KEEPING CHILDREN SAFE ONLINE

By Alex Green, Clare Wilkins and Grace Wyld
with contribution from Cliff Manning
July 2019

CONTENTS

FOREWORDS

Chris Ashworth: Head of Public Benefit, Nominet

Welcome to our second Discovery Paper in the series that explores the social issues facing young people today. ‘Keeping Children safe online’ looks in detail at the online education and support structures surrounding young people at a critical point in the wider debate concerning online harms and has been undertaken to inform Nominet’s ambition to improve the lives of one million young people a year by 2020. The paper reflects on the gap between provisions and needs, the gap between emerging thinking and the real-world application, and the gap between expectations of parents or carers and the young people they are seeking to protect.

Today, a young person’s life is a complex combination of the on and offline worlds. Has our understanding of, and approach to safety, education and resilience-building evolved at the same pace as the fundamental shifts in how society engages with one another? What were once ‘analogue risks’, such as bullying, and harassment are not just mimicked online but exaggerated and altered—forcing us to reassess how we respond. Improvements in education addressing an issue are normally finessed and fine-tuned over many decades as our understanding evolves. We haven’t had that luxury in the Internet safety domain but hope this Discovery Paper lends its weight to where we need to go next. Just as young people need to learn fast to thrive in a society that is increasingly digital-by-default, so must we.

Tris Lumley: Director of Innovation and Development, NPC

We often view the advent of digital as revolutionary. This is true. But the online world is simultaneously just another forum in which very old concerns and issues play out. This will be a familiar story for parents seeking to keep their children safe. The web creates spaces and mechanisms in which risks and harms play out differently from how most parents and teachers grew up. But it is also is just another 'space' in we should apply all our thinking about the juxtaposition of risks and harms versus opportunities and freedoms.

In this context, we believe charities and civil society should do two things:

- Incorporate their existing values, principles and practices into how they ensure digital technologies are used for maximum benefit against their missions. Are they using the web safely for their stakeholders, putting their own house in order, etc?
- Analyse and assess how these technologies are affecting their stakeholders, and put forward perspectives, insights, challenge and ideas into the policy arena to change the wider debate and policy direction.

At NPC we are always trying to ensure charities make best use of available technologies (be they evidence, data analysis, or digital technology) to deliver services effectively. We want charities to embrace policy debates, to represent the perspectives and insights of their constituents' lived experience, and to share their practitioners' expertise.

It’s great to partner with progressive tech organisations like Nominet who want landscape research to inform their own strategies and everyone else's. As the online safety field develops, we want to see much more of this landscape work. Things are changing fast through digital technology, so we all need a shared understanding of risks and opportunities if we are to succeed in helping those we exist to serve.

Vicki Shotbolt: CEO, Parent Zone

In the 13 years since Parent Zone began the rise of digital has had a significant impact on families. Much of that impact has been positive—some of it has been harmful—but all of it has created complex questions for children and those who support them.

It is heartening to see funders, delivery organizations and government taking a more holistic approach to online risk, harm and resilience. The support sector and policies have been slow to 'mature' in their approach and consequently, families have been left to navigate their way without sufficient support but responses are changing.

Parent Zone became a social enterprise because the funding opportunities available were very limited. We have had to develop a mixed-income model and learn how to work effectively with industry in order to achieve our mission. We have had many successes through this model but funding for tackling the social challenges caused by technology should not be left to industry alone. Building a more diverse and sophisticated funding environment is essential to ensure that the sector can meet the ever-growing range and complexity of needs.

Funding helps delivery but we must also hold ourselves accountable for what we deliver. In such a rapidly changing environment, it is essential that we constantly review, and improve, what we do and the ways that we do it—not to stay on trend—but to ensure that we actually meet our collective duty: to protect and support children now and in the future.

INTRODUCTION

How should children be supported to stay safe online?

Welcome to generation digital. A generation where 59% of 11 to 12 year-olds are on social media[1], and over one in three Internet users is a child[2]. But high levels of usage and confidence among today's children and young people do not necessarily translate to high levels of skill or capability in using online platforms safely.

We know the majority of children grow up feeling confident using technology and online platforms, and are often younger than the permitted age on many platforms. However, we also know that children do not necessarily possess sufficient critical thinking skills to be discerning about online content and behaviour as required to stay safe and flourish in a rapidly changing online environment. Children are not naturally awake to the potential risks found online, nor are they likely to be proactively critical about content they see. Children need help to grow into astute, critical and engaged digital citizens, with the skills and confidence to stay safe in an online world.

Children's lives are increasingly impacted by the rise of new technology. Alongside the considerable benefits and opportunities posed by the Internet come a wide range of risks. Risk is not the same as harm, but that doesn't mean risks should be ignored. Special attention needs to be given to transition points, such as when a child moves to a new school or gets their first smartphone, and online safety is everyone's responsibility.

There are major variations in the level and type of access to online services different children have, as well as their opportunities to access support to develop and flourish. Children may have shifting and complex vulnerabilities in the offline world, which can be exacerbated and added to when engaging online—especially when the online spaces they access are designed for adults. All children should therefore receive adequate support from the community of adults around them to help them safely engage online. And for this to happen, these adults must feel confident in providing that support.

How though, should children be best supported? Parents are increasingly worried about how to keep their children safe online, as are schools and government. It is obvious that online child safety practices are falling behind. The fluid movement between offline and online spaces and the interconnectedness of digital services means risk and harm are not easily 'located' in one online space, feature or behaviour. This 'mosaic effect' makes identifying and mitigating online risks a significant challenge for children, parents, professionals and the platforms themselves.

In response, the static 'rules and tools' approach is giving way to a more dynamic model, centred around building digital resilience and wellbeing. This approach, whilst acknowledging risks and potential harms, recognises the positive contribution technology and the online world can have on children's lives, the integral role it plays in their social world, and the positive way they can shape it.

This shift is important because it recognises four important truths:

1. Information alone will not achieve behavioural change.
2. Online risk does not necessarily translate to actual harm.
3. Online risks are almost universally an extension of offline risks.
4. Children need a consistent and confident community of support around them if they are to thrive and make the most of the opportunities offered by online engagement.

By involving children in efforts to equip them with the skills and capabilities they need, alongside better regulation and efforts to build a better Internet—where online platforms are one day safe by design—there is a far greater chance of achieving safe engagement with the online world.

In addition to shifting our approach, we also need to consider changing our language. The term 'online safety' is an adult-driven phrase burdened with associations of danger and the need for protection. It is not generally a term used by children and for some it may in fact be alienating. As a result, many initiatives are aimed at adults rather than children.

Children may be the ultimate beneficiaries of online safety efforts, but they are unlikely to be driving the agenda. As a sector, we need to recognise this tension and overcome it by involving children and supporting adults in the design and implementation of initiatives to keep them safe.

About this paper

This discovery paper, written by NPC in partnership with Parent Zone, is a sister paper to our report on Charities, young people and digital mental health services. We examine the landscape of online child safety support and education and what provisions exist to support them, with a primary focus on those aged 10-16. We focus on this age group because it is a critical time in a child's cognitive development and social interactions. As children move from primary to secondary school, they can experience disruption through introduction to a broader set of social norms. Many will also move on from monitored online usage on devices in the home, to having their own smartphone with potentially unlimited online access.

This paper is based on an extensive literature review and a series of interviews with experts in the field. We've designed it to be particularly useful to donors with an interest in funding organisations working in this space. In this paper we present:

- **Contextual information on children's online safety, including mapping significant risks and the current policy context.**
- **An overview of the types of online safety initiatives, along with key organisations and programmes.**
- **Analysis of the gaps and challenges in existing provision for online safety, education and support.**
- **Opportunities for charity sector funders to support improved online safety for children.**

We are grateful for the support of Parent Zone who have contributed the case studies presented throughout this paper. We would like to thank the following people for giving their time and expertise:

- David Presky, York House School.
- David Wright, South West Grid for Learning.
- Professor Emma Bond, University of Suffolk.
- Jay Harman, 5Rights.
- Will Gardner, Childnet International.

All quotes have been anonymised throughout this report.

CONTEXT: THE RISKS CHILDREN FACE ONLINE

Some key figures about children's online safety:

- In 2015, for the first time, children made up **1 in 3** of all global users of the Internet.[3]
- **94%** of 8 to 11 year-olds, **99%** of 12 to 15 year-olds and **99%** of 16 to 25 year-olds spend one or more hour(s) a day online and on their smartphones.[4]
- **Half** of secondary school pupils and over a quarter of primary school pupils have communicated with people they don't know using social media.[5]
- Around **one in ten** children who use the Internet aged 8-11 and almost twice as many (19%) aged 12-15 say they have encountered something online that they found worrying or nasty.[6]

How should we understand online risks and harms?

Children are at particular risk online

More than one in three Internet users is a child[7], and NSPCC findings suggest that 59% of UK 11 to 12 year-olds have social media accounts.[8] While children are often very confident using technology, this does not mean they have the capabilities, skills, critical thinking and emotional understanding needed to make good decisions or be discerning about the content they come across. The adult characterisation of generations who have grown up with digital technology as 'digital natives' can obscure the need to help children develop digital skills.[9]

There can be a dangerous gap between a child's ability to use a technology, and their critical understanding of how it works. For example, children might be proficient playing video games but unlikely to know that games often influence users to keep playing longer through persuasive design.[10] Depending on their stage of cognitive development, children may find it hard to think about the longer-term consequences of their online behaviour, and may be more likely to take impulsive action and seek immediate rewards online, for example through posting personal information.[11] Of course the same can be true of adults.

Many parents assume that their children, who have grown up with digital technology around them and are familiar with it, are inherently capable online. When they do realise the risks, parents and carers can often feel powerless to provide the same support to their child's digital life as they would in all other areas of growing up. The same is true for teachers and other professionals who provide critical emotional and social support.

This anxiety can undermine adult confidence in supporting children, resulting in children not receiving the guidance they need. Children's exposure to risk grows, whilst their opportunities to recover shrink. Adults must recognise this disparity between comfort and capability when it comes to digital. They must feel confident owning their role of ensuring children enjoy safe and productive engagement with their online world.

The Internet can enhance and extend risk, but risks are not solely online

Children have changing and complex vulnerabilities, both online and offline. Offline vulnerability to risk is a strong predictor of online vulnerability.[12] The online world can offer unrestricted access to a wide range of content, greater speeds and scales of interaction and an unrelenting persistence of communication unmatched in the offline world. This can enhance existing vulnerabilities, and expose new ones, even if such vulnerabilities are not obvious in the offline world.[13]

There is little evidence showing that online interactions in isolation are solely responsible for harm. Instead, risks are the product of multiple interacting factors, including:

- online and offline contexts;
- individual capabilities; and
- the functions and features of online platforms.

Taken together, these risks can lead to some children experiencing significant harm online. Addressing such harms in a meaningful way means looking beyond digital responses alone. Parents, carers, teachers, youth workers and policy makers will need to consider the context a child is living in, and the online and offline factors contributing to their harm. These must be addressed as a whole, using a holistic approach, rather than attempting to solve any one element in isolation.

All children, regardless of their offline vulnerabilities, require some level of support and protection appropriate to their age and development stage. We must recognise that their needs and vulnerabilities will change as they grow up. Such changes must be matched with varied and flexible skillsets and knowledge patterns to help children navigate emerging challenges and risks over time.

We need to balance the risks, harms and benefits of online use

In recent years, online safety has come under the spotlight, but even though risk does not necessarily lead to harm, intense media and policy attention has not always differentiated between them or the types of risk and harm. Whilst public attention is welcome, the small base of existing evidence on the specific mechanisms that cause harm[14] means more work is needed to improve our understanding of this area and how society should respond.

More evidence is needed to understand the true severity of certain risks in leading to harm. Research studies have investigated harm in relation to some aspects of health, sexual behaviour and bullying, but there is limited evidence on privacy-related or economic harms,[15] despite these being highlighted as significant concerns for children's online use.[16] There is also limited evidence about the prevalence of harms, with incidence rates derived from self-reported survey data showing great variability. For example, studies on cyber-bullying have reported rates ranging from 9% to 72%.[17] Better evidence would help us prioritise where to focus our attention and who is most effected by online harm, and it would improve the sectors ability to design impactful interventions.

The internet undoubtedly exposes children to risks, but it can also offer valuable benefits. Research with children shows they are generally very positive about their online experiences, and enthusiastic about being constructive digital citizens.[18] But while web platforms give opportunities to be content creators as well as consumers, unfortunately only a minority of children take these up.[19] Being passive receivers online excludes children from full participation in an increasingly digital public sphere.

We need to go beyond just building resilience against harms and go further in supporting children to develop their capabilities to engage constructively online. Furthermore, we need a broader sense of community resilience and to build a better, safer Internet which reduces exposure to harm in the first place.

How can we build resilience against risk?

Resilience is often described as an individual's ability to 'bounce back' from challenges, but true digital resilience is the ability to not just survive but thrive.[20]

We know the Internet can provide great benefits to children and young people, so it is important that resilience-building initiatives also help them to build the skills and capabilities they need to make the most of its opportunities.

Resilience isn't something that can be built by avoiding risk. Instead children need opportunities to practice evaluating and coping with risky scenarios in supportive and safe contexts.[21] Research has suggested that the use of online content filters to restrict risk can lead to reduced resilience.[22]

Resilience isn't a character trait that individuals have or don't have. Instead resilience is dependent on multiple environmental factors including home environment, digital skills and peer support.

This means we need to think about how to build resilience within communities; in peer groups, schools and families.

Categorising risk in a dynamic and rapidly evolving space

It can feel like government and civil society are struggling to keep pace when children quickly shift their attention to new platforms and features. Rather than focusing on the specific online platform, our understanding of risk needs to place children and their priorities at the centre. For instance, strategies specifically based on platforms such as Bebo (closed 2013) or Vine (closed 2017) would be ineffective today. The EU Kids Online project developed the following typology of risk, supported by a survey of over 9,000 children and young people:

- **Content:** what children see online.
- **Conduct:** what children do online.
- **Contact:** who children interact with online.

Children say they are most likely to encounter risk through content[23]

Content risks relate to scenarios where children are passive consumers of media and text. Content is the most significant risk identified by children, parents or carers. Despite this, only a minority of children (16% of 8 to 11 year-olds and 31% of 12 to 15 year-olds) report having seen something worrying or nasty online in the past year.

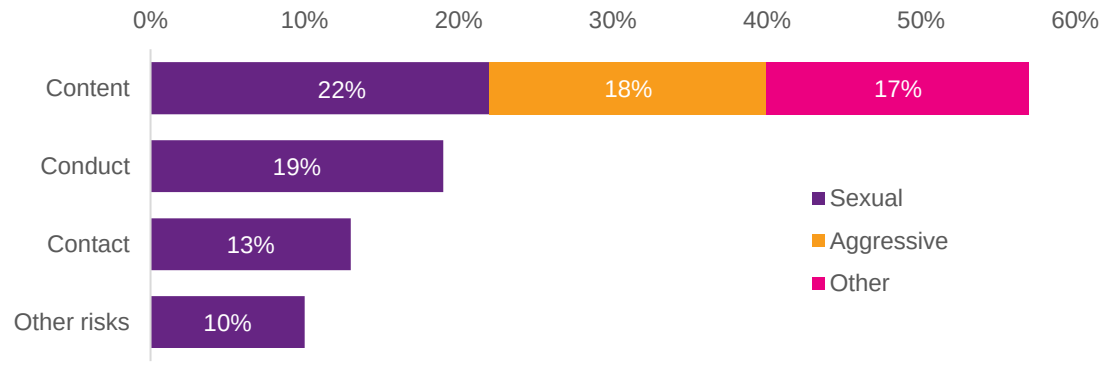


Figure 1: 9 to 16 year-olds in Europe who identified one or more risks online (n=9,636). *Source: EU Kids Online (Livingstone et al, 2014b)*[24]

And they are most likely to encounter harmful content on video sharing platforms

Despite the attention given to social media sites, children say they are most likely to encounter upsetting content on video-sharing sites like YouTube (32%), followed by other websites (29%), with social media platforms at only 13%. Youtube does have a children's version (Youtube Kids) but its usage is very low and instead children are encountering upsetting content on the adult site. Only 10% report encountering upsetting content in online games, but games often have far fewer controls for managing risk than social media platforms.[25]

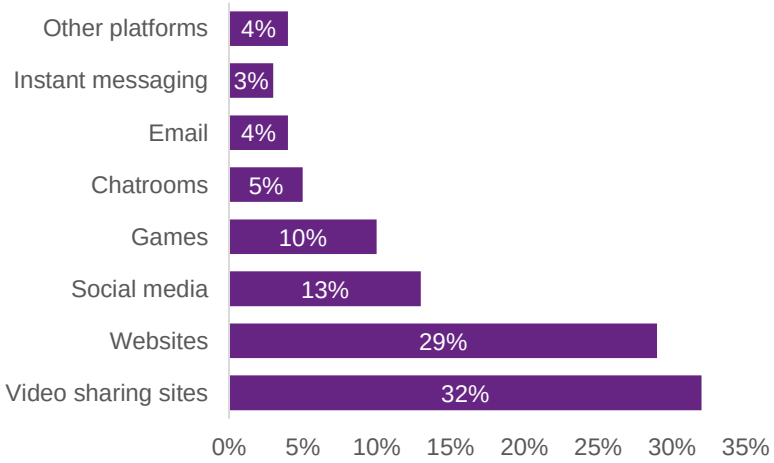


Figure 2: 9 to 16 year-olds in Europe who mentioned a platform when describing online risks (n=4,356). *Source:* EU Kids Online (Livingstone et al, 2014b)

Insights into the types of risks children encounter online

	Content Child as receiver (of content)	Contact Child as participant (adult-initiated activity)	Conduct Child as actor (perpetrators and victims)
Aggressive **(relates to violence and aggressive behaviour)**	Aggressive content includes depictions of violence, torture or attacks on people, or self-inflicted aggression, such as suicide related content. Of those children who had harmed with suicidal intent, 70% reported self-harm and suicide related Internet use.[26]	Aggressive contact includes being harassed or targeted online, or data being gathered online to enable offline attacks. 24% of children and young people have experienced harassment and hate online.[27]	Aggressive conduct includes perpetuating cyberbullying or circulating violent content. Face to face bullying remains more frequent than online, but a survey of children who had been cyberbullied suggests that 41% developed social anxiety, 37% developed depression, 26% had suicidal thoughts and 25% self-harmed.[28]
Sexual **(relates to sexual content and behaviour)**	Sexual content includes pornographic videos, text and other media. Older children and boys report seeing more sexual content online, but younger children and girls report being more upset by it.[29] Sexual content is experienced on and offline – 14% of children who have seen sexual content saw it online, 12% on TV, and 7% in print.[30]	Sexual contact includes abuse, exploitation and grooming. Grooming often spans platforms, luring children from public social media spaces to private channels, and can span international networks. In 2017, the Internet Watch Foundation accessed 80,319 confirmed reports of websites hosting or linking to images of child sexual abuse. 43% of the children in images were 11-15 years old, 57% were aged 10 or younger, and 2% were aged 2 or younger.[31]	Sexual conduct includes the creation and dissemination of sexual content, such as sexting, and risky behaviour around online dating. 15% of 11-16 year-olds in Europe have received sexual messages, and about a quarter of them had been upset by it.[32]
Values **(relates to content and behaviour that may influence values)**	Content risks related to values include exposure to extremist ideologies, racist, sexist and homophobic material. 82% of young people report seeing or hearing hate speech online.[33]	Contact risks related to values include online radicalisation and recruitment by organised criminal or terrorist groups. There is limited evidence on the scale of this problem, despite several high-profile media cases.	Conduct risks related to values include situations where children may be espousing extremist views, undertaking hacking or trolling.
Commercial **(relates to financial and commercial activity)**	Commercial content risks include online advertising or sponsored material which attempts to influence commercial choices. Younger children find it particularly difficult to recognise marketing content, especially when embedded in games or social media influencers.[34]	Commercial contact risks include cyberscams or being influenced to spend excessively, for example through in-app purchases within games. Children are also more likely to accept data use terms which put them at risk of data exploitation.	Gambling, content piracy and fraud. While traditional gambling is prohibited, children can experience similar interactions through 'loot boxes' in games or using 'skins' as virtual currency.

The policy context

UK Government agenda for online safety

Online child safety has grown in prominence in the UK policy agenda in recent years. The recent Online Harms White paper (April 2019) sets out a clear scope for government action in three categories:

1. Harms with clear definition.
2. Harms with less clear definition.
3. Underage exposure to legal content.[35]

The table in the appendix identifies the elements of the white paper specific to children, such as terrorist content and activity, modern slavery, incitement to violence, child sexual exploitation, harassment, and encouragement of suicide. To address these harms, the white paper proposes three strands of action:

1. Establishment of an independent regulator and statutory duty of care.
2. Development of technological solutions.
3. Greater empowerment of users.

The white paper makes few references to the role of the social sector in developing interventions and being part of building a safer Internet. It acknowledges a patchwork of initiatives, some of which have been promising. It is also worth noting that commercial harms, such as in-game gambling, personal data misuse or influence through embedded marketing, remain outside of its scope.

A statutory duty of care and independent regulator

The 2019 Online Harms white paper proposes establishing a statutory duty of care to make companies take more responsibility for the safety of their users, with compliance overseen and enforced by an independent regulator.

This would apply across a broad scope of companies that allow users to share or discover user generated content or interact with each other online, including social media platforms, gaming platforms, file hosting services, public discussion forums, messaging services and search engines. This has the potential to shift the power dynamic, placing greater responsibility for online safety onto tech companies.

The proposed regulator will have powers to:

- Require annual transparency reports, outlining the relevance of harmful content on platforms and the actions being taken to address them.
- Request information on how content is selected for users, including details of algorithmic decision making.
- Ensure that organisations operate an effective and easy-to-access complaints process where appropriate.
- Formulate codes of practice to guide organisations in fulfilling their legal duty.
- Issue fines and impose liability on individual members of organisations' senior management.

The UK Government plans further consultation on the development of an independent review mechanism, which might, for example, allow independent bodies to make 'super complaints' to the regulator in order to defend the needs of users. While the creation of an independent regulator with these powers represents the potential for a significant improvement in online safety, much depends on the implementation of these plans. The regulator will need to be sufficiently resourced and there must be enough political will to support it in the exercise of its powers.

Development of technological solutions

The white paper argues that the current balance of responsibility to stay safe online falls too heavily on users. To correct this imbalance, it states that companies should invest in the development of safety technologies and indicates that the independent regulator will work with industry bodies and other regulators to support innovation and adoption of safety technology.

The introduction of greater data privacy regulation has been criticised for providing a competitive advantage to large tech companies as they are better resourced to meet new requirements.[36] To make it easier for start-ups and small businesses to embed safety during the development or update of products and services, the government will also work with the industry and civil society to develop a safety by design framework.

This will link up with existing legal obligations around data protection by design from the GDPR[37] and secure by design principles from the Code of Practice for Consumer Internet of Things.

Empowerment of users

The UK Government is developing a new online media literacy strategy to ensure a coordinated approach to online media literacy education and awareness for children, young people and adults. This will be developed in consultation with major digital, broadcast and news media organisations, the education sector, researchers and civil society.

Alongside this, the regulator will also have broader responsibilities to promote education and raise awareness about online safety, and to promote the development and adoption of safety technologies to tackle online harms.

Case study: 5Rights Foundation

5Rights takes the existing rights of children and young people (under 18) and articulates them for the digital world. 5Rights is an example of how an organisation can shape regulation. It reflects a growing movement towards safety by design but also the importance of listening to the views of children, parents, carers teachers, academics, policy makers and the tech sector.

In 2018, following a call for evidence, the UK Information Commissioner's Office (ICO), produced an Age Appropriate Design Code, outlining the design standards providers of online services and apps used by children are expected to meet when they process their data. The code is a requirement of the Data Protection Act 2018, which supports and supplements the EU General Data Protection Regulation (GDPR). The code incorporates many features of the 5Rights Framework on the rights of children in the digital environment.

These include:

- The Right to Remove.
- The Right to Know.
- The Right to Safety and Support.
- The Right to Informed and Conscious Use.
- The Right to Digital Literacy.

INTERNET SAFETY INITIATIVES

Provision of services in this sector fall roughly into four broad categories of initiatives:

1. Education and awareness;
2. Coordination;
3. Helplines;
4. Content moderation and reporting.

Below we introduce some of the key initiatives. Particular examples of innovative or best practice in online child safety are also presented throughout this report.

There are plenty of resources, initiatives and information about 'online safety' available online or in person. It is not practical to identify and map every intervention. However, to provide an indicative overview of how provision is distributed, NPC reviewed significant initiatives currently available or operating in the UK, identifying 67 initiatives. The majority are focused on education and awareness (44). Of these, 33 resources were aimed at parents, carers, 18 at teachers and 16 at children.

Education and awareness

There are many initiatives providing education and awareness resources for children, parents, carers, teachers and professionals, including from NSPCC, Getsmartonline, and Parent Zone. Initial research by NPC identified in excess of 44 currently active.

ThinkUKnow

ThinkUKnow provides online safety resources for children and young people, parents and professionals. It is delivered by the Education team of NCA-CEOP, whose role is to tackle the sexual abuse and exploitation of children.

Internet Matters

Internet Matters is a not-for-profit funded by 16 industry partners, including BT, Google, Facebook and Instagram. It aims to be the 'go-to' resource for parents and provides a range of online safety resources.

South West Grid for Learning (SWGfL)

South West Grid for Learning is the lead partner in the UK Safer Internet Centre. It is a charitable trust working with schools and professionals to provide training and resources. It also develops technical solutions, including a child-friendly search engine and Internet services for schools.

Childnet

Childnet is a charity working with children, parents, teachers and professionals to deliver capacity building and training on online safety. It also provides resources through its website and runs a national youth leadership programme to enable young people to educate their peers.

Coordination

Coordination initiatives exist to link up services and sectors to better disseminate information, build commitment and support collaborative initiatives. Despite multiple initiatives in this area, the online safety sector remains relatively fragmented, as is discussed in the following section.

UK Council for Internet Safety

Expanding the scope of the former UK Council for Child Internet Safety, UKCIS is a collaborative forum for government, the tech sector and civil society. Current priorities include reviewing research on adult online harms, providing updated guidance to schools on sexting and evaluation of online safety provision.

WePROTECT Global Alliance

The WePROTECT Global Alliance was established by the UK Government in 2016 to address online child sexual exploitation and abuse (CSEA), with over 130 members including national governments, NGOs and tech companies. It aims to build global commitment, support national responses to CSEA and lead collaborative initiatives to develop interventions.

Insafe Network

Insafe is a network of national Safer Internet Centres across Europe, supported by the European Commission's Better Internet for Kids Programme and coordinated by European Schoolnet. Safer Internet Centres vary in terms of audience and objectives, but all deliver a mix of education, helpline and awareness initiatives, including the annual Safer Internet Day. In the UK, the Safer Internet Centre is a collaboration between the Internet Watch Foundation, Childnet and South West Grid for Learning.

Helplines

There are a limited number of dedicated online safety helplines operating in the UK. In contrast to other EU countries in the Insafe network, the helpline run by the UK Safer Internet Centre is to support professionals rather than children or carers. However, this is not to say that help for online risk and harms is not available through other channels.

Children, parents and carers and other supporting adults who are experiencing harm online or concerned about risk may contact other helplines and services such as TheMix. These broader helplines can play a vital role not just in providing support but in helping people manage, report or recover from online harms.

Professionals Online Safety Helpline (POSH)

Co-funded by the European Commission, POSH was set up in 2011 to help professionals working with children with online safety issues. It provides a signposting, advice and mediation service, with direct channels to tech companies to escalate concerns.

NSPCC and O2 Online Safety Helpline

Operated through a partnership between NSPCC and O2, this helpline provides advice for parents and carers on online safety, including advice on how to set up content controls. An accompanying website provides educational resources for parents.

Childline

Founded in 1986, and merged with the NSPCC in 2006, Childline provides a counselling service for children and young people through online chat, messages and a telephone helpline. Childline supports online safety issues as part of its broad offer. It also provides guidance resources on its website.

Content moderation and reporting

There are multiple initiatives for removing inappropriate content from platforms, including pre and post moderation by automated systems, users and platform staff. These are largely operated by platforms, but there are also independent services provided by the National Crime Agency's Child Exploitation and Online Protection command (NCA-CEOP), the Internet Watch Foundation and South West Grid for Learning.

'We reported them quite a few times…they didn't do anything about it.'

(Girl, 8 years old)[38]

Approximately seven in ten 12 to 15 year-olds are aware of online reporting systems, and nine in ten say they would tell someone if they saw upsetting content.[39] However, many children report not receiving a response or being disappointed with the outcome, leading to a lack of confidence that companies are taking their concerns seriously.[40] Whilst there are police run systems for reporting hate crime and other criminal activity, they have been designed by adults and therefore may not be intuitive for children.

Internet Watch Foundation (IWF)

The IWF is a not-for-profit funded by the European Commission and over 130 members from the tech sector. IWF provides services for content reporting, proactive search and removal of child sexual abuse content, and automated prevention of content sharing through a hash list of images and videos.

Platform reporting functions

Major social platforms, including Facebook, YouTube and Twitter, have facilities to report content. However, moderation action is based on individual platforms' content policies and moderation teams are often under-resourced. This has enabled the growth of large communities centred on racism and hate.

Case study: The UK Safer Internet Centre

The UK Safer Internet centre is a partnership between Childnet International and South West Grid for Learning (SWGfL) and the Internet Watch Foundation, co-financed by the European Commission. Their child exploitation and abuse reports play a vital role in providing expert advice, and makes it easier for anyone to report illegal child exploitation and abuse.

The UK Safer Internet Centre hosts Safer Internet Day. Held annually in the first week of February since 2004, Safer Internet Day is marked in over 140 countries, coordinated by the European Commission's Insafe and INHOPE network. More than 2,100 organisations and schools across the UK were involved in 2019, helping to inspire a national conversation about using technology responsibly, respectfully, critically and creatively.

The UK Safer Internet Centre is an important focal point for a range of guidance and initiatives. For example, the Research Highlight Series, compiled by the UK Council for Internet Safety Evidence Group, brings together the latest research findings in the field of child online safety with expert curated summaries.

WHAT ARE THE GAPS AND CHALLENGES?

1. Children have complex and shifting vulnerabilities

Online risk emerges from multiple factors, including complex interactions between individual capabilities, home, school and peer groups contexts and the opportunities of online environments. For some children, online environments can expose and enhance new areas of vulnerability, even if they are not exposed to particular risks offline.[41]

Offline vulnerability to risk is a strong predictor of online vulnerability, and the Internet provides a consistency of communication unmatched in the offline world.[42] Children experiencing family difficulties are often particularly vulnerable online.[43]

There are some common characteristics which are often associated with a higher level of vulnerability to online harms. These include:

- Socioeconomic status;
- Transition from primary to secondary education;
- Gender, sexuality, family support and special educational needs.

Socioeconomic status (SES)

SES has a significant effect on how children use the Internet. Children from low SES homes tend to make less daily use of the Internet.[44] They also report having significantly fewer digital skills than their better-off peers.[45]

In contrast, academic research has indicated that parents with higher SES tend to offer more forms of online support to their children and are more active in monitoring screen time.[46] Whilst research has identified some trends in this area, further work is needed to fully understand the connections between SES and online harms.

Transition from primary to secondary education

Transition from primary to secondary school is a period of disruption for children and significant cognitive development. They must adapt to new academic and social pressures and are exposed to an expanded peer group with a broader set of home contexts and social norms. It is also a time when many children receive their own smartphone for the first time and gain greater independence in accessing online services away from home.

There is limited research on the risks associated with this period, but we found it was repeatedly identified by respondents as a key area of concern.

Girls and young women

Multiple research studies have identified that girls and young women face a greater risk of harm online. 86% of images of child sexual exploitation and abuse identified by IWF in 2017 were of girls, and 59% of girls/young women aged 11-21 say social media is a major cause of stress[47]. High proportions report frequent judgements on their appearance, pressure to send sexual images, and pressure to engage in sexual activity.[48]

This isn't an exclusively online phenomenon. 52% of girls have either experienced harassment on the street or know someone who has.[49] This suggests online platforms are replicating and exacerbating broader societal issues of sexism and restrictive gender norms.

It is important to note that while most studies indicate that girls are at greater risk, there are some areas where boys may be at greater risk. These include dating and gaming platforms.[50]

Children exploring their sexual orientation

Children who are questioning or exploring their sexual orientation or gender identity appear to be particularly vulnerable to online harm. LGBTQ+ children are likely to be experiencing stigma, isolation and discrimination offline which can enhance online vulnerability.[51]

There is very little research in this area, but it is likely that people will seek social interaction and support online which they are not receiving offline. Children often do not fully understand the consequences of sharing personal information, sending images or arranging to meet strangers met online.[52] There is limited targeted provision for these children, despite recommendations made repeatedly by organisations like Barnardo's.[53]

Special educational needs and neurodiversity

Parents and carers of children with special educational needs are more concerned about their online safety and tend to do more active mediation of online use, but they also see greater potential benefits for developing social and emotional skills.[54]

There is some provision in this area: Cerebra has published guidance for parents and carers of children with autism and learning difficulties,[55] Childnet has produced teaching resources for students with special educational needs in Key Stages 2 and 3, and Mencap's SafeSurfing project produced a short online safety course for children with learning disabilities. However, there is limited research to guide interventions and provision does not cover the full diversity of needs.

Family support

Children without consistent, informed and confident parents or carers are more vulnerable to online risks, especially if those children are also experiencing vulnerabilities in other areas of their life. It is vital therefore to support parents, carers and 'turn to' professionals to develop their authoritative parenting skills and the confidence to apply this to a child's digital life.

Particular regard must be given to children's additional needs. This could help mitigate some of the increased risks caused by other vulnerabilities. The role of teachers becomes more significant when children spend less time with their parents or carers, so they need to be well equipped.

2. The funding landscape is not diverse

Most initiatives are funded by tech companies

The majority of online safety initiatives are funded, at least in part, by tech companies. There is an absence of consistent, significant funding from other sources, such as school funding, and what is there has steadily depleted. Funding from tech companies is valuable and it is right that these companies are taking socially responsible action. But for some, for example those publicly listed, their accountability is often first to their shareholders, so they can't act in opposition to their business model or jeopardise their revenue. Whilst funders expertise is likely to increase when they are close to the subject area, their objectivity will decrease. Tech companies' interest and practical expertise in developing technological solutions may explain why there is such prevalence of technical guidance for parents and carers.

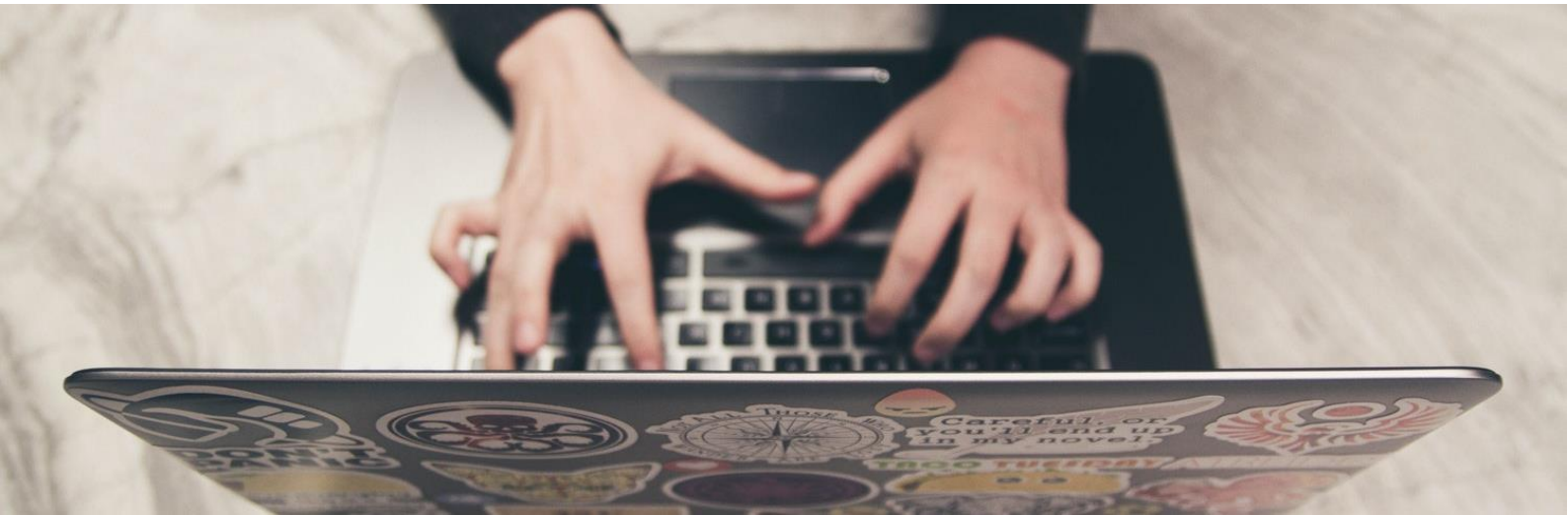
The narrow funding base available to charities may be limiting the sector's ability to campaign. Organisations focused on policy change find it harder to fundraise, and others are understandably reticent to speak in opposition to their core funders. Whilst funding from tech companies can be impactful and is hugely valuable, charities need a more diverse pool of funding for long term sustainability, and for a broader set of approaches to be enabled to grow. And indeed, tech companies cannot be expected to shoulder the burden alone. Other funders must step up.

Short term outputs can be prioritised over long term outcomes

There are examples of long-term tech funding developed in partnership with the sector, such as O2's partnership with NSPCC and Google's 'Be Internet Legends' curriculum. However, not all tech companies are open to collaboration and long-term investment—particularly if they themselves are new to recognising their role in children's online safety. Lack of specific expertise in this complex area, combined with commercial pressures, policy drivers and an enthusiasm to move fast, can lead some companies to seek new, short term, high visibility initiatives over longer term, responsive programmes that are developed and delivered in partnership with the social sector. This can lead to prioritising scale of outputs over the development of effective services and provision.

Funding can also be trend-driven, meaning there is high volume of online resources which are highly visible and trackable in the short term, but lack longevity of impact. This was identified as a key issue for helplines in the 2016 evaluation of the Insafe helpline network.[56] More evidence is needed on what initiatives and approaches are already working or could be developed. Tech companies should be encouraged to respond and build on such initiatives. This would reduce waste on re-invented, short term, isolated initiatives that lack impact.

'Tech-funded education programmes are unsurprisingly guilty of leaving out the things that might challenge the company brand or business model. When we speak to children, they are shocked about how much data is held on them and how it is used, and that this isn't part of their education - they should know about it.'



3. Online environments were built for adults and are not always safe for children

While education can help build digital capabilities that increase resilience, we can't—and shouldn't—expect all children to be fully resilient or bear the burden of staying safe online by themselves. The market for appropriate children's platforms is slim, and there is poor understanding of how to design safe and engaging platforms for children. As we saw on page 10, children are most likely to encounter harmful content on video sharing platforms. But despite being designed for children by one of the world's largest tech companies, most haven't heard of YouTube Kids and the platform is dogged by negative media stories about inappropriate content found on it.[57]

This is partly an issue of commercial consideration. Most online platforms are designed for adults and seek to make money from them, whether through e-commerce, advertising, collecting data or selling services. Platforms designed for adults mean children face heightened risks, just as they would in a similarly designed offline space. It's worth noting though that this isn't just an issue for children. Doteveryone's 2018 Digital Attitudes report found that almost half of adult respondents felt they had no choice but to sign up to online services, even when they had concerns about the potential risks.[58]

There is also the ever-present problem that many children lie about their age online. A desire to 'age up' their experience by exploring spaces and social interaction designed for and targeted at a higher age and development level is often part of a child's development. This may be especially true for children experiencing additional vulnerabilities who may seek alternative sources of information or engagement not provided at home or school.

It is positive that there is growing international recognition that online environments are not appropriate for children. The UN Committee on the Rights of the Child (UNCRC) is currently developing a General Comment on Children's Rights and the Digital Environment, which will clarify how digital technologies affect the full range of children's rights and what governments should do to protect, respect and realise children's rights online. In addition, the W3C TAG Ethical Web Principles will inform a review and implementation of new web specifications to 'put internationally recognised human rights at the core of the web platform'. Within the UK, the ICO's Age Appropriate Design Code, the UKCIS Digital Resilience Framework and the development of a Safety By Design framework, as outlined in the Online Harms white paper, will further strengthen regulation of services used by children.

There is a major gap in online service provision for children moving from primary to secondary school.[59] Platforms intended for children tend to be aimed at a much younger audience (for example CBeebies), while children over the age of 13 can legally use Facebook and other major social media sites. This leaves a lack of choice for children who have grown out of resources like CBeebies who want a more sophisticated platform than is available, so they use sites designed for more adult interactions despite the risks this might entail.

Although a helpful step, provision of appropriate alternative spaces for children should not be seen as a silver bullet or considered in isolation. Dedicated spaces and services can provide children with safer opportunities to develop their skills, confidence and resilience, but adults must be mindful not to rely solely on technological solutions. Not all risk can be removed from age appropriate spaces and they should not be seen as the solution alone. Children remain vulnerable to conduct issues like peer-to-peer bullying and may still be vulnerable to attention from those seeking to exploit them, where they are coerced into migrating the conversation to other platforms with different privacy and encryption settings.

Case study: fragFINN, Germany

fragFINN is free search engine and curated list of age appropriate websites was launched in Germany in 2007. It is funded by the technology sector as part of the German Government's "Ein Netz fur Kinder" (a network for children) initiative.

This award-winning project has evolved to reflect the changing and often complex needs of children. Read-aloud functions for visually impaired children or those with reading difficulties, and videos with subtitles and audio descriptions, allow accessibility and demonstrate inclusiveness.

Hugely popular with children and parents in Germany, fragFINN helped inspire the European Commission's move to a more 'positive content' policy approach. The fragFINN app for Android and iOS was launched to cater for the increasing use of tablet devices and mobile phones amongst children.

4. Duplication can lead to confusion, increasing parental anxiety, and decreasing parental support

The online safety space is populated but fragmented. There is duplication and overlap in resources produced by multiple organisations; a lack of clear, authoritative messaging; and a large volume of outdated legacy resources. Not only does this mean many initiatives fail to add value, and therefore waste resources, it makes it hard for parents, carers and professionals to identify the highest quality and most relevant material. It can be challenging to keep up with emerging issues, particularly for frontline practitioners and professionals who need to respond to crisis situations.[60]

Lack of coordinated and coherent guidance for adults contributes to increasing parental anxiety about their child's online safety,[61] and decreasing levels of parental activity to support their children.[62] Parents and carers are the most important influence on their children's resilience. They must be active in supporting their children, equipped with the best information, and confident about the guidance they can give.

Confusion around online safety is compounded by media reporting which can sensationalise and perpetuate false narratives of harm, and hoaxes like the recent Momo scare.[63] The issue grows when skewed discourse begins to influence policy and professionals. This can lead to ineffective intervention, which diverts resources, and risks creating new barriers to children realising the potential benefits of the Internet.

5. There is varying quality of education and guidance

Guidance to parents and caregivers is narrowly focused

While there are lots of resources for parents and carers, they often have a narrow focus, and many are outdated. Many of the guides and resources funded by tech companies focus on the practical mechanics of implementing forms of media restriction at home, for example setting Internet controls on devices or putting time limits on access, despite research showing that these kinds of approaches aren't useful for reducing risk.[64]

In contrast, there are far fewer resources targeted at developing supportive home environments. The role of parents and carers in children's digital lives and safety is often under-acknowledged. They are often viewed merely as gatekeepers, providing or limiting access to the Internet. In reality their role is more complex. They establish the rules and boundaries necessary for children to cope and flourish in the digital age. Supporting parents to develop their parenting skills, particularly in relation to digital, can positively impact on children's online safety and resilience.

Restrictive approaches can also increase risk: children whose parents implement forms of general restriction, such as forbidding access to the Internet, social media, and electronic games, tend to be the least resilient online.[65] Instead, parents and carers should focus on creating a supportive environment for children as this is the main predictor of children developing autonomy and resilience.

There is a growing evidence base on effective parenting but this is often ignored or not applied to parenting in a digital context. There is a paucity of research on how the established models of 'good enough' parenting are applicable to digital. There is also a lack of understanding around what kind of skills parents need to support children, while some research has found no statistically significant link between parents' digital skills and their children's self-regulation online,[66] other studies have shown a relationship between the use of unhelpful, restrictive strategies with a lack of parental digital skills and confidence.[67] This may be addressed, in part, by the current Preparing for a Digital Future research project at LSE, funded by the MacArthur Foundation.

Schools lack capacity to deliver education

Schools are delivering education about online safety, and will be required to do more from September 2019,[68] but their capacity to do so is limited. Data from South West Grid for Learning's 360safe assessment school indicates that over 40% of schools don't have any teacher training related to online safety.[69] Provision of training for school governors is even lower, with over half of schools having no training for their governors.[70] Without effective training for teaching staff, or the governance boards overseeing practice, practice in education is unlikely to improve.

The lack of internal capacity in schools has also created a market for companies selling assemblies or class sessions on online safety, but this kind of one-off treatment model only raises awareness in the short term and is ineffective for building the skills required for resilience.[71] Instead, children need ongoing support within safe environments to develop skills and resilience, both at home and in school. Internet safety education must mature into becoming embedded in schools.

Outside of schools, training for professionals who work with children can be even sparser. 70% of respondents to a survey of professionals working with children and young people in education, health and children's services had received no training in assessing online risk, and over 80% had received no training in supporting children recovering from online abuse. This could be solved relatively easily, as even short training courses for adults can be highly effective in improving knowledge and confidence.[72]

Case study: Parent Info

Parent Info was developed by Parent Zone in collaboration with the National Crime Agency's CEOP command, with initial funding from the Department of Education. The Parent Info website hosts articles and guides on everything caused or amplified by the Internet. The accompanying newsfeed can be easily embedded into a school or organisation's website, allowing parents to access expert advice on websites they already frequently access.

Today, Parent Info is used by more than one in five British schools. A recent impact evaluation by the London Connected Learning Centre highlighted the positive response from parents, and that schools have utilised it for building staff knowledge and confidence around online harms.

This free resource is an excellent example of how cross-sector organisations can take a collaborative, holistic approach to parents, teachers and children as they navigate increasingly digital lives.

Children and their communities are not involved enough in the design of provision

There is a focus on restriction over empowerment

Education about online safety exists and is reaching children. But much of this provision focuses on children limiting their online participation by staying off platforms or refraining from posting. From a child's perspective, restrictive safety strategies have clear limitations and are outweighed by potential benefits from ignoring them. Research shows that children often actively decide to engage in risky behaviour online, weighing up the potential harms and benefits to do so.[73] For example, one young participant in Ofcom's Media Lives study decided to keep her Snapchat profile public despite receiving inappropriate unsolicited messages because she enjoyed being able to share her stories openly and receive a higher number of likes and favourable comments.[74]

Children's perception of what is risky is likely to differ from an adults, and they lack the critical thinking to assess those risks in the way an adult would. When looking at appetite for risky behaviour, we should consider the need children have to connect with their peers and avoid social exclusion. This can impact their online activity, where the need for inclusion can outweigh any adult warnings, restrictions or better judgement.

'Empowering young people and giving them agency in the area of online safety is so important. And young people normally exceed our expectations. There is so much potential in what we can achieve working with young people.'

Provision is designed and delivered top down

Online safety education is not driven by demand from children but by the concerns of adults. It is of course right that services are commissioned and delivered by adults, but this poses a real challenge in making education relevant and valuable for building digital capabilities. Research with young people reports them successfully developing their own strategies for managing online risk,[75] however these strategies aren't shared in formal education and there is an absence of mechanisms to enable learning across peer groups. While online safety education for children can't be user-driven, it needs to be user-centred and learn from children's lived experiences. Children need to be empowered to make the right decisions online.

Case study: Project Rocket, Australia

Project Rocket is an innovate Australian youth-driven initiative to tackle bullying, hate and prejudice. Predominantly aimed at schools, its ground-breaking approach uses role play, interactive discussions and workshops that emphasise setting positive norms. Project Rocket aims to provide children with proactive strategies to tackle cyber bullying, with outcomes aligned with the Australian Curriculum, Alannah and Madeline Foundation's Smart Framework. It is officially certified by the Federal eSafety Office.

Project Rocket works with Facebook and Instagram on a Digital Ambassadors programme building peer networks to create supportive communities and act as a catalyst for school-based action. The same partnership includes an Action Hub designed to convert the positive one-off experiences of face-to-face Project Rocket workshops into more lasting change that can be led by children and young people.

Project Rocket is an excellent example of how a youth-lead organisation has been able to establish strong connections and funding from the technology sector. It is also a member of the Facebook Advisory Board and the Twitter Trust and Safety Council.

WHAT ARE THE OPPORTUNITIES FOR FUNDING?

It is clearly evident that the sector has to diversify its funding. From our analysis of the risks and challenges of online child safety, we have identified five avenues of opportunities and recommendations for funders and programme designers. These can be categorised into three priority approaches: **building digital capabilities and resilience at a community level, co-design with children and their communities, and the building of a better, age appropriate Internet.** Meanwhile, spanning right across the sector, we also need to **improve our understanding of online safety, and to provide leadership within a fragmented sector.**

Figure 3: Areas where funding can have an impact keeping children safe online.

1. Building capabilities and resilience at a community level

To build children's resilience and digital capabilities, a systems change approach is needed. It is insufficient to look at what children need without looking to the networks around them, particularly their parents, carers and teachers. It is unhelpful to think of children as more confident and familiar with technology than their parents, carers and teachers, because they lack the critical thinking to flourish online.

Resilience needs to come from a community level, which means equipping and empowering adults to know how to address online risks and harms with children. Parents and carers are one of the most significant influences on children, balancing rules and boundaries with opportunities to explore and develop, which can help children flourish in the digital age.[76] Parents and carers need the skills and resources to be able to talk to their children

about online safety in a broader definition of harms that originate and take place both online and offline. Schools and youth services should offer high quality and long-term training, rather than one off visits or assemblies.

Charities we spoke to would like for their one-off programmes to be more embedded in schools:

'Wheeling in a one-off assembly isn't the best thing as schools don't have the capacity for follow up. Schools shouldn't have to rely on external agencies, but the number of schools with continuing professional development (CPD) for online safety is dropping.'

Children's peer groups are another opportunity for building community level resilience. Evidence shows that education on safety, privacy and risk online must look beyond individual decision-making (for example in relation to privacy and data-sharing) and enable children to think collectively about what kinds of cultures (online and offline) they want to be a part of and support.[77]

2. Co-design with children and their communities

One of the charity sector's great strengths lies in its relationships with the communities it serves. Charities which already work with children and young people are well placed to magnify their voices in the development of online safety provision. User involvement is all about designing and delivering solutions 'with' people rather than 'at' people, to share power and ensure better answers are found.[78] There is a clear opportunity to develop programmes which enable children, and those who the initiatives are developed for, such as parents, carers and professionals, to have greater influence over the design of education and actively contribute to research that builds knowledge around online safety. Putting restrictions on children will not always stop children from encountering harm online but work to encourage safe online use will be more effective when children have played a role in its' design.

'We need to reduce the fear that stops children coming forward, particularly in relation to sexting, pornography and relationships. We need to change the agenda from policing and legality to discussing consent. Kids are doing what kids do, mobile phones are the new bike shed. There will always be new specific issues, the important thing is to evolve how we respond to them.'

3. Building a better Internet

Whilst we welcome the Government's Online Harms white paper's focus on empowering users, online safety is not solely about resilience and education. Ultimately, we need to work towards a future where online platforms are safe by design. It is short sighted to focus only on resilience without simultaneously looking to stop children from experiencing harm online in the first place. This isn't just about children: adults don't want there to be a trade-off between their access to the Internet and their safety and privacy either.

'The Internet has always been seen as a platform on which all people are treated equally. But that means children are being treated like adults, and that has led to a lot of the harms we now see.'

Regulation is needed to tackle existing challenges. The proposed development of a statutory duty of care and independent regulator in the UK, and the UNCRC's general comment on Children's Rights and the Digital Environment are both positive, and powerful steps towards addressing this. But the long-term solution is for the technology of the future to be built with prevention of harm at its core. Nominet have strongly welcomed the

Government's ambition, set out in the Online Harms white paper, for the UK to be a world-leader in the development of online safety technology.

Embedding safety by design in platforms requires supporting all technology start-ups and existing service designers to anticipate the impact of their products on the public, particularly the most vulnerable and children. There is significant work underway to produce guiding principles, codes of conduct and practical tools to address this, including the Safety by Design framework being developed by DCMS, the UKCIS Digital Resilience Framework and W3C ethical principles. However, to be effective all of these initiatives and frameworks need to be coordinated and made available in practical and purposeful ways for start-ups and SMEs, especially where there is a lack of experience in the sector.

Safety technologies are a huge opportunity for the UK. The Online Harms white paper describes how 'a dynamic and innovative market has sprung up around online safety, developing tools for business to protect their users from harms'. Making the UK a world leader in online safety means learning from the fin-tech, health-tech, civic-tech and ed-tech eco-systems in which Britain is already world leading, along with the broader achievements of the Tech for Good ecosystem. There are multiple ways funders and Government can help build the 'Safety-tech' ecosystem, some of which are already beginning to emerge. This might include encouraging open-innovation partnerships between entrepreneurs and established organisations, such as through Challenge Funds, using convening power to raise the profile of online safety initiatives and developing a consistent and attractive portfolio of early-stage opportunities for investment.

Working within the existing online environment, there are specific opportunities for start-ups to develop companion apps or middleware which mediate interaction between existing platforms. The BBC's Own It app is one example of what might be done here. There is also a lack of safe online environments—or digital sandboxes—where children can practice interacting online in moderated environments and develop resilient peer communities. Environments like these can enable children to take managed risks, thereby developing digital confidence, capability and resilience.[79] Finally, there are opportunities to directly address content risks through building on the successful work of the Internet Watch Foundation to provide collective and open web services for improved content moderation across platforms.

'We need to develop safe digital spaces where all children can make mistakes safely within their community to learn and develop.'

Case study: BBC Own It

Announced by the BBC in November 2018, this innovative app uses chatbot technology to help children engage with the issues that matter to them. Combining the latest machine-learning technology with children's self-reporting of their own online activity and mood, the app provides nudges, advice and support at the point they need it.

By offering intervention guidance and expert-curated content in a non-prescriptive way, BBC Own It helps children build their own critical understanding and positive behaviours. The contextual nature of the app also supports the kind of authoritative parenting that has a positive impact on children's wellbeing. As part of the broader BBC 'Own It' brand, this approach demonstrates that technology can do much to engage and support young people, as well as parents and carers.

The increasing predominance of independent use of tablet and mobile phone devices by children means apps of this kind could play an important role in supporting wellbeing.

4. Improving understanding of what works

There is a growing body of academic research concerning online child safety. However, there are key gaps in knowledge, particularly around the design and efficacy of interventions[80], the detail of vulnerabilities that increase risk of harm, and the risks of interactions in less studied environments like online games.

While many initiatives have been developed by diverse stakeholders and some build on logical theories of change or existing evidence, few have been independently evaluated. We lack the evidence to determine what works and why. Where evaluations are undertaken, they tend to focus on immediate outcomes, such as reach, rather than reduction in harm or improvement in wellbeing.[81] For example, while there are multiple programmes intended to combat cyberbullying in the UK, none have been formally evaluated.[82] There is also ongoing disagreement about underlying mechanisms of harm, including continuing debate about the importance of screen time[83] and social media use[84], despite these forming the basis of current initiatives. As a result, we are missing vital understanding to design better services and provision for online safety.

Finally, better translation of research and briefing for policy makers is important. The gap between evidence on screen time and emergent policy has already been highlighted, but there are other challenges including the focus on quantity over quality of education and approaches to online safety that fail to consider broader social and economic contexts.

5. Providing leadership

The UK's online safety landscape is populated but fragmented. There is duplication of effort, a lack of attention to some areas of risk and vulnerability, for example commercial risks or special education needs, and a focus on restrictive strategies. However, there are also examples of good practice and collaboration between industry, government and civil society. Clearer leadership in the sector would improve signposting to the highest quality resources and help people to navigate an otherwise confusing landscape.

It may be that some of this role will be undertaken by the independent regulator proposed by the Online Harms White paper, but civil society needs to have a strong voice in shaping interventions and future directions. Organisations like 5Rights are undertaking this work, but funding for this kind of work is challenging as it often does not produce quantifiable outputs. It can be seen as challenging the commercial interests of tech companies who are influential funders but genuinely independent funding is needed if online harms are to be dealt with.

CONCLUSION

Children are accessing online content and engaging in the online world more than ever before. They need to be supported to do so safely and constructively. By virtue of their age and lack of wider life experience, children often lack skills to negotiate the challenges of engaging in an online world, and they need to nurture these skills in order to become discerning consumers and constructive online citizens. Children need help with a range of issues, from managing the persistence of communication that makes cyberbullying so damaging, to recognising lack of rigour or moderation of content and expressed views.

There are problems with the current support landscape. Many systems designed to help children are focused on adults conveying one-time lessons or messages that focus on restriction or withdrawal from the online world, rather than equipping children with the skills and capabilities to negotiate their own safe online experience. This creates several problems. Resources for adults can be fragmented, poorly signposted, heavily duplicated and out of date. This in turn can make it difficult for adults to properly support children, speak their language, or be consistently relevant to children whose online preferences change quickly and who drive new trends faster than adult training materials can be generated to respond to them.

Parents and other supporting adults can understandably become anxious about the need to be consistently up to date on the fast-changing preferences, behaviours and technologies that children adopt, adapt and create. Helping parents to recognise the existing skills, knowledge and capabilities they have in caring for their children and how those can be applied to digital contexts, despite rapid changes in the landscape and the types of products children are accessing, can alleviate some of this anxiety and help parents to provide their children with better all-round support.

An evidence based, systems change approach should be adopted to help parents, teachers and carers create a community of support around children. This needs to be centred around the processes for equipping children with the digital resilience and critical understanding they need, rather than the specific details of individual platforms or technologies that will rapidly date and drop out of favour.

If we are to reframe ‘online safety’ away from being an adult term into something children embrace and value as part of their wider education, we need to work more closely with children and co-design interventions. Co-design is vital if interventions are to respond to the actual risks and harms children are concerned about in their daily life, alongside those that professionals know may affect them but which children may not readily identify. We need to provide children with more relevant age appropriate spaces in which to learn, analyse their online decisions and build resilience, and form their own mode of operation without generating a footprint in the bigger online landscape. And we must recognise the interplay of both online and offline vulnerabilities in relation to economics, family, ability and identity, especially for children who experience additional vulnerabilities.

Finally, we need to ensure that the online world that children enter is as safe as possible, and this can be achieved by more responsible corporate citizenship and more rigorous regulation at government level, consistently driven and challenged by charity campaigning work.

For charities and funders alike, there are rich opportunities to drive forward best practice when it comes to online child safety. Internet usage and online engagement is only going to grow amongst children, and funders and charities need to work together to develop safer online environments, build supportive and resilient communities, and equip children with the capabilities to not just survive but thrive in an increasingly digital world.

APPENDIX

Scope of UK Government agenda for online safety

	Harms with a clear definition	Harms with a less clear definition	Underage exposure to legal content
Relevant to children and young people	• Terrorist content and activity. • Organised immigration crime. • Modern slavery. • Incitement of violence. • Sale of illegal goods/ services, such as drugs and weapons (on the open Internet). • Content illegally uploaded from prisons. • Extreme pornography. • Revenge pornography. • Harassment and cyberstalking. • Hate crime. • Encouraging or assisting suicide.	• Extremist content and activity. • Promotion of Female Genital Mutilation (FGM). • Cyberbullying and trolling. • Coercive behaviour. • Intimidation. • Disinformation. • Violent content. • Advocacy of self-harm.	
Specific to children and young people	• Child sexual exploitation and abuse. • Sexting of indecent images by under 18s (creating, possessing, copying or distributing indecent or sexual images of children and young people under the age of 18).		• Children accessing pornography. • Children accessing inappropriate material (including under 13s using social media and under 18s using dating apps; excessive screen time).

ENDNOTES

[1] Lilley, C., & Ball, R. (2013). Younger children and social networking sites, NSPCC

[2] Livingstone S, Davidson J, Bryce J, Batool S, Haughton C, Nandi A. (October 2017) Children's online activities, risks and safety. A literature review by the UKCCIS Evidence Group.

[3] Livingstone S, Davidson J, Bryce J, Batool S, Haughton C, Nandi A. (October 2017) Children's online activities, risks and safety. A literature review by the UKCCIS Evidence Group.

[4] Livingstone S, Davidson J, Bryce J, Batool S, Haughton C, Nandi A. (October 2017) Children's online activities, risks and safety. A literature review by the UKCCIS Evidence Group.

[5] Livingstone S, Davidson J, Bryce J, Batool S, Haughton C, Nandi A. (October 2017) Children's online activities, risks and safety. A literature review by the UKCCIS Evidence Group.

[6] Ofcom (January 2019) Children and Parents: Media Use and Attitudes Report

[7] Livingstone S, Davidson J, Bryce J, Batool S, Haughton C, Nandi A. (October 2017) Children's online activities, risks and safety. A literature review by the UKCCIS Evidence Group.

[8] Lilley, C., & Ball, R. (2013). Younger children and social networking sites, NSPCC.

[9] Livingstone, S., Haddon, L., Görzig, A. & Ólafsson, K. (2011) EU kids online: final report.

[10] Zakkoyya H. Lewis, Maria C. Swartz, and Elizabeth J. Lyons. (April 2016) What's the Point?: A Review of Reward Systems Implemented in Gamification Interventions. Games for Health Journal.

[11] Kidron B, Rudkin A. (December 2017) Digital Childhood: Addressing Childhood Development Milestones in the Digital Environment. 5Rights

[12] Katz A, El Asam, A. (2018) Vulnerable Children in a Digital World. Internet Matters

[13] Palmer, T. (2015) Digital dangers: The impact of technology on the sexual abuse and exploitation of children and young people. Barnardo's

[14] Slavtcheva-Petkova, V., Nash, V.J. & Bulger, M. (2015) Evidence on the extent of harms experienced by children as a result of online risks: implications for policy and research. Information, Communication & Society. 18 (1), 48–62.

[15] Slavtcheva-Petkova, V., Nash, V.J. & Bulger, M. (2015) Evidence on the extent of harms experienced by children as a result of online risks: implications for policy and research. Information, Communication & Society. 18 (1), 48–62.

[16] Online Harms White Paper, (April 2019)

[17] Slavtcheva-Petkova, V., Nash, V.J. & Bulger, M. (2015) Evidence on the extent of harms experienced by children as a result of online risks: implications for policy and research. Information, Communication & Society. 18 (1), 48–62.

[18] Livingstone S, Davidson J, Bryce J, Batool S, Haughton C, Nandi A. (October 2017) Children's online activities, risks and safety. A literature review by the UKCCIS Evidence Group.

[19] Livingstone S, Davidson J, Bryce J, Batool S, Haughton C, Nandi A. (October 2017) Children's online activities, risks and safety. A literature review by the UKCCIS Evidence Group.

[20] Rosen, R. (January 2017) Ordinary magic for the digital age: understanding children's digital resilience. Parent Zone

[21] Newman, T. (2002) Promoting resilience: a review of effective strategies for child care services.

[22] Przybylski A, Mishkin A, Shotbolt V, Linington S. (2014) A shared responsibility: Building children's online resilience, Virgin Media and Parent Zone

[23] Livingstone, S., Marsh, J., Plowman, L., Ottovordemgentschenfelde, S., & Fletcher-Watson, B. (2014) Young children (0-8) and digital technology: a qualitative exploratory study - national report – UK. Joint Research Centre, European Commission.

[24] Livingstone, S., Marsh, J., Plowman, L., Ottovordemgentschenfelde, S., & Fletcher-Watson, B. (2014) Young children (0-8) and digital technology: a qualitative exploratory study - national report – UK. Joint Research Centre, European Commission.

[25] Livingstone, S., Marsh, J., Plowman, L., Ottovordemgentschenfelde, S., & Fletcher-Watson, B. (2014) Young children (0-8) and digital technology: a qualitative exploratory study - national report – UK. Joint Research Centre, European Commission.

[26] Mars B., Heron J., Biddle L., Donovan JL., Holley R., Piper M., et al. (October 2015) Exposure to, and searching for, information about suicide and self-harm on the Internet: Prevalence and predictors in a population-based cohort of young adults.

[27] Livingstone S, Davidson J, Bryce J, Batool S, Haughton C, Nandi A. (October 2017) Children's online activities, risks and safety. A literature review by the UKCCIS Evidence Group.

[28] The Annual Bullying Survey (2017) Ditch the Label. The Annual Bullying Survey 2017].

[29] Livingstone, S., Marsh, J., Plowman, L., Ottovordemgentschenfelde, S., & Fletcher-Watson, B. (2014) Young children (0-8) and digital technology: a qualitative exploratory study - national report – UK. Joint Research Centre, European Commission.

[30] Livingstone, S., Marsh, J., Plowman, L., Ottovordemgentschenfelde, S., & Fletcher-Watson, B. (2014) Young children (0-8) and digital technology: a qualitative exploratory study - national report – UK. Joint Research Centre, European Commission.

[31] Internet Watch Foundation (2017) Annual Report

[32] Livingstone S, Davidson J, Bryce J, Batool S, Haughton C, Nandi A. (October 2017) Children's online activities, risks and safety. A literature review by the UKCCIS Evidence Group.

[33] Livingstone S, Davidson J, Bryce J, Batool S, Haughton C, Nandi A. (October 2017) Children's online activities, risks and safety. A literature review by the UKCCIS Evidence Group.

34 Veltri, Giuseppe & Lupiáñez-Villanueva, Francisco & Gaskell, George & Theben, Alexandra & Folkvord, Frans & Bonatti, Luca & Bogliacino, Francesco & Fernández, Llüisa & Codagnone, Cristiano. (2016). Study on the impact of marketing through social media, online games and mobile applications on children's behaviour.

[35] Online Harms White Paper, (April 2019)

[36] Markman, J. GDPR is great news for Google and Facebook, really. In Forbes, 22 May 2018

[37] Information Commissioners Office website: Data Protection by design and default

[38] Family Kids & Youth (2017) for the Royal Foundation of the Duke and Duchess of Cambridge and Prince Harry

[39] Ofcom (January 2019) Children and Parents: Media Use and Attitudes Report

[40] Family Kids & Youth (2017) for the Royal Foundation of the Duke and Duchess of Cambridge and Prince Harry

[41] Palmer, T. (2015) Digital dangers: The impact of technology on the sexual abuse and exploitation of children and young people. Barnardo's

[42] Katz A, El Asam, A. (2018) Vulnerable Children in a Digital World. Internet Matters

[43] Livingstone S, Davidson J, Bryce J, Batool S, Haughton C, Nandi A. (October 2017) Children's online activities, risks and safety. A literature review by the UKCCIS Evidence Group.

[44] Livingstone, S., Haddon, L., Vincent, J., Mascheroni, G., & Ólafsson, K. (2014) Net children go mobile: The UK report.

[45] Livingstone, S., Haddon, L., Vincent, J., Mascheroni, G., & Ólafsson, K. (2014) Net children go mobile: The UK report.

[46] Livingstone, S. & Zhang, D. (2019) Inequalities in how parents support their children's development with digital technologies. Parenting for a Digital Future: Survey Report 4. LSE

[47] Internet Watch Foundation. Annual Report 2017

[48] McGeeny E, Hanson E. (2017) Digital Romance: A research project exploring young people's use of technology in their romantic relationships and love lives.

[49] Girlguiding, Girls' Attitudes Survey 2018

[50] Palmer, T. (2015) Digital dangers: The impact of technology on the sexual abuse and exploitation of children and young people, Barnardo's

[51] McGeeny E, Hanson E. (2017) Digital Romance: A research project exploring young people's use of technology in their romantic relationships and love lives.

[52] Palmer, T. (2015) Digital dangers: The impact of technology on the sexual abuse and exploitation of children and young people, Barnardo's

[53] Palmer, T. (2015) Digital dangers: The impact of technology on the sexual abuse and exploitation of children and young people, Barnardo's

[54] *Livingstone, S. Zhang, D.* Children with special educational needs and disabilities more likely to encounter harm online, say parents, LSE blog

[55] Cerebra (2015) Learning Disabilities, Autism and Internet Safety: A Parent's Guide

[56] Dinh T, Farrugia L, O'Neill B, Vandoninck S, Velicu A. (March 2016) Insafe Helplines: operations, effectiveness and emerging issues for internet safety helplines EU Kids Online, European Schoolnet and Kapersky Helpline Fund

[57] MacDonald K. Parents: don't panic about Momo – worry about YouTube Kids instead in *The Guardian*. 28th February 2019

[58] Miller C, Coldicutt R, Kos A. (May 2018) People, Power and Technology: The 2018 Digital Attitudes Report

[59] 5Rights (2018) Disrupted Childhood: The Cost of Persuasive Design

[60] Dinh T, Farrugia L, O'Neill B, Vandoninck S, Velicu A. (2016) Insafe Helplines: operations, effectiveness and emerging issues for internet safety helplines, EU Kids Online, European Schoolnet and Kapersky Helpline Fund

[61] Internet Matters (2018) Look Both Ways: Practical Parenting in the Age of Screens

[62] Ofcom (2018) Children and Parents: Media Use and Attitudes Report, p.18

[63] Phippen A, Bond E. (2018) Digital Ghost Stories; Impact, Risks and Reasons, South West Grid for Learning

[64] Przybylski AK, Nash V. (2017) Internet Filtering Technology and Aversive Online Experiences in Adolescents

[65] Przybylski A, Mishkin A, Shotbolt V, Linington S. (2014) A shared responsibility: Building children's online resilience, Virgin Media and Parent Zone

[66] Przybylski A, Mishkin A, Shotbolt V, Linington S. (2014) A shared responsibility: Building children's online resilience, Virgin Media and Parent Zone

[67] Livingston, S. Digital skills matter in the quest for the 'holy grail,'v on the LSE blog, 2017

[68] Online Harms White Paper, (April 2019)

[69] Phippen A. (2018) UK Schools Online Safety Policy and Practice Assessment South West Grid for Learning Trust

[70] Phippen A. (2018) UK Schools Online Safety Policy and Practice Assessment South West Grid for Learning Trust

[71] Government guidance: Using External Visitors to Support Online Safety Education: Guidance for Educational Settings

[72] Bond E, Dogaru C. (April 2019) An Evaluation of an Inter-Disciplinary Training Programme for Professionals to Support Children and Their Families Who Have Been Sexually Abused Online. Br J Soc Work.

[73] Livingstone S, Davidson J, Bryce J, Batool S, Haughton C, Nandi A. (October 2017) Children's online activities, risks and safety. A literature review by the UKCCIS Evidence Group.

[74] Ofcom. (2019) Children's media lives – Wave 5

[75] McGeeny E, Hanson E. (2017) Digital Romance: A research project exploring young people's use of technology in their romantic relationships and love lives.

[76] Przybylski A, Mishkin A, Shotbolt V, Linington S. (2014) A shared responsibility: Building children's online resilience, Virgin Media and Parent Zone

[77] McGeeny E, Hanson E. (2017) Digital Romance: A research project exploring young people's use of technology in their romantic relationships and love lives.

[78] Clay, T., McLeod, R. (2018) Make it count: why impact matters in user involvement, NPC

[79] Livingstone S, Davidson J, Bryce J, Batool S, Haughton C, Nandi A. (October 2017) Children's online activities, risks and safety. A literature review by the UKCCIS Evidence Group.

[80] Livingstone S, Davidson J, Bryce J, Batool S, Haughton C, Nandi A. (October 2017) Children's online activities, risks and safety. A literature review by the UKCCIS Evidence Group.

[81] Livingstone S, Davidson J, Bryce J, Batool S, Haughton C, Nandi A. (October 2017) Children's online activities, risks and safety. A literature review by the UKCCIS Evidence Group.

[82] Livingstone S, Davidson J, Bryce J, Batool S, Haughton C, Nandi A. (October 2017) Children's online activities, risks and safety. A literature review by the UKCCIS Evidence Group.

[83] Przybylski, A. & Orben, A. (2019) We're told that too much screen time hurts our kids. Where's the evidence?, The Guardian.

[84] Orben, A., Dienlin, T. & Przybylski, A.K. (2019) Social media's enduring effect on adolescent life satisfaction. Proceedings of the National Academy of Sciences. 116 (21), 10226–10228.

TRANSFORMING THE SOCIAL SECTOR

NPC is a charity, think tank, and consultancy to the social sector. Over the past 15 years we have worked with charities, funders, philanthropists and others, supporting them to deliver the greatest possible impact for the causes and people they exist to serve.

NPC occupies a unique position at the nexus between charities and funders. We are driven by the values and mission of the social sector, to which we bring the rigour, clarity and analysis needed to better achieve the outcomes we all seek. We also share the motivations and passion of funders, to which we bring our expertise, experience and track record of success.

Increasing the impact of charities: We exist to make charities and social enterprises more successful in achieving their missions. Through rigorous analysis, practical advice and innovative thinking, we make charities' money and energy go further, and help them to achieve the greatest impact for people.

Increasing the impact of funders: NPC's role is to make funders more successful too. We share the passion funders have for helping charities and changing people's lives. We understand their motivations and their objectives, and we know that giving is more rewarding if it achieves the greatest impact it can.

Strengthening the partnership between charities and funders: Our mission is also to bring the two sides of the funding equation together, improving understanding and enhancing their combined impact. We can help funders and those they fund to connect and transform the way they work together to achieve for people.

New Philanthropy Capital
Harling House, 47-51 Great
Suffolk St, London SE1 0BS
020 7620 4850
Info@thinkNPC.org
@NPCthinks

Registered charity No 1091450
A company limited by guarantee
Registered in England and Wales No 4244715

www.thinkNPC.org