munro, 2011)[14]. They may be more likely to seek out peers online, particularly when English is not their first language. Online safety messaging and resources must therefore be accessible for all children and young people. Where appropriate, training and service delivery organisations should consider providing online safety messaging and resources in a range of languages and formats.

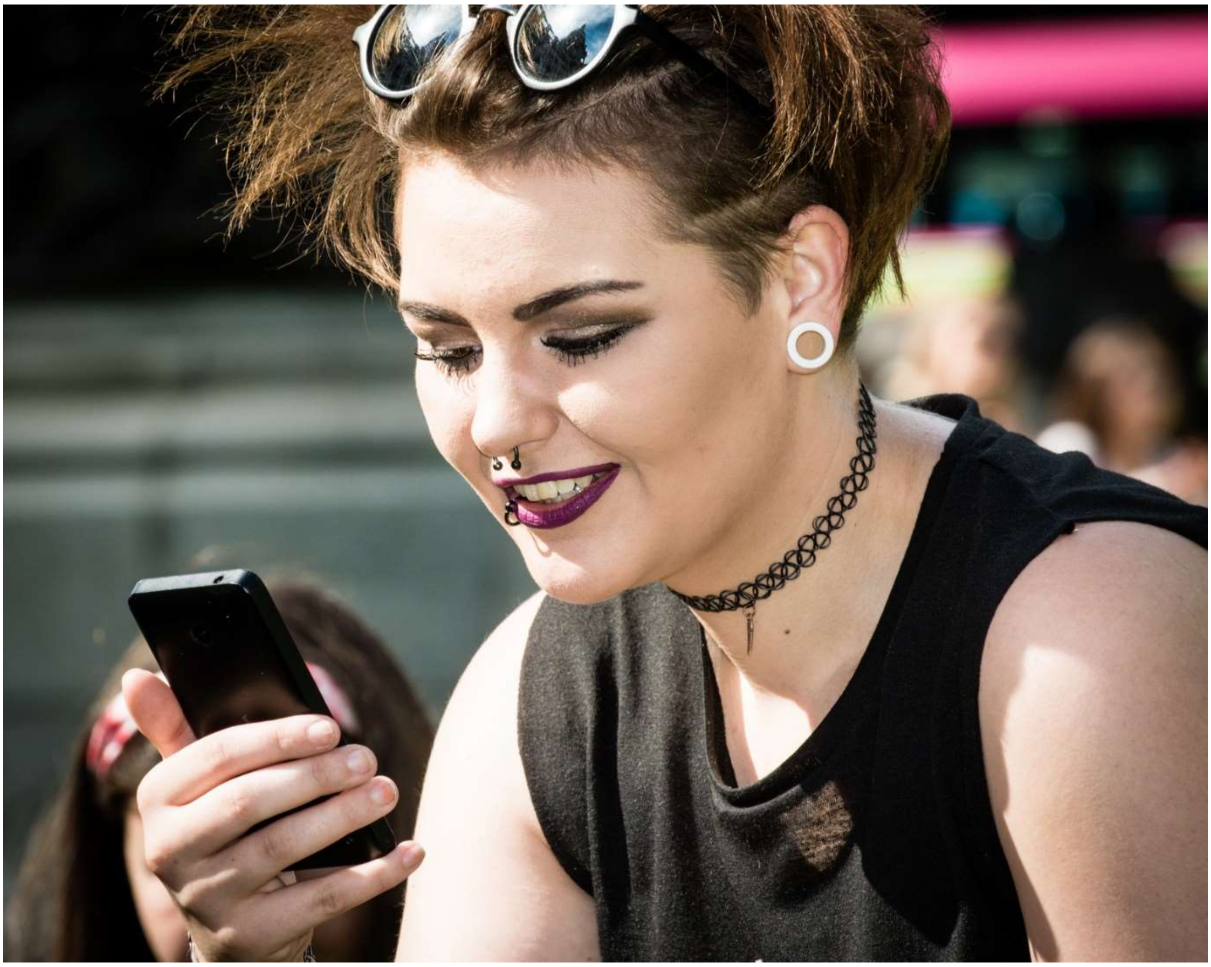
**Political opinion:** While radicalisation of children and young people through social media and gaming has been reported as a rising concern in England, there is no current evidence that this is an issue in Northern Ireland. In terms of local context, incidents of children and young people being targeted by paramilitary organisations have always been a concern, and while social media may act as a medium by which to facilitate meetings, there is no evidence as yet that the online world has increased the risk of children and young people being targeted.

While a universal set of messages, priorities and actions is critical, particular thought must be given to how best to support more vulnerable children and young people, and indeed their parents

[13] Department of Education (2018) Statistical Bulletin 2018/2 Annual enrolments in school and in funded pre-school education in Northern Ireland 2017/18 https://dera.ioe.ac.uk/31137/1/DE-enrolment-stats-bulletin-revised-feb-2018.pdf

[14] Munro, E.R. (2011) The protection of children online: a brief scoping review to identify vulnerable groups. Childhood Wellbeing Research Centre.

and/or those who care for them. While this strategy doesn't begin to address the specific needs of these children and young people, nor does it identify specific relevant messaging, it does provide a framework by which training and service delivery organisations can address the online safety needs of the children and young people they work with through the implementation of this strategy. The strategy also highlights the need for participation of children and young people throughout the process to ensure that their needs continue to be met.



## What does the evidence tell us about keeping children and young people safe online?

An extensive review of evidence and policy was carried out to support the development of this strategy. A number of implications were identified for consideration.

### Legal and policy context

- Legislation and policy must adapt to emerging practices and trends impacting on the safety and wellbeing of children and young people when online.
- It is important to stay connected with and learn from online safety bodies in the UK, Ireland and beyond.
- International research recommends that online safety policies & strategies require more joined up thinking and the need for multi-stakeholder collaboration, including the involvement of industry representatives and youth participation.
- Development of policies, training and support service in online safety should be informed by evidence of existing gaps and the needs of practitioners and service users, as well as by evidence of 'what works' to improve online safety.

### Protecting children and young people

- The varying terminology used to describe online risks (e.g. cyberbullying, sexting, sextortion etc.) make it difficult to measure and record the number of incidents and the associated impact on children and young people.
- There remains a lack of evidence on the impact the internet and digital technology is having on much younger users, both positive and negative, and on the correlation between increasing usage and health and wellbeing indicators.
- Greater emphasis is needed on 'empowering' children and young people to navigate the online world confidently, appropriately and safely, rather than restricting their opportunities.

- Educating children and young people about online safety should cover issues around responsible and appropriate online behaviour, data protection and personal legal responsibilities.

- Focus should be placed on children's rights in a digital age with regard to the right to protection, provision and participation, as per the United Nations Convention on the Rights of the Child (UNCRC) and article 8 of the European Convention on Human Rights.

## Parents and carers

- Parents and carers have a primary role in supporting their child or young person to safely navigate the online world.

- Parental rule-setting surrounding their child/children's online use, where possible and appropriate, should focus less on restricting children and young people's usage and more on educating and empowering them to develop skills and knowledge to stay safe online.

- Parents and carers should be aware that additional filters and parental controls will be necessary to support the online safety needs of their children, and in particular younger children, and should be given the skills, knowledge and support to use these tools effectively.

- Parents and carers must promote a positive example in terms of their internet use, while also considering the potential impact they are having on their child's digital footprint when disclosing information and/or photos online.

- Online safety should be part of a wider public awareness campaign. The messages being promoted should be clear, consistent and effectively communicated.

## Schools, colleges and child/youth services

- Schools, colleges and youth services already take an active role in equipping children and young people with digital skills. Current curricular guidance from CCEA encourages teachers to focus on the creative aspects, including preparing pupils for active civic engagement and creating positive content, to allow children and young people to avail of all the opportunities for learning and communicating online.

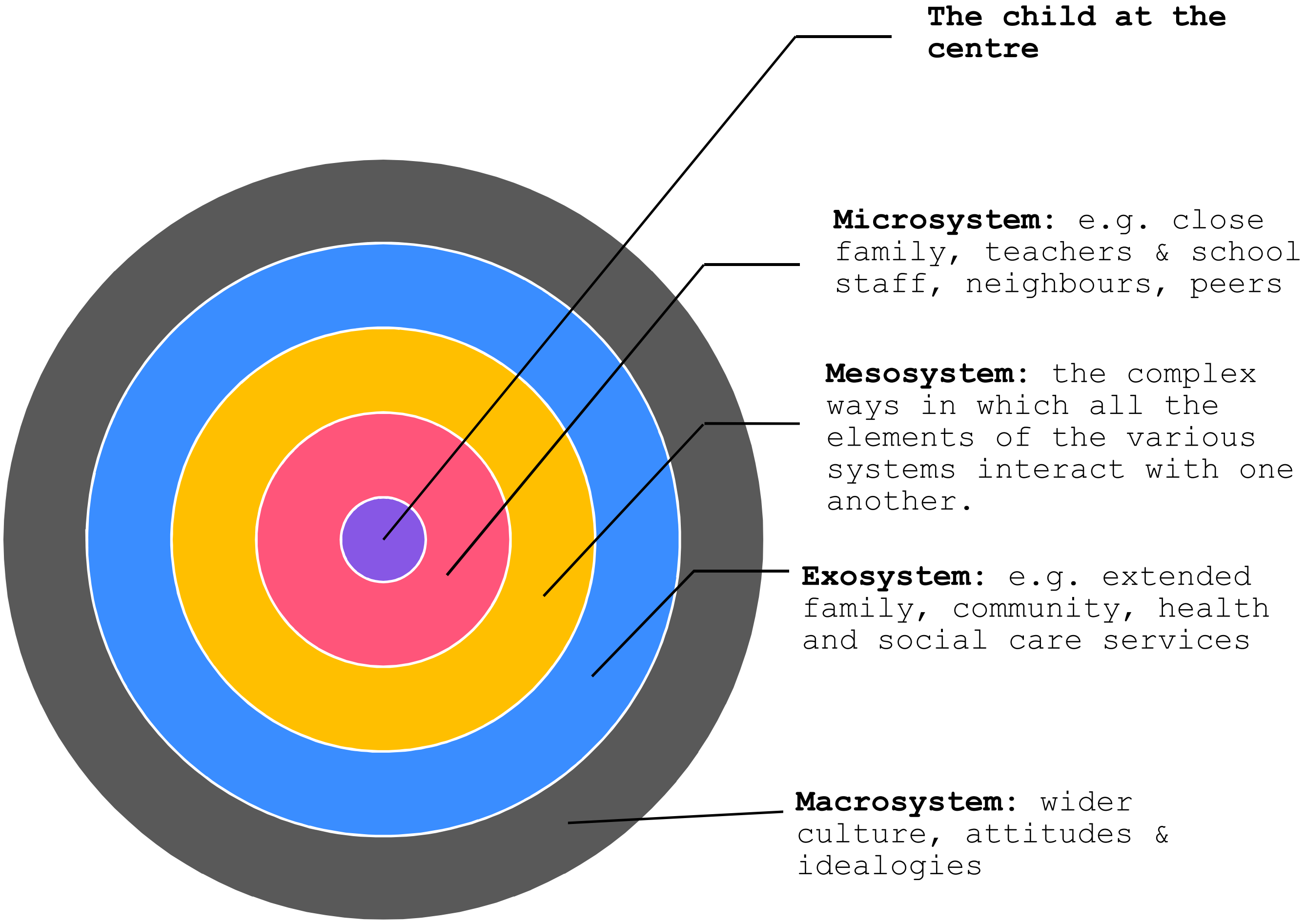
- Strategies to be considered by teachers/educators & youth work practitioners include empowering children and young people through preventative education so they can effectively respond to risk; and peer-to-peer education and mentoring programmes, as evidence suggests that children and young people are most likely to tell a friend if something bothers them online.

- Recording mechanisms in schools, colleges & youth services of safeguarding incidents should include details of any online element to ensure online safety incidence data can be recorded to monitor emerging trends and respond accordingly.

- Online safety self-review tools, such as the 360 degree safe (for schools) and Online Compass (for other statutory and voluntary youth organisations) provide a strong framework to support the embedding of online safety.

## Who should be involved in online safety?

While acknowledging that parents/carers hold primary responsibility for ensuring that their children and young people are equipped to stay safe online, the responsibility doesn't lie solely with them. This is in line with Bronfenbrenner's (1979) [15], Ecological Systems Theory (see figure 1 below), which highlights the range of systems and services which interact with one another over time to shape and influence the child.



**The child at the centre**

**Microsystem:** e.g. close family, teachers & school staff, neighbours, peers

**Mesosystem:** the complex ways in which all the elements of the various systems interact with one another.

**Exosystem:** e.g. extended family, community, health and social care services

**Macrosystem:** wider culture, attitudes & idealogies

**Figure 1: Bronfenbrenner's Ecological Model**

[15] Bronfenbrenner, U. (1979) The ecology of human development: experiments by nature and design. Cambridge, MA. Harvard University Press.

For this reason, this Online Safety Strategy aims to educate, support & involve a wide range of key stakeholders, including:

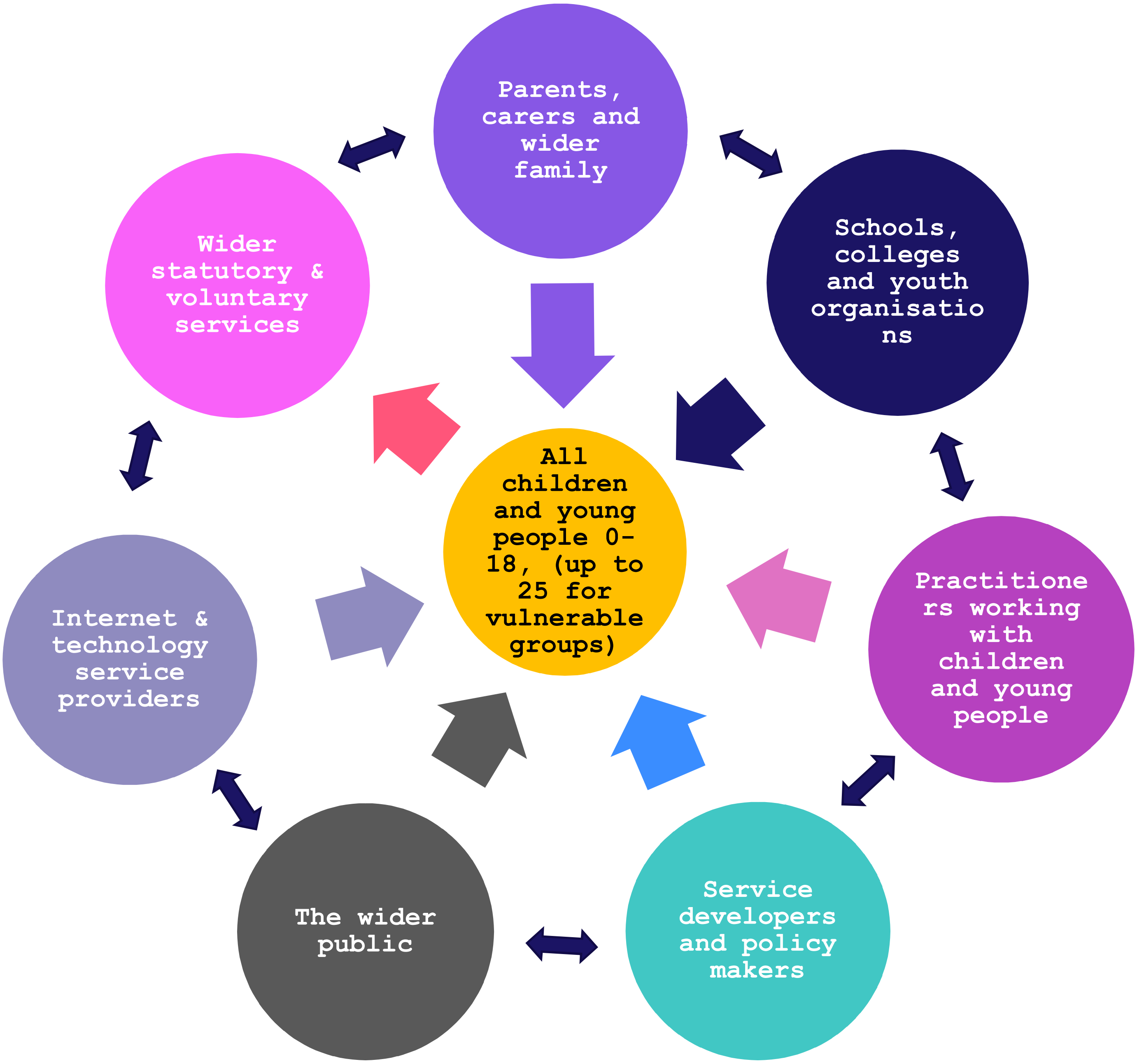

Parents, carers and wider family
Schools, colleges and youth organisatio ns
Practitione rs working with children and young people
Service developers and policy makers
The wider public
Internet & technology service providers
Wider statutory & voluntary services
All children and young people 0-18, (up to 25 for vulnerable groups)

**Figure 2: Stakeholders involved in keeping children and young people safe and well online.**

# The strategic context for online safety

## Children's Rights

This strategy takes a rights based approach and commits to all provisions set out by the European Convention on Human Rights (1953); the Human Rights Act (1998), and the UN Convention on the Rights of the Child (1989[16]),

A number of UNCRC articles are particularly relevant, including:

- A child's right to participation in issues affecting them (Article 12, UNCRC)
- A child's right to freedom of expression (Article 13, UNCRC)
- A child's right to privacy (Article 16, UNCRC)
- A child's right to access to information (Article 17, UNCRC)
- A child's right to protection from violence (Article 19, UNCRC)
- A child's right to health (Article 21, UNCRC)
- A child's right to education (Article 28, UNCRC)
- A child's right to leisure, play and culture (Article 31, UNCRC)
- A child's right to protection from sexual and other forms of exploitation (Articles 34 & 36, UNCRC)

In addition, article 8 from the European Convention on Human Rights:

- Everyone has the right to respect for his private and family life, his home and his correspondence (Article 8, ECHR)

In March 2019, the Committee on the Rights of the Child announced the development of a General Comment on children's rights in relation to the digital environment. The aim of this is to '*strengthen the case for greater action and elaborate what measures are required by States in order to meet their obligations to promote and protect children's rights in and through the digital environment, and to ensure that other actors, including business enterprises, meet their responsibilities'*. Submissions have been made and the Comment is now in development.

Livingstone (2016) classifies children's digital rights as follows:

- The right to **protection** against threats.
- The right to **provision** of resources to help children develop and grow.
- The right to **participation** in society and to have a say in issues affecting them.

[16] United Nations (1989) *United Nations Convention on the Rights of the Child (UNCRC)*, Geneva

This model is referenced widely in the literature.

The **5-Rights Foundation**[17] is an interdisciplinary network of stakeholders, *'working towards a digital environment that anticipates the presence, meets the needs and respects the rights of children'.* The 5 rights vision is that *"children and young people should be supported to access digital technologies creatively, knowledgeably and fearlessly"*

In collaboration with children and young people, parents, carers, teachers, practitioners, policy makers and technology representatives, the Foundation has developed a set of minimum requirements for a child to 'enjoy a respectful and supportive relationship with the digital environment'. These are:

- **The Right to Remove:** children should be able to control their digital footprint and easily remove anything they have put up that they no longer want to be there.
- **The Right to Know:** children should be fully informed about how and why their data is being used.
- **The Right to Safety and Support:** children should be able to easily access support if they are upset by or harmed by anything online.
- **The Right to Informed and Conscious Use:** children should have all the information they need to be able to make their own decisions about how they want to engage in the online world.
- **The Right to Digital Literacy:** children should have the skills and knowledge they need to engage in the online world and to understand the consequences of their engagement.

These developments in terms of children's rights must inform any action stemming from this Online Safety Strategy.

## European context

The **EU Agenda for the Rights of the Child** aims to promote, protect and fulfil the rights of the child in all relevant EU policies and actions. It emphasises that online technologies bring unique opportunities to children and young people by providing access to knowledge and allowing them to benefit from digital learning and participate in public debate. The European Commission aims to achieve a high level of protection of children and young people in the online world, including their personal data, while fully upholding their right to access the internet for the benefit of their social and cultural development.

[17] Five Rights Foundation https://5rightsfoundation.com/about-us.html

The **'Strategy for a Better Internet for children' (May 2012)** proposes a series of actions to be undertaken by the European Commission, Member States and by the wider industry, such as mobile phone operators, handset manufacturers and providers of social networking services. The strategy aims to give children and young people the digital skills and tools they need to fully and safely benefit from being online, as well as unlocking the potential of the market for interactive, creative and educational online content. One of the key actions stemming from this strategy is the implementation of the Better Internet for Kids (BIK) programme, previously the Safer Internet Programme.  Key activities include:

- **Safer Internet forum:** an annual international conference in Europe where a wide range of relevant stakeholders come together to discuss the latest trends, risks and solutions related to children and young people's online safety.

- **Internet Governance Forum (IGF)** – an annual forum bringing together various stakeholder groups to discuss public policy issues relating to the internet.

- **Safer Internet Centres (SICs):** these are present in 31 European countries, and give advice and information to children and young people, parents/carers and teachers – typically comprising an awareness centre, helpline and youth panel. The SICs youth panels are consulted on online safety issues and development of relevant information and material. SICs hosting hotline services receive reports on online illegal content. **Insafe** and **INHOPE** (collaborative network of hotlines) work together through a network of SICs across Europe.

- In the UK, the **UK Safer Internet Centre (UK SIC)** is a partnership of three organisations with experience and expertise in making the internet a safer place: the Internet Watch Foundation (IWF), Childnet International and South West Grid for Learning (SWGfL). The UK SIC carries out awareness-raising campaigns, works closely with youth panels, and operates a hotline and a helpline for professionals working with children and young people.

- **Safer Internet Day (SID):** this is an annual event held in February each year in over 100 countries. SID aims to promote safer and more responsible use of online technology and mobile phones, especially among children and young people across the world. Globally, SID is coordinated by the joint Insafe/INHOPE network, with the support of the European Commission, and 31 national SICs across Europe.

The **European Union General Data Protection Regulation (GDPR)** was introduced in May 2018, bringing significant changes to how organisations can use personal data, as well as stronger sanctions for those who misuse data. The regulation makes specific reference to the protection of children's personal data, as follows:

> "Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child."

The UK has specified that children over 13 can consent to their data processing. GDPR specifies that children must be provided with age-appropriate information to help them understand what their rights are and how their information will be used.

Given the UK's decision to leave the European Union, it is critical that mechanisms are put in place to ensure the continuation of conversations and sharing of good practice on online safety.

## United Kingdom context

In 2008, the UK Department for Children, Schools and Families (DCSF) commissioned Professor Tanya Byron to review the risks to children and young people from exposure to potentially harmful material on the internet and in video games, and to assess the effectiveness and adequacy of existing measures to help protect children and young people from being exposed to such material. The Byron Review **'Safer Children in a Digital World' (2008)**[18] made a series of recommendations to the UK government including the creation of a **UK Council on Child Internet Safety (UKCCIS)**, which was launched in September 2008 (chaired by Home Office/Department for Education). In late 2018, this was further developed into the **UK Council for Internet Safety (UKCIS)**; the remit has moved beyond children and young people to improve internet safety for all. The UKCIS Board includes over 30 organisations including industry, law enforcement, academia, and the charity sector, as well as representatives from the devolved nations.

[18] Department for Children, Schools and Families, and the Department for Culture, Media and Sport. *Safer Children in a Digital World The Report of the Byron Review*, 2008 [Online] Available from http://webarchive.nationalarchives.gov.uk/20130401151715/http://www.education.gov.uk/publications/eOrderingDownload/DCSF-00334-2008.pdf

UKCCIS developed **'Click Clever Click Safe: The First UK Child Internet Safety Strategy (2009)'**[19]. The strategy sets out work carried out to keep children and young people safe online; commitments to parents/carers, children and young people and the work UKCCIS is planning to do to make these happen; and how the public can monitor their level of success in making children and young people safer. A number of initiatives have stemmed from this, including the 'Zip it, block it, flag it' green cross code for internet safety, which has been adopted by social networking sites as well as schools and charities. Additionally, online safety became a compulsory part of the curriculum from the age of 5 as a result of this strategy.

More recently, UKCCIS published **Education for a Connected World: A framework to equip children and young people for digital life**[20]. This Framework sets out the skills and knowledge that children and young people should have at different developmental stages, across a range of topics including:

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, wellbeing and lifestyle
- Privacy and security
- Copyright and ownership

The **5 Rights Foundation (2019) 'Towards an Internet Safety Strategy'** proposes 7 pillars on which an internet safety strategy must be built. These are:

- parity of protection,
- design standards,
- accountability,
- enforcement,
- leadership,
- education and
- evidence-based interventions.

[19] [Online] Available from: https://www.ceop.police.uk/Documents/UKCCIS_Strategy_Report.pdf

[20] Education for Connected World: UKCCIS (2018) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/683895/Education_for_a_connected_world_PDF.PDF

In April 2019, as a response to growing concerns on potential abuse and harm online, the UK Government published the **'Online harms White Paper'**. While the paper relates to all users, the specific vulnerabilities of children are highlighted. The 'online harms' terminology adopted by this paper is a useful inclusive reference that can encompass traditional forms of abuse such as grooming or bullying etc., as well as issues that impact on mental health and wellbeing, such as the addictive nature of online activity or the impact on sleep.

The paper sets out a vision including the following:

- A free, open and secure internet.
- Freedom of expression online.
- An online environment where companies take effective steps to keep their users safe, and where criminal, terrorist and hostile foreign state activity is not left to contaminate the online space.
- Rules and norms for the internet that discourage harmful behaviour.
- The UK as a thriving digital economy, with a prosperous ecosystem of companies developing innovation in online safety.
- Citizens who understand the risks of online activity, challenge unacceptable behaviours and know how to access help if they experience harm online, with children receiving extra protection.
- A global coalition of countries all taking coordinated steps to keep their citizens safe online.
- Renewed public confidence and trust in online companies and services

In particular, this paper proposes a new regulatory framework for online safety which will clarify, enhance and enforce the responsibilities of internet providers and companies providing online services. The involvement of NI Government departments in supporting the progression of this paper will be critical, as will the consideration of any emerging actions and implications in a local context.

The **Information Commissioner's Office (2019[21]) released 'Age appropriate design: a code of practice for online services'** for consultation. This is aimed at any organisation providing online products or services likely to be accessed by children, and provides guidance on how they should ensure that children's personal data is safeguarded and processed fairly. The guidance is aligned to the

[21] https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-public-consultation.pdf

UNCRC and GDPR and contributes to the wider focus on ensuring the protection of children's rights online while working in the best interests of the child.

## Northern Ireland policy context

A number of key safeguarding policy drivers provide the backdrop to the development of this Online Safety Strategy. The Department of Health (DoH) is the lead department on child protection and is responsible for child protection policy. In March 2016, DoH launched the new **Co-operating to Safeguard Children and Young People in Northern Ireland**[22]', providing the overarching policy framework for safeguarding children and young people in the statutory, private, independent, community and voluntary sectors, and outlining how communities, organisations and individuals must work both individually and in partnership to ensure children and young people are safeguarded as effectively as possible.

The **Children and Young People's Strategy 2017-2027 (Department of Education)** was published in December 2019. Aligned to the outcome that 'children and young people live in safety and stability', the Children and Young People's Strategy highlights the need to educate children and young people on how to stay safe online, while also ensuring that parents have the knowledge and confidence to monitor their children's safety.

In addition, **'Safeguarding children: a cross-departmental statement on the protection of children and young people' (OFMDFM, 2009)** emphasised the need for enhanced collaboration and integration of UK-wide and cross-jurisdiction bodies that have responsibility for policing, regulation and public awareness-raising around Internet use. The Safeguarding Board Northern Ireland (SBNI) was established in 2012 under the **Safeguarding Board (Northern Ireland) Act 2011**[23]**.** The SBNI acts in accordance with the Act and **'Guidance to Safeguarding Board for Northern Ireland (2014)**[24]**.** The SBNI's **Strategic Plan 2018-2022**[25] outlines four strategic priorities namely:

1. To provide leadership and set direction in the safeguarding and protection of children and young people.

[22] DoH, Co-operating to Safeguard Children and Young People in Northern Ireland. (March 2016) [Online] Available from: https://www.health-ni.gov.uk/publications/co-operating-safeguard-children-and-young-people-northern-ireland

[23] The Safeguarding Board (Northern Ireland) Act 2011 [Online] Available from: http://www.legislation.gov.uk/nia/2011/7/contents

[24] DHSSPS, Guidance To Safeguarding Board For Northern Ireland (May 2014). [Online] Available from: https://www.dhsspsni.gov.uk/sites/default/files/publications/dhssps/sbni-guidance-may2014.PDF

[25] SBNI, Safeguarding Board for Northern Ireland Strategic Plan 2018-2022. [Online] Available from: https://www.safeguardingni.org/sbni-strategic-plan-2018-2022

2. To provide a voice to children and young people affected by domestic and sexual violence and abuse.
3. To improve outcomes for children and young people affected or potentially affected by neglect through promoting the early recognition and improvement of agency responses.
4. To provide a voice for children and young people affected by mental health issues.

The strategic plan highlights SBNI's specific commitment to online safety, noting that they will *'continue to work to keep children and young people safe online and deliver on the intentions contained in the Northern Ireland Executive e-Safety Strategy and Action Plan (in development)'.*

**Cyber Security: A Strategic Framework for Action 2017-2021** was released by the Department of Finance in 2017. While not primarily targeted at children, the Framework has potential to impact children's lives; the key aim is to build a safe and innovative society where individuals, businesses and communities can safely and skilfully access the most leading edge digital resources. Strands of work will focus on:

- **Leadership**: establishing governance structures to support coordination of efforts across Northern Ireland and wider UK.
- **Defend**: the framework will seek to address cybercrime and keep individuals and businesses protected through enhancement of security provisions and cybercrime reporting mechanisms. Security of public Wi-Fi (in particular through the Smart Cities initiative) is identified as a key action, as is education and awareness raising of cyber security issues.
- **Deter**: the framework will seek to build on resources to respond to and punish cybercrime, as well as prevention approaches which will educate and deter those who are at risk of becoming involved in cybercrime.
- **Develop**: the framework will also focus on growing local talent in the cyber industry through provision of digital skills programmes, continued professional development and building and sharing opportunities for a career in cybersecurity.

The **SBNI 'Child Safeguarding Learning and Development Strategy and Framework' (2015 – 2018)** aims to contribute to the improvement of child protection and safeguarding training and education by setting out the key minimum learning outcomes to equip staff and volunteers in organisations, with the skills, knowledge and competence to promote the safety and well-being of children and young people, within the remit of their roles and responsibilities. Online safety is highlighted as one of the focus areas which will include interagency training and learning outcomes.

Online safety of children and young people falls within the remit of all government departments in some capacity, therefore a cross-departmental strategy is essential. In 2013, OFMDFM carried out an audit of departmental actions, gaps and future priorities around online safety and produced a summary paper 'Synopsis of actions within the public sector to enhance child internet safety' OFMDFM (2013). In informing the development of this draft strategy, follow up interviews were undertaken with departments to capture any progress within departments and identify any further gaps for consideration (the findings have been incorporated in this draft strategy).

The **Department of Education** provide guidance to schools around digital matters via a number of key circulars:

**2016/27 -** Online Safety (current circular)

**2016/26** – Effective Educational Uses of Mobile Digital Devices

**2015/21** – School obligations to manage data

**2013/25** – E-Safety guidance

**2011/22** – Internet safety

In 2014, NCB on behalf of the SBNI **published 'An exploration of e-safety messages to young people, parents and practitioners in Northern Ireland',** a scoping study mapping agencies currently delivering online safety training and support in Northern Ireland. The publication identifies the key messages given across the four risk areas of content, contact, conduct and commercialism, and considers the usefulness and impact of these messages. Key findings from this study included a lack of consistency across Northern Ireland in terms of training delivered and messages given, and highlighted the need for a comprehensive cross-departmental strategy to support the consistent roll-out of online safety training and support.

There is currently work ongoing by the Department of Education and the Public Health Agency to develop a **Wellbeing Framework for Children and Young People.** There is definite cross-over in terms of the remit of these two strategic documents; effort will be made to align commitments to action where possible.

## Current online safety provision in NI

Online safety training and support for children, young people, parents/carers and practitioners is currently delivered across Northern Ireland by a number of training and development organisations. NCB's (2014) report for SBNI on current delivery of online safety messaging across Northern Ireland identified a number of common themes in support:

- **Online safety training**: this is delivered by a wide range of organisations across Northern Ireland, spanning the statutory, voluntary, community and private sectors. There are varying levels of collaboration evidenced, with some good examples of extensive partnership working between these organisations.
- **Messages**: the most common areas targeted by online safety messages in Northern Ireland include using mobile phones, cyberbullying, use of privacy settings and sharing of personal information, and 'sexting'.
- **Dissemination**: online safety messages tend to be delivered in one of four ways:
    - *Resources* to help educate children and young people, and those who care for and work with them, about online safety (such as videos, leaflets, checklists, books, website information).
    - *Training materials* to help professionals educate children and young people, and those who care for and work with them, about online safety (such as handbooks, manuals, session plans).
    - *Training courses* that are delivered in a variety of formats to children and young people and those who care for or work with them.
    - *Public awareness campaigns* on online safety to raise awareness and educate children and young people and those who work with and care for them (such as PR and advertising, press releases, TV and radio footage, print media etc.).

The online safety Evidence and Policy Review (NCB, 2016) which informed this strategy details a full list of providers of online safety training, information and support identified during the review. There have also been numerous developments since. While this strategy doesn't seek to duplicate this work, there is much concern around the often disparate nature of key messages and approaches to training delivery and practitioners report feeling unsure about which resources to 'trust'. This strategy outlines actions to enhance current supporting structures and aims to provide much needed clarity and coordination of messaging. Ensuring quality of resources, training and dissemination methods, and advocating for the measurement of impact on the children, young people and families that services are delivered to.

# The process: designing an Online Safety Strategy for Northern Ireland

## The co-design model

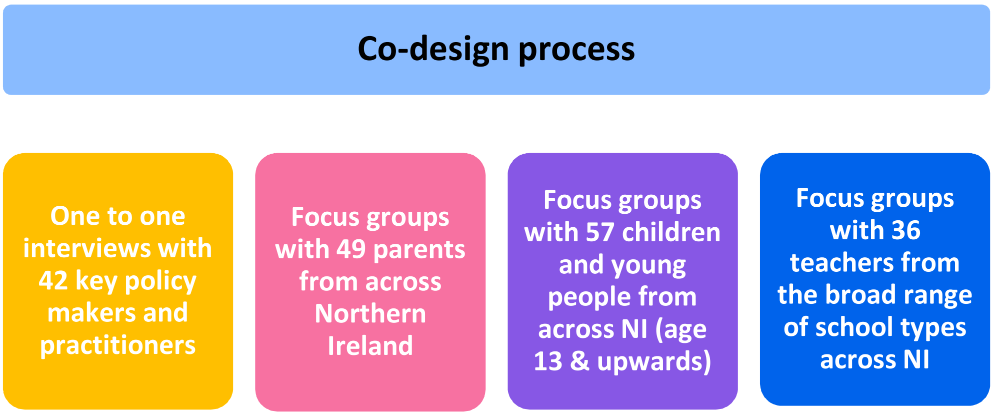
A co-design process informed the development of this Online Safety Strategy for children and young people in Northern Ireland.  This collaborative approach incorporates the voices of children, young people, practitioners and other key stakeholders throughout the design and development process to ensure that any strategic plan and actions developed are fully informed by the real needs and experiences of the people whose lives it will impact.  The following formal structures informed the design, evidence collection and drafting of this Online Safety Strategy:

**Project Board**
Membership from across relevant government departments, statutory & voluntary sector organisations

**Young People's Advisory Group**
20 members, 5 meetings plus ongoing engagement

**Parent Teacher Advisory Group**
20 members, 3 meetings plus ongoing engagement

The following evidence-gathering activities took place as part of the co-design process:



Co-design process

One to one interviews with 42 key policy makers and practitioners

Focus groups with 49 parents from across Northern Ireland

Focus groups with 57 children and young people from across NI (age 13 & upwards)

Focus groups with 36 teachers from the broad range of school types across NI

A complete list of all organisations and individuals involved in the co-design process, along with a summary of comments received, are included in Appendices 1& 2.

## The consultation process

The Online Safety Strategy consultation opened on 4th March 2019 and invited stakeholders (including children and young people) to give their views on its content. An e-survey was shared widely, alongside a children and young person's version.

A total of 334 survey responses were received from individuals, schools and other organisations, as well as 10 written responses submitted outside of the survey template.

964 children and young people also responded; of these:

- 80% were aged between 10 and 15,
- 10% under 10
- 10% over 16.

Various awareness raising and engagement activities also took place alongside the consultation survey. Responses were overwhelmingly positive, with the vast majority of respondents supportive of the proposed approach set out in the draft strategy. Quotes from the responses are included in appendix 2.

> ***"We welcome the emphasis on facilitating young people's use of the internet in a positive way while staying safe online."***

Following analysis of responses, updates were made to the draft strategy, including:

- Review of the language and terminology used throughout, with 'e-safety' replaced with online safety.
- Increased focus placed on children's rights.
- Emerging policy and research reflected, including recent GDPR implications and the HM Government Online Harms White Paper.
- Further emphasis placed on potential wellbeing implications for children and young people.
- Further clarity provided around the governance structure and implementation plans.

# Moving forward: A strategic approach to online safety

## Vision

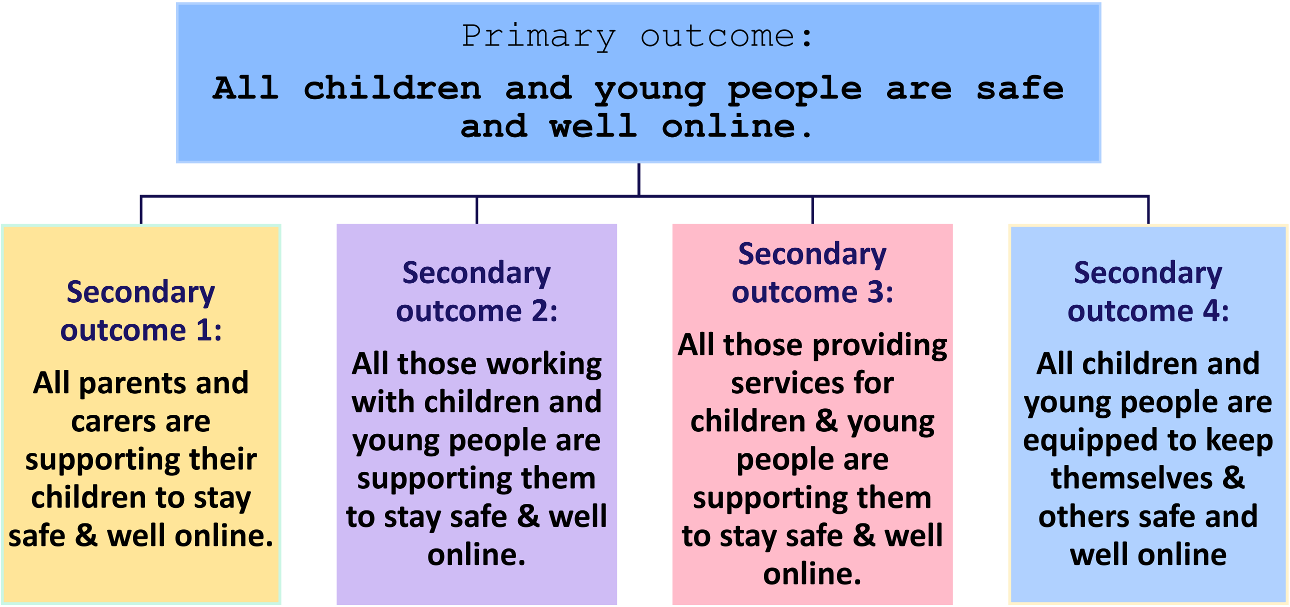
**Our vision is** that all children and young people enjoy the educational, social and economic benefits of the online world, and that they are empowered to do this safely, knowledgably and without fear.

## Outcomes

This Online Safety Strategy aligns to the outcomes of the Children and Young People’s Strategy 2017-2027, in particular, that all children and young people:

- are physically and mentally healthy
- live in safety and stability
- enjoy play and leisure
- learn and achieve

Additionally, this strategy aims to deliver the following outcomes relevant to online safety:



Primary outcome:

**All children and young people are safe and well online.**

**Secondary outcome 1:**

**All parents and carers are supporting their children to stay safe & well online.**

**Secondary outcome 2:**

**All those working with children and young people are supporting them to stay safe & well online.**

**Secondary outcome 3:**

**All those providing services for children & young people are supporting them to stay safe & well online.**

**Secondary outcome 4:**

**All children and young people are equipped to keep themselves & others safe and well online**

## Core principles

Several common themes emerged throughout the stakeholder engagement and consultation processes, which must inform any work taken forward to support the online safety of children and young people.

- The mobile nature of technology has rendered much online safety messaging around restriction and monitoring of online access outdated. While restrictions undoubtedly have their place, particularly for very young children, online safety support must focus on the **empowerment and education** of children and young people, building digital resilience and enabling them to make use of the opportunities while keeping themselves safe and well.

- All stakeholders recognised the importance of a **prevention and early intervention approach** to online safety rather than a reactionary one, emphasising the need for consistent online safety education from the earliest years and continuing until adulthood. This does not preclude the need for appropriate intervention services should incidents arise.

- The strategy must provide **consistency of opportunity** for all. Stakeholders discussed the postcode lottery, with messaging and online safety support dependent on where a child or young person lives. Additionally, inconsistent access and opportunities still exist for some young people, particularly for the most vulnerable groups.

- The Online Safety Strategy, and any ongoing service design and delivery, must be **evidence informed**, making use of the most up to date research on 'what works'. Stakeholders' feedback and a review of available data has also highlighted a gap in **evidence of need.** This Online Safety Strategy must take a **participatory approach** to address this, ensuring that the voices of all stakeholders, including children and young people, parents, carers and practitioners, are fully included in future service design and delivery.

These themes have been translated into a set of core principles and commitments to action, set out below, which will underpin this Online Safety Strategy for Children and Young People in Northern Ireland. It is recommended that all future online safety policies, services and programmes for children and young people take due cognisance of these principles in design and approach.

**Core principles of the Online Safety Strategy for Children & Young People**

- All children and young people have the **right** to access and make use of the knowledge that the online world provides, as long as the information doesn't cause harm to themselves or others.

- All children and young people must be **equally** supported to stay safe and well online, and respect the rights of others to be safe online, regardless of where they live.

- All children and young people, where possible, must be **educated** and **empowered** to access the online world safely, rather than be restricted.

**We will…**

- Take a **joined up approach** to online safety, with all departments committing to improving online safety outcomes for all children and young people.
- Make use of **innovative new tools and methods** provided by the online world in order to disseminate information.
- Take an **evidence-based** approach, ensuring that online safety training and support services are based on both evidence of need and 'what works' to keep children and young people safe online.
- Take an **outcomes** based approach, recognising the need to demonstrate impact on the lives of children and young people.
- Ensure the meaningful **participation** of stakeholders, including children, young people, parents and carers (including corporate parents) to ensure their voice is heard throughout online safety policy and service development.
- Recognise a **tiered** approach to online safety service development and delivery, acknowledging that children and young people all have different needs at different stages in their lives.
- Ensure that all emerging actions recognise the need for **additional support** to be in place **for 'at risk' and vulnerable groups**.
- Recognise the need for a **prevention and early intervention** approach to online safety throughout service development and delivery.
- Ensure that online safety training and support is delivered in **partnership** with parents, carers, those working with children and young people, and the wider community.
- Recognise a **flexible** approach to online safety that can incorporate the rapid pace of emerging technologies and associated risks.

## Commitments to action

In line with the 'whole child' approach to care and support for children and young people, this strategy recognises that the online world is woven throughout every part of children and young people's lives. Online safety relating to children and young people is integral to the wider safeguarding agenda for children and young people. Everyone has a role to play in protecting children and young people online, therefore this strategy is necessarily cross-departmental, representing the NI Executive's collective response to online safety. As such, it must be given due cognisance in the development of all future departmental strategies and guidance impacting children and young people, and align with wider population outcomes.

Utilising the learning gathered throughout the co-design and consultation processes, including existing knowledge of what works elsewhere, this strategy sets out commitments to action across three key areas, to ensure that we achieve our vision of keeping all children and young people safe and well online. Through the commitments to action identified and the necessary actions of all stakeholders, we aim to protect children from exploitation and abuse in all forms in the digital world.

**We will:**

1. **Create a sustainable online safety infrastructure for Northern Ireland**
2. **Educate children and young people, their parents and carers and those who work with them**
3. **Develop evidence-informed quality standards for online safety provision**

## Commitment 1: We will create a sustainable online safety infrastructure for Northern Ireland

This strategy seeks to provide leadership and overall coordination for online safety education and empowerment across NI. To facilitate this, we will support the development of a strong infrastructure, including relationships and resources, which will allow collaboration, consistency and the sharing of good practice within and outside of Northern Ireland. Key areas for change include:

**Developing a central hub for online safety information and facilitation of signposting:** In addition, while a number of excellent resources exist to support online safety, parents/carers, children, young people and practitioners have told us that they aren't sure how to access structures at a regional level. A central repository of online safety information, support and guidance is needed to support dissemination of consistent messaging to children and young people, parents/carers, practitioners, policy makers and the wider public. This resource should be free to access, accessible by all, and should facilitate signposting to existing relevant resources and indeed support services in the event of an incident of concern. Again, the SBNI as coordinating body for online safety will play a critical role in maintaining this hub, ensuring that it is kept up to date with emerging information and resources, and can add to, rather than duplicate, existing resources and services.

**Strengthening links between NI, wider UK and global online safety structures:** Moving forward with online safety provision in Northern Ireland, it is critical that we look beyond our own region and actively involve ourselves in policy discussions at a regional, national and global level. The Department of Health currently sits on the UK Council for Internet Safety (UKCIS); we must strengthen and build on this and other links between the NI Executive and such UK wide online safety bodies, ensuring that we are active players in the overarching development of online safety approaches, and opening up two-way communication channels and opportunities for learning and sharing of best practice. This is particularly important given the wide membership of UKCIS, which includes government representation across the four nations; voluntary, community, statutory and education sector bodies with an interest in online safety; and industry representatives and internet providers, including BT, Sky, Virgin Media and Talk Talk. Working closely with these organisations at a policy level must be a strategic priority for Northern Ireland. There must also be mechanisms in place to allow local children, young people, parents/carers, and those who work with or care for them, to inform this wider discussion.

**Developing a consistent approach to online safety in schools through strong Departmental direction on technical provision:** The Education Authority (EA), via C2K, provide the infrastructure to support the use of ICT in schools. A key part of this for online safety purposes is the filtering system. In line with this strategy's commitment to empowerment and education rather than restriction where possible, EA currently provides a tiered approach, with flexibility for senior staff to allocate pupils to one of five internet security groups:

- Internet default
- Internet Social Networking (e.g. Twitter, Facebook)
- Internet Streaming (e.g. YouTube, BBC iPlayer)
- Internet Advanced (e.g. shopping, webmail, online forums etc.)
- Internet Gaming (e.g. Games required for learning)

EA also provide technical support for schools via a helpline, as well as online safety training and guidance for staff to support the education of pupils.  While teachers and education policy makers reported that school filtering systems were strong, a number of teachers reported that their school had bypassed the core security systems by installing a second Wi-Fi line, often used to support external devices such as i-Pads. Changes and improvements to the EA C2K Wireless system have eradicated the need to install a second line. DE already provide detailed guidance for schools in this area, highlighting that this additional provision is not necessary, however despite this, many schools continue to do this.  This exposes children to additional risk.  The Education and Training Inspectorate (ETI) cover this area in their inspection procedures, referencing the Online Safety Circular 2016/27.  The focus is on provision of online safety messages for pupils, and through discussions with groups of children asks what information they have been given on online safety and how they stay safe on-line.  Moving forward, an ongoing review of technical provision within schools, and continued reminders and enhanced education for schools will be required to further safeguard children in this area.

**Commitment 1: We will create a sustainable online safety infrastructure for Northern Ireland.**

**Summary of key actions.**

- Developing a central repository of online safety information and facilitation of signposting
- Strengthening of links between NI and wider UK and global online safety structures
- Developing a consistent approach to online safety in schools through strong departmental direction and enhanced education for schools on technical provision

## Commitment 2: We will educate children and young people, their parents and carers, and those who work with them

Responsibility for educating children and young people doesn’t fall solely to teachers. Indeed, parents have the primary responsibility for safeguarding their children and young people, in conjunction with a number of other sources. Education can take place at home, at school, in residential or custodial care, at youth clubs and organisations, while socialising with friends or wider family, via the online world, and in a wide range of other settings. Education initiatives in online safety must therefore be targeted not only at children and young people themselves but at parents, carers, the wider family, those working with children and young people in a paid or voluntary capacity, and indeed the wider population to an extent. Parents and those working with children and young people must also be supported to model acceptable behaviour in their own use of e-technologies. Key areas for change include:

**Developing a consistent approach to online safety messages for children, young people, parents, carers and practitioners:** As noted by a range of stakeholders during the co-design and consultation processes for this strategy, online safety messaging often appears confusing and conflicted. Parents feel ill-informed and are trying to enforce rules that are outdated and irrelevant. Whilst children and young people feel that they know enough to keep themselves safe online, they also said that they don't think their friends do, and that stronger messaging is required. Practitioners don't know which resource to trust and often end up creating their own, leading to further disparity. Clarity and consistency of messaging is a key concern for this strategy; we therefore recommend the development of a core set of online safety messages relevant to all. These messages must first and foremost focus on education and empowerment of children and young people, enabling them to make best use of the online world in a safe, secure and respectful way, rather than restricting their access, while at the same time safeguarding the most vulnerable. In line with Section 75 considerations, further specialised messaging should also be developed to reflect individual differences in children and young people's needs, and thought must be given to how best to disseminate these messages, developing resources in a range of formats to ensure they are accessible to all children and young people. Messages should also be developed for parents and carers, practitioners and the wider population, recognising the specific role that each has to play in the safeguarding of children and young people.

**Embedding a culture of online safety within schools, colleges and child/youth services:** Again in line with the 'whole child' approach, this strategy emphasizes that online safety is the responsibility of all and therefore does not fall only under the remit of schools or college. Further effort is needed to achieve a consistent strategic approach to online safety across schools, colleges, health and social care services, as well as other statutory, voluntary and community children and youth organisations. Departmental guidance for such services and organisations must shift the focus to embedding of online safety within the organisational culture. While a standalone Online Safety Strategy is necessary within such organisations to enhance visibility of key issues, online safety should be addressed as a fully integrated aspect of overall safeguarding within schools, colleges and youth organisations. In particular, while the majority of schools and child and youth organisations have appointed a dedicated person with responsibility for online safety, it is essential that this person has clear links with the safeguarding team. Their role in embedding a culture of online safety must be clarified and strengthened, with appropriate resourcing allocated to allow them to build their capacity and that of their colleagues, overseeing policy development, training and support for children and young people, and championing online safety throughout the organisation.

Formal schooling does however continue to provide a key opportunity for widespread education in online safety issues. Agreed core messaging must be incorporated within the cross-curricular skill of 'Using ICT' and the areas of learning of Personal Development and Mutual Learning (primary) and Learning for Life and Work (post-primary), and wider school curriculum at all ages and stages, and where appropriate using structured lesson plans (such as the UKSIC/SWGFL 'Digital literacy and citizenship' lesson plans), while allowing flexibility to suit the needs and stage of the class.

**Skilling up practitioners who work with children, young people and families:** Stakeholder feedback from the 2016 co-design process told us that online safety usually falls within the responsibility of one or two key people within a service or organisation, with the wider team not particularly educated, or often interested, in the issues. While it is important to have one or more staff members with a higher level of knowledge/expertise, a basic knowledge of the online world is essential for all those working with children and young people. This strategy therefore focuses on the need to upskill all those working with children and young people, and proposes a number of key actions to support this, including a wider focus across primary training and in continued professional development for key practitioners.

**Commitment 2: We will educate children and young people, their parents and carers, and those who work with them:**

**Summary of key actions.**

- Developing a consistent approach to online safety messages for children, young people, parents, carers and practitioners.

- Embedding a culture of online safety within schools, colleges and children and youth services and organisations.

- Skilling up practitioners who work with children, young people and families.

## Commitment 3: We will develop evidence-informed quality standards for online safety provision

**Understanding the scale of the problem through research and data collection:** development of online safety guidance, policy and services must be based on up to date evidence of need, and of 'what works'.  Investment should be made in research to continue to improve our knowledge on the impact of the online world and the risks facing children and young people, and on 'what works' best to support them to safely navigate the online world.  We must also work to understand local need to ensure that service development adequately addresses this.  Outside of official crime statistics, there is little regular data collected on either the scale of online safety related incidents happening across NI, nor of the particular issues and concerns facing children, young people and parents or carers on a regular basis.  It is important to remember that the incidents which make the headlines, or appear as crime statistics are the exception; we know little about the everyday online safety needs of children and young people.

This strategy proposes the need to collect and collate more robust data to inform future strategy direction.  This will require stronger direction on recording and reporting of incidents across the children and youth sector, and a commitment to further research to help us understand the real impact on children and young people's lives in Northern Ireland.  The recent Addressing Bullying in Schools (NI) Act 2016, which has not yet come into operation, will legislate for the recording of information pertinent to incidents of bullying in schools, including circumstances and motivation for the incident.  While plans don't currently extend to collating this information at population level, the information must be used by schools to inform their own work.  A similar approach could be taken to online safety to ensure that we have up to date information on the actual occurrence of online safety related incidents.

**Strengthening self-assessment processes for online safety:** Self-assessment is a critical tool in developing and maintaining a consistent approach to online safety across Northern Ireland.  For schools, colleges, youth and community organisations, an online safety self-assessment tool will help to embed online safety within the school ethos.  The '360 degree safe' tool is already used by a number of schools, and allows them to consider their overall approach to online safety, from putting the appropriate policies and procedures in place, to implementing them in every day practice.  An associated but less detailed tool, the Online Compass, is available for other organisations to follow a similar approach. This strategy proposes the widespread promotion of self-assessment tools such as these within schools, colleges and statutory organisations, as well as across voluntary and community sector organisations.

**Introduction of an accreditation scheme for online safety training delivery organisations:** In developing this strategy, extensive work has been carried out to gather evidence of existing training and education services, and numerous programmes have been identified across the private, voluntary and statutory sector. This leads to confusion for those organisations seeking to purchase training for the young people or practitioners they work with, and again results in inconsistency of messaging. While this strategy does not seek to duplicate ongoing work, and indeed cannot endorse one training programme over another, there must be a guarantee that these programmes and services are providing a consistent, safeguarding approach to online safety for all children and young people. The introduction of an accreditation scheme for training organisations has been successful in supporting the delivery of a high quality standard of service in Australia. Organisations who wish to be included on a list of approved providers of online safety training in Australia must apply to the voluntary certification scheme, and comply with a number of criteria around messaging, delivery methods and a commitment to practitioner training. This strategy proposes the introduction of a similar approach in Northern Ireland. Once in place, consideration must be given to additional resources for schools to buy-in training from approved trainers.

**Commitment 3: We will develop evidence-informed quality standards for online safety:**

**Summary of key actions:**

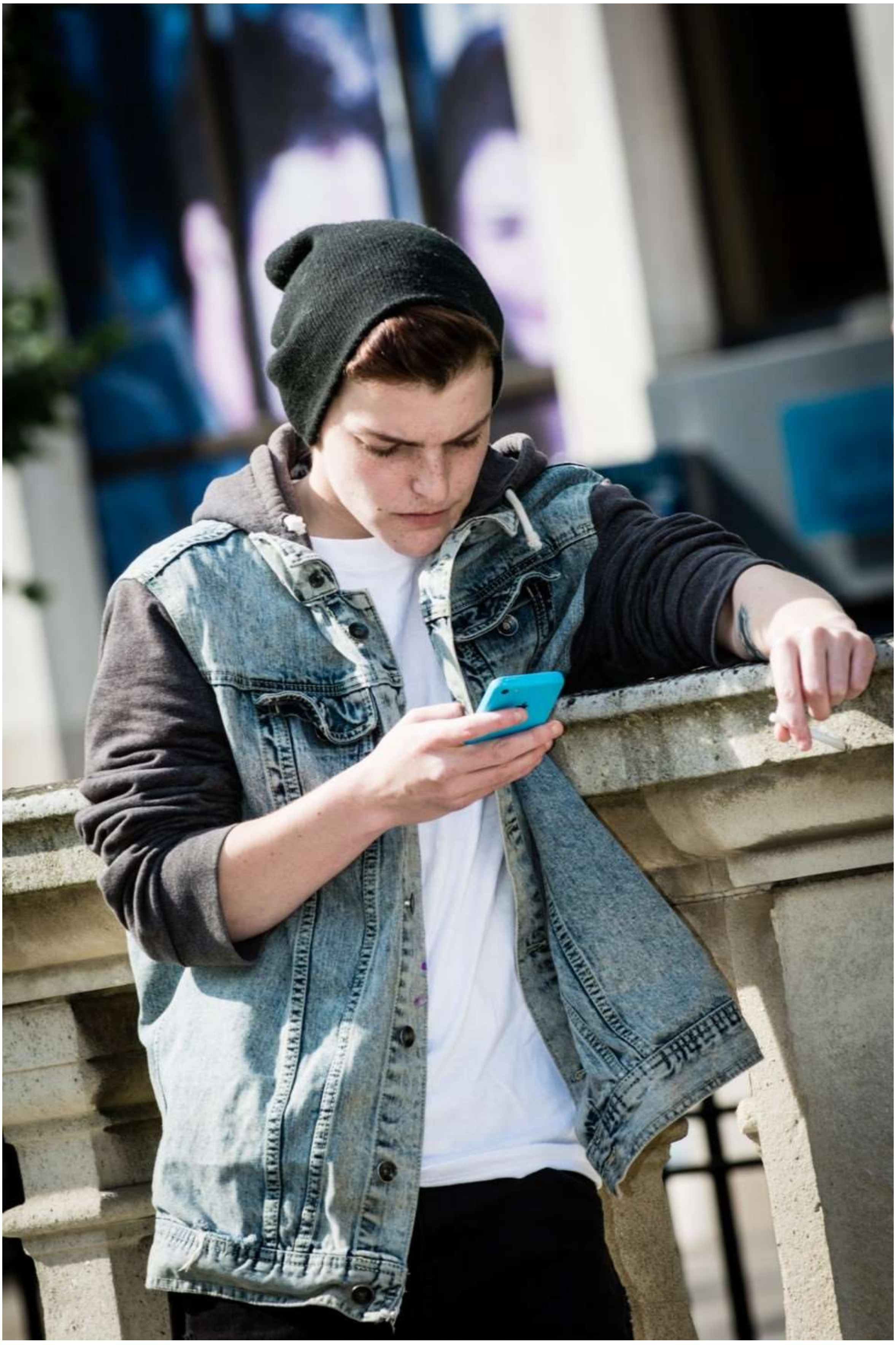
- Understanding the scale of the problem through research and data collection.

- Strengthening self-assessment processes for online safety.

- Introduction of an accreditation scheme for online safety training delivery organisations.

# Summary: key commitments to action through the Online Safety Strategy

| Outcomes | All children and young people are safe and well online.<br>All parents and carers are supporting their children to stay safe and well online.<br>All those working with children and young people are supporting them to stay safe and well online.<br>All those providing services for children & young people are supporting them to stay safe and well online.<br>All children and young people are equipped to keep themselves and others safe and well online. | | |
|---|---|---|---|
| Commitments to action | 1. We will create a sustainable online safety infrastructure for Northern Ireland. | 2. We will educate children and young people, their parents and carers and those who work with them. | 3. We will develop evidence-informed quality standards for online safety provision. |
| Areas of activity | • Developing a central repository for online safety information and facilitation of signposting.<br>• Strengthening links between NI & wider UK and global online safety structures.<br>• Developing a consistent approach to online safety in schools through strong departmental direction and enhanced education for schools on technical provision. | • Developing a consistent approach to online safety messages for children, young people, parents & carers, and practitioners.<br>• Embedding a culture of online safety within schools, colleges and child and youth services and organisations.<br>• Skilling up practitioners who work with children, young people and families. | • Understanding the scale of the problem through research and data collection.<br>• Strengthening self-assessment processes for online safety.<br>• Introduction of an accreditation scheme for online safety training delivery organisations. |



# Making a difference: Delivering this Online Safety Strategy for Children and Young People

A three year action plan 2020-2023 will be developed to support this strategy.  The action plan will be reviewed annually by the SBNI with a report produced for the NI Executive. To support this, governance and accountability structures will be put in place, as set out in figure 3 and summarised below.

## Developing governance and accountability structures

**SBNI** will take the lead as central coordinating body with responsibility for online safety.

The **Child Protection Senior Official's Group (CPSOG)** was established in September 2018 to address cross-cutting child protection issues which require cross-departmental input and coordination.  The CPSOG meets on a quarterly basis and is chaired by the Department of Health.  Its standing membership comprises representatives from the Departments of Education, Justice and Finance.   Representation from other NI government departments may be requested should a specific issue arise which extends beyond the remit of core member departments.  The CPSOG will take oversight of the Online Safety Strategy as a cross-cutting child protection issue.

SBNI currently hosts an **e-Safety Forum**, comprising representatives from statutory, community and voluntary sector children and youth organisations.  Such a forum has a critical place in a functioning online safety infrastructure for Northern Ireland.  Membership, chair arrangements and Terms of Reference for this forum will be reviewed regularly to ensure they remain representative and fit for purpose, and mechanisms will be put in place to support joint working and a two way flow of information between this and other key groups within the accountability structure.  The voices of practitioners, parents/carers and children and young people will be represented at the forum through its members.

The **Department of Health** currently sits on the **UKCIS**, along with representatives from the other devolved nations.  Additionally, the SBNI is delighted to have UKCIS representation on the e-Safety Forum to advise on the availability of new resources and developments. Since September 2019 a member of the e-Safety Forum has also become a member of UKCIS's Education Working Group which meets on a six weekly basis. This membership further develops links across the four nations and promotes cross jurisdiction learning, as well as ensuring that appropriate links can be made with industry representatives and internet providers.

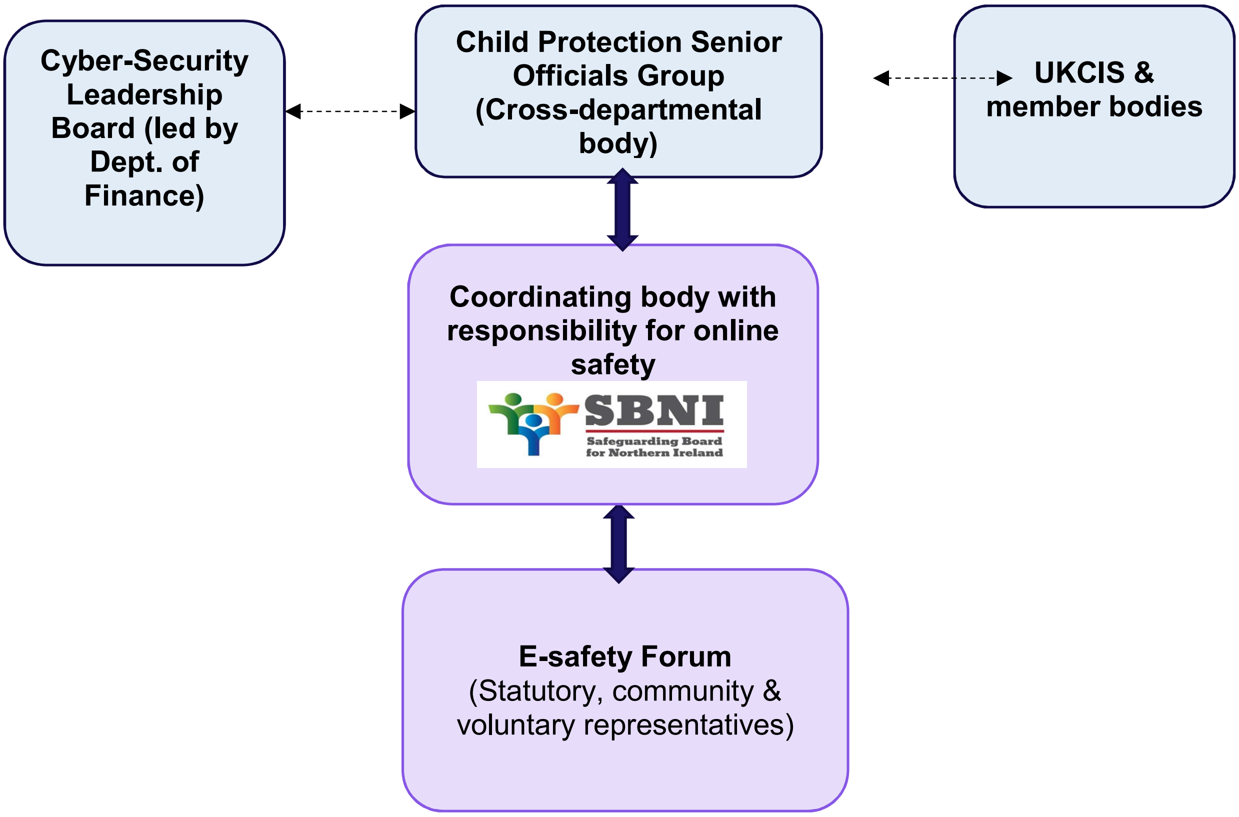

Cyber-Security Leadership Board (led by Dept. of Finance)
Child Protection Senior Officials Group (Cross-departmental body)
UKCIS & member bodies
Coordinating body with responsibility for online safety
SBNI
Safeguarding Board for Northern Ireland
E-safety Forum
(Statutory, community & voluntary representatives)

**Figure 3: Governance and accountability structures**

## How do we know we're making a difference?

### Measuring impact: the Outcomes Based Accountability process

In line with the recent government commitment via the draft Programme for Government 2016-2021, an Outcomes Based Accountability (OBA) approach will be used to measure the impact that this strategy is having on children, young people, parents, carers, practitioners and the wider population. Key definitions include:

**Population accountability:** this considers the condition of well-being of whole populations in a community, city, county, region or country. In relation to this strategy, the condition would be that all children and young people in Northern Ireland are safe and well online.

**Outcome:** a clear statement of the condition of wellbeing that we want to achieve for our population e.g. *all children and young people are safe and secure online.* By their very nature, these outcomes will be quite broad and multi-dimensional and cannot be achieved by a single organisation, service or programme working in isolation. Rather, it takes sustained, collaborative and concerted action by many organisations, services and programmes working alongside key stakeholders.

**Indicator:** a measure used to quantify the achievement of this population outcome, *e.g. recorded number of crimes against a child or young person that include an online element.*

The population outcomes targeted by this Online Safety Strategy for Children and Young People are set out on page 32 of this strategy. The first step in moving forward with this strategy will be to develop an outcomes framework, including selection of appropriate indicators, and to use the 'Turning the Curve' process set out in the OBA approach to develop an action plan. In the first instance, a number of suggested indicators to demonstrate impact have been identified below. It is important to note that many of these are not currently collected routinely (marked with*); a key part of the OBA process will be to develop plans to collect data once appropriate indicators have been finalised.

**Primary outcome: All children and young people are safe and well online.**

**Preliminary indicators may include:**

- #% (number and percentage) of online safety related crime involving children and young people*.
- #% of online safety incidents reported (to schools, colleges, youth and community organisations, and via CEOP, Police 101 and other core reporting facilities)*.
- #% of children and young people citing social media as a contributory factor to self-harm or poor mental health.

**Secondary outcome 1: All parents and carers are supporting their children and young people to stay safe and well online.**

**Preliminary indicators may include:**

- #% parents/carers reporting that they have the skills and knowledge they need to keep their child safe*
- #% parents/carers who report knowing where to access support and information to keep their children safe online*.
- #% parents/carers who have attended online safety training in the past year*

**Secondary outcome 2: All those working with children and young people are supporting them to stay safe and well online.**

**Preliminary indicators may include:**

- #% of those working with children and young people reporting that they have the skills and knowledge they need to keep children and young people safe online*
- #% of schools/youth organisations using a self-assessment tool
- #% of those working with children and young people who have attended online safety training in the past year.*

**Secondary outcome 3: All those providing services for children & young people are supporting them to stay safe & well online**

**Preliminary indicators may include:**

- #% local businesses who have taken steps to strengthen safety of any online elements of their service

**Secondary outcome 4: All children and young people are equipped to keep themselves safe & well online**

**Preliminary indicators may include:**

- #% children and young people who feel confident that they are safe when accessing the online world.*
- #% children and young people who report having successfully accessed support if needed;
- #% of children and young people who report being happy/satisfied that the support structures responded effectively to meet their needs and concerns;

**Performance accountability:** this describes how well particular services or programmes perform and whether or not they are achieving the outcomes they are supposed to be achieving. Each programme or service will have a set of performance measures which relate to whether programme/service participants are any better off as a result of participating, e.g. how many participants on an online safety training programme feel they now have better skills to keep themselves safe online.

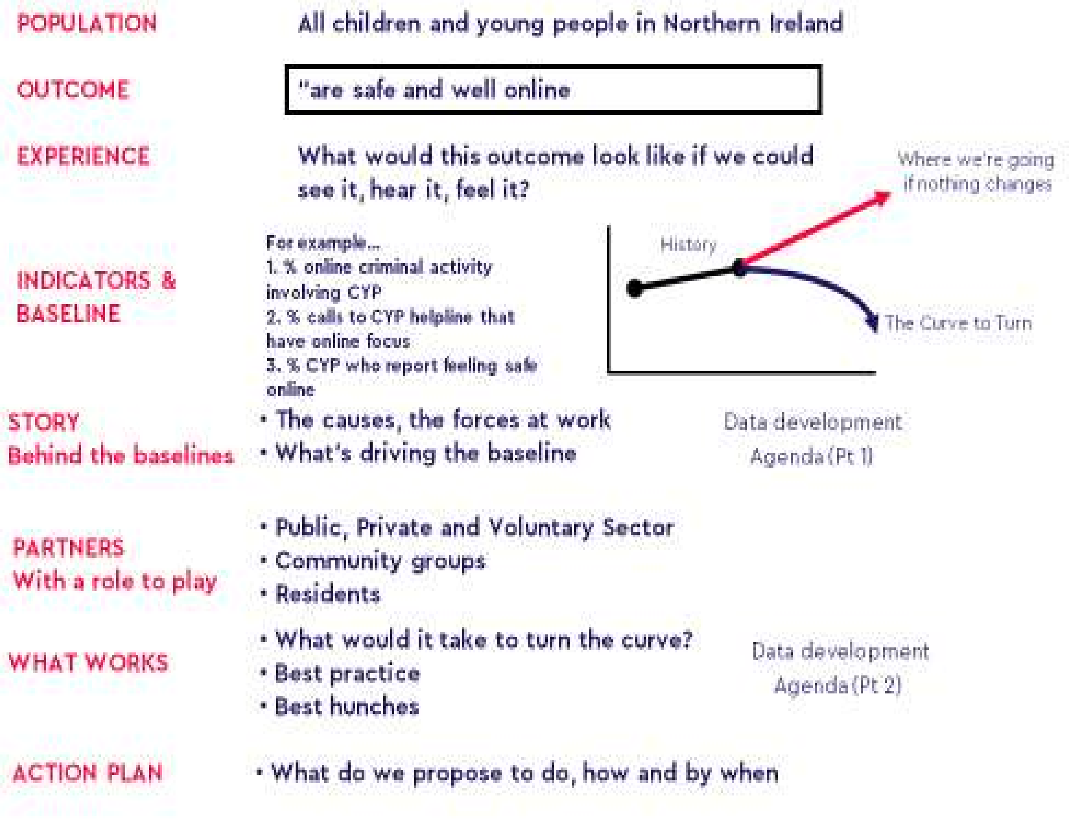
**Performance measure:** These are measures of how well an individual programme or service is performing. This is measured using three questions:

- How much did we do?
- How well did we do it?
- Is anyone better off?

Once an action plan has been finalised, performance measures must be developed for each key action in order to demonstrate impact of actions and their contribution to turning the curve on the population level indicators.

### Turning the Curve process

Moving forward, relevant indicators will be refined through the full implementation of the OBA 'Turning the curve' process (figure 4 below). We already know that baseline data on the impact of the online world on children and young people in Northern Ireland is scarce; a key part of the Turning the Curve process will therefore be the identification of a data development agenda to ascertain further data that we need to collect in order to measure impact. Performance measures must also be developed to measure impact of any resulting actions and their contribution towards the overarching



POPULATION — All children and young people in Northern Ireland

OUTCOME — "are safe and well online

EXPERIENCE — What would this outcome look like if we could see it, hear it, feel it?

INDICATORS & BASELINE — For example...
1. % online criminal activity involving CYP
2. % calls to CYP helpline that have online focus
3. % CYP who report feeling safe online

STORY Behind the baselines
- The causes, the forces at work
- What's driving the baseline

Data development Agenda (Pt 1)

PARTNERS With a role to play
- Public, Private and Voluntary Sector
- Community groups
- Residents

WHAT WORKS
- What would it take to turn the curve?
- Best practice
- Best hunches

Data development Agenda (Pt 2)

ACTION PLAN
- What do we propose to do, how and by when

outcomes. This strategy is a ‘live’ document; the outcomes, indicators and actions will be reviewed using the Turning the Curve methodology on an annual basis.

**Figure 4: Steps to Turning the Curve**

# References

Barnardo's NI (2018) Connections- Parenting infants in a digital world
http://www.barnardos.org.uk/connections-parenting-infants-in-a-digital-world.pdf

Bronfenbrenner, U. (1979) The ecology of human development: experiments by nature and design. Cambridge, MA. Harvard University Press.

CEOP 'Think u know'
https://www.thinkuknow.co.uk/parents/articles/Looked-after-children-Specific-risks/

Cerebra (2012) Learning disabilities, autism and internet safety: a parent's guide.
http://www.parentsprotect.co.uk/files/learning_disabilities_autism_internet_safety_parent_guide.pdf

Children's Commissioner (2018) Who knows what about me? A Children's Commissioner report into the collection and sharing of children's data. England: Children's Commissioner

https://www.childrenscommissioner.gov.uk/wp-content/uploads/2018/11/who-knows-what-about-me.pdf

Davies S.C., Atherton F., Calderwood C., McBride M. United Kingdom Chief Medical Officers' commentary on 'Screen-based activities and children and young people's mental health and psychosocial wellbeing: a systematic map of reviews'. Department of Health and Social Care (2019).
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/777026/UK_CMO_commentary_on_screentime_and_social_media_map_of_reviews.pdf

Department for Children, Schools and Families, and the Department for Culture, Media and Sport. *Safer Children in a Digital World The Report of the Byron Review*, 2008 [Online] Available from
http://webarchive.nationalarchives.gov.uk/20130401151715/http://www.education.gov.uk/publications/eOrderingDownload/DCSF-00334-2008.pdf

Department of Education (2018) Statistical Bulletin 2018/2 Annual enrolments in school and in funded pre-school education in Northern Ireland 2017/18 https://dera.ioe.ac.uk/31137/1/DE-enrolment-stats-bulletin-revised-feb-2018.pdf

Department of Health (then DHSSPS) (2014) Guidance To Safeguarding Board For Northern Ireland. [Online] Available from:
https://www.dhsspsni.gov.uk/sites/default/files/publications/dhssps/sbni-guidance-may2014.PDF

Department of Health (2016) Co-operating to Safeguard Children and Young People in Northern Ireland. (March 2016) [Online] Available from: https://www.health-ni.gov.uk/publications/co-operating-safeguard-children-and-young-people-northern-ireland

Five Rights Foundation https://5rightsfoundation.com/about-us.html

Five Rights Foundation 'Towards an internet safety strategy' https://5rightsfoundation.com/static/5rights_Towards_an_Internet_Safety_Strategy_FINAL.pdf

Five Rights Foundation 'Disrupted Childhood Report'

https://5rightsfoundation.com/static/5Rights-Disrupted-Childhood.pdf

HM Government (2019) Online Harms White Paper. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

Information Commissioner's Office (2019) Age-Appropriate Design: a code of practice for online services. Consultation Document. https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-public-consultation.pdf

Livingstone (2017) Children's online activities, risks and safety: A literature review by the UKCCIS Evidence Group https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650933/Literature_Review_Final_October_2017.pdf

Munro, E.R. (2011) The protection of children online: a brief scoping review to identify vulnerable groups. Childhood Wellbeing Research Centre.

NIYF, Belfast YF & Include Youth (2018) Elephant in the Room http://www.niyf.org/wp-content/uploads/2018/12/ELEPHANT-IN-THE-ROOM-A4-V2_.pdf

NSPCC (2019) How safe are our children?
https://learning.nspcc.org.uk/media/1747/how-safe-are-our-children-2019.pdf

OFCOM (2019) Children and Parents: Media use and attitudes report. https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf

Safeguarding Board for Northern Ireland: The Safeguarding Board (Northern Ireland) Act 2011 [Online] Available from: http://www.legislation.gov.uk/nia/2011/7/contents

Safeguarding Board for Northern Ireland Strategic Plan 2018-2022. [Online] Available from: https://www.safeguardingni.org/sbni-strategic-plan-2018-2022

Stonewall (2014) Staying Safe Online.
https://www.stonewall.org.uk/sites/default/files/staying_safe_online_guide.pdf

UKCCIS (2018) Education for a Connected World.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/683895/Education_for_a_connected_world_PDF.PDF

UK Chief Medical Officer (2019) 'Commentary on screen based activities and CYP mental health and psychosocial wellbeing: a systematic map of reviews'
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/777026/UK_CMO_commentary_on_screentime_and_social_media_map_of_reviews.pdf

United Nations (1989) *United Nations Convention on the Rights of the Child (UNCRC)*, Geneva

World Health Organisation (2019) Guidelines on physical activity, sedentary behaviour and sleep.
https://apps.who.int/iris/bitstream/handle/10665/325147/WHO-NMH-PND-2019.4-eng.pdf?sequence=1&isAllowed=y

Young Minds (2016) Resilience for the digital world.
http://www.youngminds.org.uk/assets/0002/5852/Resilience_for_the_Digital_World.pdf

# Appendix 1: Summary of stakeholder engagement

The strategy development has been supported by a wide range of people. Some of these have been involved throughout the process, including the Project Board, Parent Teacher Advisory Group and the Young People’s Advisory Group. Others have contributed through participation in the various research activities, or through responding to the consultation.

## Online Safety Project Board

The following representatives have overseen the development of the strategy as members of the Project Board. (Please note that representation from some departments/organisations has changed through the course of strategy development)

| Name | Organisation | Name | Organisation |
|---|---|---|---|
| Eilis McDaniel (Chair) | Department of Health | Kathryn Anderson | Education Authority |
| Angela Kane | Department of Education | Stephen Wilson/ Zoe McKee / Gary McDonald | Police Service NI |
| Helen McKenzie/ Teresa McAllister | Safeguarding Board NI | Colin Reid/ Orla O’Hagan | NSPCC |
| Alasdair MacInnes | Department of Health | Steven McNeill | South Eastern Health and Social Care Trust |
| Michael McArdle | Department of Health | Celine McStravick | National Children’s Bureau |
| John Noble/ Shauna Mullan | Department for the Economy | Claire Dorris | National Children’s Bureau |
| Martine McKillop/ Carol Gordon | Department of Justice | Derek McDowell/ Shane McKinney | DAERA |

| Young People’s Advisory Group | Parent Teacher Advisory Group |
|---|---|

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| David | Roisin | Niamh | Aoife | Joan O’Kane | Ciara Cassidy | Michelle McParland |
| Michael | Ciara | Alex | Jenni | Mhairi Hill | Gerard McStocker |  |
| Kalem | Jack | Emma | Ana | Lee Kelly | Charlie Tuxworth |  |
| Harry | Edward | Ryan | Samantha | Siobhan Matthewson | David Kennedy |  |
| Tara | Evan | Anthony | Emma | Roisin Rocks | Isobel McKane |  |

**Stakeholder interviews (carried out early 2016)**

| Organisation |  |  |  |
|---|---|---|---|
| Safeguarding Board NI | RQIA | NHSCT | Southern Regional College |
| Department of Health | Parenting NI | SHSCT | INEQE |
| The Executive Office | VOYPIC | WHSCT | Wayne Denner |
| Department of Education | Fostering Network | CYPSP | iTeach |
| Department of Justice | Mencap NI | NSPCC | Equiniti |
| Department for the Economy | Kinship Care NI | Sport NI/Child Protection in Sport Unit | Presbyterian Church in Ireland |
| DAERA | Nexus NI | C2K NI | Catholic Church in Ireland |
| Department for Communities | Rainbow Project | Libraries NI | Girl Guiding Ulster |
| Youth Justice Agency | Belfast Metropolitan College | Arts Council NI | Radar NI |

| | | | |
|---|---|---|---|
| NI Anti-Bullying Forum | Northern Regional College | PSNI | Family Friendly Wi-Fi |
| Belfast Health & Social Care Trust | South East Regional College | | |

**Focus groups:**

| **Teacher focus groups: (carried out early 2016)** | Venue | Meeting with: | Number of attendees |
|---|---|---|---|
| | Education Authority | Chief Education Welfare Officers | 5 |
| | St Killian's College | Larne Area Learning Community (Including Larne High School, Larne Grammar School, St Killian's College) | 5 |
| | Sacred Heart College, Newry | Newry Area Learning Community (including Abbey Christian Brothers Grammar School, Newry High School, Newtonhamilton High School, Our Lady's Grammar School, Sacred Heart Grammar School, St. Coleman's Boys Grammar School, St. Columban's College, Kilkeel, St. Joseph's Boys High School, | 15 |

| | | | |
|---|---|---|---|
| | | St. Joseph’s High School, St. Louis Grammar School, St. Mark’s High School, St. Mary’s High School, St. Paul’s High School) | |
| | St Fanchea’s College | Fermanagh Area Learning Community (including Devenish College, Enniskillen Royal Grammar School, Erne integrated College, Mount Lourdes Grammar School, St. Aidan’s High School, St. Fanchea’s College, St. Joseph’s College, St. Kevin’s College, St. Mary’s College, Irvinestown, St. Mary’s High School, Belleek, St. Michael’s College) | 11 |
| **Young people’s focus groups:** | Venue | Meeting with: | Number of attendees |
| | Belfast | YP Advisory Group | 17 |
| | Derry | Rainbow Project | 10 |
| | Belfast | Action Deaf Youth | 7 |
| | Dungannon | St Patrick’s Academy | 10 |

|  |  |  |  |
|---|---|---|---|
|  | Belfast | NEETS Youth Forum | 3 |
|  | Belfast | Include Youth | 2 |
|  | Enniskillen | Include Youth | 2 |
|  | Belfast | Arthritis Care | 6 |
| **Parent focus groups:** | Venue | Meeting with: | Number of attendees |
|  | Jordanstown | Jordanstown Special School | 4 |
|  | Portadown | Blossom Sure Start (BME Group) | 14 |
|  | Belfast | Colin Early Intervention Community | 7 |
|  | Belfast | Open call to parents/carers | 5 |
|  | Belfast | Orangefield PTA | 18 |
|  | Belfast | Shankill Zone | 1 |

**Consultation engagement activities (April 2019)**

| **Organisation** | **Activity** |
|---|---|
| Children’s Law Centre | Direct engagement with children and young people |
| NSPCC | Direct engagement with children and young people |
| Barnardo’s Sixth Sense Project | Direct engagement with children and young people |
| East Belfast primary ICT Cluster (Orangefield Primary School) | Parent and teacher engagement |

| | |
|---|---|
| Special School Area Learning Community (Lisnally Special School) | ICT Coordinators from 5 special schools; parents and teachers. |

# Appendix 2: Summary of stakeholders feedback

## Feedback during initial development phase:

**Young people:**

*‘Parents are nervous as they don’t know too much about [the internet] and because there has been a lot of stories like cyber-bullying’.*

*‘My family over-exaggerate the dangers a lot. I will be laughing at something and they will be going: “Who took that photo, who is that etc.”’*

(Discussing designated teacher) ‘*They are the high up teachers, the ones responsible for child protection and things like that and I would not necessarily want to go to one of those; they don’t choose the 25 year old teachers who get what you are going through, it is the 50 year old ones who have been teaching so long they forget they have been pupils’.*

**Parents/carers**

*‘I try to give them trust and not question. I keep the Xbox in the living room but still don’t feel like I’m in control of what they’re watching on their phones or tablets. I try to read their behaviour when I go in to check but they’re exposed to so much I don’t know how to control what they see’.*

*‘I’m very strict with my teenagers about age restrictions on games but my husband isn’t so it makes it very hard’.*

**Policy makers**

*‘We can’t consider e-safety in a silo. It’s all part of the wider safeguarding focus with particular links to Child Sexual Exploitation’.*

*‘There is a wide range of messages out there, including the ‘scaremongering’ approach. We don’t want to stop anyone doing what they are doing, but we need to standardise messages, share good practice and identify key themes and issues then people can make it their own’.*

**Practitioners:**

*‘We tend to be reactive to specific issues so at the moment there would be huge things in our school around Snapchat. But we are never prepared for it. It is always after the event, unfortunately’.*

(Discussing online safety training) *‘The parents you want to target are not coming. It is the parents that come that you know you have no worries. They are the ones that are sitting in front of you’.*

(Discussing school policies) *‘There is pretty much nothing in place, really, if I am honest about it. Apart from acceptable use of internet within a closed system anyway, so it is entirely pointless. But it is just a box ticking exercise. It is just paperwork. It is not actually affecting having our kids make good decisions online, really, at this stage’.*

**Key issues raised by stakeholders are summarised below:**

## Children and young people

- Think they know enough to keep themselves safe online but yet often think that their friends don't.
- Want to know the consequences of their actions rather than being told not to do something.
- Know who to go to in school if they have a problem, but would rather talk to their friends than a teacher.
- e-safety messages vary from school to school, as does the way of delivering the messages.
- Want to know that if they do report something, their concerns are taken seriously.
- Most say they know more than adults about 'tech stuff'.

## Parents/carers

- Want e-safety messages to be real life and hard hitting.
- Think e-safety training should be for the wider family, including grandparents.
- Need to set a good example for children with their own online behaviour.
- Think that children know more than adults about technology.
- Many parents ignore age restrictions and set their children up on social media etc.
- Fears include rapidly changing risks, in particular on health and wellbeing.

## Policy makers

- Departments find it difficult to collaborate under current structures, particularly as there are no facilities to share resources.
- Strategic guidance would help prioritise e-safety, however it will still lie within a safeguarding remit.
- Would like a much stronger evidence base on what works to protect children and young people online, to inform spending.
- e-Safety Strategy should be aligned with new Children and Young People's Strategy and other emerging relevant strategies

## Practitioners

- Too many conflicting messages and a lack of guidance on which training programmes to 'trust'. A prescribed list of aproved trainers would be useful.
- Little resources available to fully embed e-safety within a school or organisation & keep up to date on emerging issues.
- e-safety should be relevant to all practitioners working with children and young people yet it's hard to get buy-in from most.
- Concerned at possible criminalisation of young people for e-safety incidents such as sexting.
- A flexible and tiered approach is essential to meet the needs of all children and young people.

## Children and young people

- Feel like there are too many restrictions and they are missing out on opportunities.
- Most young people have online friends they don't know in real life, and many have met up with them, so they think that many of the e-safety messages are out of date.
- Phones are the most popular device and young people access the online world round the clock.
- Young people think there are no such things as safe or unsafe apps, it's about knowing how to use them.
- Teaching young people about e-safety should be fun and interactive and by someone they can relate to.

## Parents/carers

- Don't really understand the different apps and find it hard to keep up.
- Think that the internet gives children and young people a false reality to live up to and adds to their pressures.
- There is so much information out there on e-safety that it is hard to know which to trust.
- Parents more likely to set time restrictions and worry that their children are using the internet late at night.
- Often e-safety training focuses on the negatives and makes parents' fears worse.

## Policy makers

- Want to see a balance between restricting children and young people's access where appropriate and educating them to stay safe.
- e-safety must be strongly represented in inspection procedures across all settings working with children and young people.
- e-safety training and support must take a child rights approach.
- Departments don't have the capacity, resources or remit to monitor individual organisations, programmes or services.

## Practitioners

- It's hard to separate e-safety from wider safeguarding, particularly in recording incidents.
- Schools and youth organisations find it hard to engage parents/carers in e-safety training.
- Many find it hard to define 'right' or 'wrong' in terms of online access and don't have sufficient guidance to make an informed decision.
- Budgets are extremely tight and capacity often at the limit within services, therefore it's difficult to fit in e-safety without dedicated resources when other priorities must take precedence.

## Consultation feedback

**Vision:**

*"We agree with the vision and like that the positives of being online are listed before the negatives, which is important."*

*"We welcome the emphasis on facilitating young people's use of the internet in a positive way while staying safe online."*

*"We welcome the vision and that it recognises the benefits of the digital environment."*

**Objectives:**

*"Maybe merit in referencing 'empowering young people and their parents'."*

*"Doesn't mention 'protecting children'".*

*"Objectives should include a focus on allowing the voices of children and young people to be heard."*

*"Mental health and well-being with regards to technology [could be included]."*

**Definition:**

*"We consider 'e-safety' outdated terminology… 'Digital safeguarding' rather than 'e-safety' may be more apt."*

*"[The definition] places too much responsibility on the user/young person."*

*lan"Whilst there are a variety of terms, the more commonly referred to title is now 'online safety' rather than e-safety."*

**Outcomes:**

*"There should be an outcome relating to a change in behaviour of internet providers/platforms."*

*"Internet providers/companies need to be included in the Strategy."*

*"I think this is a great step forward."*

**Core principles:**

*"Need restrictions on what young people and children can access online."*

*"Greater emphasis on responsibility of parents of younger children is needed."*

*"I still believe that certain aspects of the online world need to be restricted…"*

**Pillars for action:**

*"The concern would be over evidence-informed quality standards for e-safety due to technology changing so rapidly… how will this be updated or monitored?"*

*"The concept of a consistent approach to e-safety in schools is very worthwhile."*

*"I would raise the question about the cost implication for all this to schools without them receiving additional funding."*

*"Research into e-safety needs to be much broader than a statistical count of incidents – particularly as many incidents will not be formally reported and recorded, or are seen as too 'everyday' to be raised despite having a harmful impact on a child or young person."*

*“We strongly agree with the areas for action, however there will need to be significant resources behind these to be able to take action”.*

**Safeguarding Board for Northern Ireland**
The Beeches
12 Hampton Manor Drive
Belfast BT7 3EN
Tel. 02895 361810
www.safeguardingni.org
Twitter: @safeguardingni

**National Children's Bureau**
The NICVA Building
61 Duncairn Gardens
Belfast
BT15 2GB
Tel: 028 9089 5006

www.ncb.org.uk/northernireland
Twitter: @ncb_ni_tweets

**Prepared by the National Children's Bureau (NCB) on behalf of the Safeguarding Board for Northern Ireland (SBNI)**