HM Government

Government response to the Internet Safety Strategy Green Paper

May 2018

Contents

1. Foreword

The Internet is a powerful force for good. It serves humanity, spreads ideas and enhances freedom and opportunity across the world. Combined with new technologies, such as artificial intelligence (AI), it is set to change society perhaps more than any previous technological revolution – connecting people, making us more productive, and raising living standards. However, alongside these new opportunities come new challenges and risks.

We strongly support the freedom of speech but that does not mean that we should turn a blind eye to abuse or bullying. Research suggests up to 25% of children and young people in the UK experience cyberbullying.[1] When the Internet is misused by individuals, and that misuse is amplified by the connectivity provided by social media platforms, it can cause real and lasting harm, especially to young people and the vulnerable.

Misuse of social media can also erode trust in the Internet and in new technologies more generally, undermining the very real benefits that the digital revolution can bring. Tackling these challenges in an effective and responsible way is therefore critical for digital technology and the digital economy to thrive.

More and more people are concerned about safety online. They feel that there are no clear standards for behaviour and that social media companies are not taking responsibility for what happens on their platforms.

Through our Digital Charter, the Government is working to ensure that the UK is both the safest place to be online, and the best place to start a digital business. We are already working with social media companies so we can protect users and change user behaviour online. The Data Protection Bill will give more power to individuals to control how their data is used and manage their online experience. And we have also asked the Law Commission to conduct a review into online abusive communications so that we can make sure the criminal law is fit for purpose when tackling abusive behaviour on social media platforms.[2]

Today, we are introducing plans for a social media code of practice and transparency reporting as part of our Digital Charter. The statutory code of practice provides guidance to social media providers on appropriate reporting mechanisms and moderation processes to tackle abusive content. By setting out clear standards for industry, we will make sure there is improved support for users online, and that more companies are taking consistent action to tackle abuse.

---

1 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650933/Literature_Review_Final_October_2017.pdf

2 https://www.lawcom.gov.uk/government-asks-law-commission-to-look-at-trolling-laws/

Transparency reports will provide data on the amount of harmful content being reported to platforms in the UK and information on how these reports are dealt with, including what mechanisms they have in place to protect users, for example, around their mental health and wellbeing. These reports will help us understand the extent of online harms and how effectively companies are tackling breaches in their terms and conditions.

As we implement these important improvements, we will also publish a full White Paper later this year as a precursor to bringing forward online safety legislation that will cover the full range of online harms. Potential areas for legislation include the code of practice, transparency reporting and online advertising. This will create a level playing field for companies by setting universal online safety expectations.

I would like to thank everyone who participated in our Internet Safety Strategy consultation. We had an excellent response to our online survey and we have engaged with a wide range of users, including young people, charities and technology companies.

It is clear that this is an issue which is close to the heart of many people in the UK and across the world. In the coming months and years, we will lead the work to ensure that the UK not only has the world's best digital economy, but is also the safest place to be online.

The Rt Hon Matt Hancock MP
Secretary of State for Digital, Culture, Media and Sport

2. Executive Summary

The Digital Charter established twin aims - to make the UK the safest place in the world to be online and to ensure the UK has the world's best digital economy. The Charter aims to agree norms and rules for the online world, as part of our work to build a thriving ecosystem where technology companies can start and grow, and where citizens can have confidence that the Internet is a well governed space.

Social media platforms have brought extraordinary benefits and innovations to everyday life. They facilitate the exchange of information, goods and services across the globe and are important enablers to UK economic growth.

Ensuring people's safety online is a fundamental element of this thriving ecosystem. We need to complement internet freedoms and innovation with safety and security to build trust in new technologies. Cyberbullying and intimidating behaviour online, which can have negative impacts on mental health and wellbeing, particularly among children, is now all too commonplace. Despite a range of voluntary initiatives, good work by a range of charities and technological innovations, online abuse remains an issue for millions of citizens. Therefore we are taking further steps to tackle this behaviour, and ensure that offline rules apply online too.

The Internet Safety Strategy Green Paper, which was published in October 2017, set out our proposals relating to tackling unacceptable behaviour and content online. Since then, the use of the Internet to spread disinformation or 'fake news', the dangers of using AI to manipulate public opinion at scale, the mass misuse of personal data and the potential for data to be used for unethical or harmful purposes, have all gained prominence as serious and real problems - demonstrating the importance of a comprehensive strategic approach to improve online safety and restore citizens' confidence in technology.

The Internet Safety Green Paper

The Government published its Internet Safety Strategy Green Paper last year as our first publication under the Digital Charter. In the Green Paper we described a wide range of online harms about which the Government is concerned, particularly those that affect children. These harms included cyberbullying, online abuse, harassment, trolling and sexting. These behaviours can have devastating impacts on victims, including on their mental health and wellbeing, and, depending on the circumstances in which they are committed, may break the law.

The prevalence of online harms was confirmed by the nearly 600 respondents to the Internet Safety Strategy consultation survey, many of whom had witnessed harmful content online, particularly online bullying, racial abuse and online misogyny.

In the Green Paper we proposed a set of principles to underpin our approach:

1. What is unacceptable offline should be unacceptable online;

2. All users should be empowered to manage online risks and stay safe; and
3. Technology companies have a responsibility to their users, and for the content they host.

In the accompanying consultation, we asked people to tell us what they thought about our proposed initiatives, and how Government can work collaboratively with a wide range of stakeholders to tackle online harms and promote safer online communities. We particularly asked for views on:

1. Supporting parents and carers
2. A social media code of practice
3. Transparency reporting for social media companies
4. A social media levy
5. Possible technological solutions
6. Developing children's literacy
7. Adult experience of online abuse
8. Concerns around online dating.

The consultation response

We had an excellent response to our consultation which ran from October to December 2017. We have also undertaken a range of roundtable discussions and focus groups with a wide variety of stakeholders. It is clear that a growing number of people, including parents and education and health professionals, are concerned about safety online. The consultation highlighted three main issues:

1. Online behaviours too often fail to meet acceptable standards;
2. Users can feel powerless to address these issues;
3. Technology companies can operate without proper oversight, transparency or accountability, and commercial interests mean that they can fail to act in users' best interests.

Consultation Survey

Our online consultation survey results provided information relating to users' current experiences online.[3] Of respondents who chose to answer the relevant consultation questions:

- 60% of respondents (296 individuals) confirmed that they had witnessed inappropriate or harmful content online;
- 41% of respondents (149 individuals) said that they had experienced online abuse. Of these, 130 individuals had experienced insults, 70 harassment, 57 threats and 51 bullying. 15 individuals said that they experienced the abuse daily and 27 said weekly. 78 individuals said that the abuse related to political or social views. 84% of

[3] See Annex A for further details of how the consultation survey response figures have been calculated.

respondents (82 individuals) said that they did not know the person/ people perpetrating the online abuse;
- 77% of respondents (330 individuals) confirmed that they knew how to report potentially illegal or upsetting content on social media, but only 36% (158 individuals) had reported this content before;
- Only 41% of respondents (66 individuals) thought that their reported concerns were taken seriously by social media companies.

The extent to which users witness harmful content, or experience online abuse is a significant concern. The fact that the abuse individuals received was frequently about political or social views is particularly worrying for our democratic discourse.

The survey also asked respondents for their views on our proposed policies. The results highlighted that:
- When asked which platforms should have a code of practice, just over half of respondents (197 individuals) agreed that platforms that enabled individuals to publish public messages which can be viewed by others should have a code. A number of respondents also suggested that platforms which enabled live stream video content (182 individuals), creation of a dating profile (172 individuals), sending private messages to others (160 individuals), sharing images/ videos (158 individuals), creating a sharable profile to enable connections with other users (145 individuals) and sharing content such as web links with others (142 individuals) should have a code of practice;
- Respondents confirmed that they would especially like transparency reports to cover: what moderation policies each site had in place and how these are reviewed (191 individuals); how many complaints have been received, how they are dealt with and the volume of content removed (137 individuals); and information on how you can get help and access safety centres on their platforms (107 individuals);
- 222 parents responded to our online survey and some highlighted that they were keen to receive more information on topics including personal data protection (72 parents), the mental health impacts of being online (69 parents), cyberbullying (62 parents), deception/fraud online (61 parents), critical thinking (61 parents), physical impacts of being online (52 parents) and digital resilience (51 parents);
- 49% of respondents (189 individuals) agreed that more safety information about digital products and platforms should be available to consumers/ users;
- 71% of respondents (260 individuals) thought that social media and application services enabling contact between users on a sexual/ romantic basis should have a minimum age rating. 51% (133 individuals) thought the minimum age rating should be 18 and above;
- 27% of respondents (100 individuals) agreed that social media and application services enabling contact between users on a sexual/ romantic basis do all they can to prevent abuse of young people;
- 60% of respondents (219 individuals) thought that the technology industry has a role to play in supporting children develop their digital literacy skills. Respondents thought that this could be done by developing materials and games which promote digital literacy, improving moderation and reporting functions on their sites, developing free materials for schools and parents;

- 34% of respondents (127 individuals) thought that peer-to-peer online safety schemes would be an effective way of helping children stay safe online.

The survey responses from organisations highlighted that:

- 95% (53 organisations) agreed that social media platforms have a duty of care to remove and reduce inappropriate behaviour or content on their platforms;
- 58% (33 organisations) agreed that companies should encourage people to use their real identity when using social media and 97% (55 organisations) agreed that the code of practice should include steps to tackle those who use anonymous social media accounts to abuse others;
- 81% (46 organisations) agreed that all social media companies should have the same standards of behaviour;
- 83% (49 organisations) agreed that more safety information about digital products and platforms should be available to consumers/ users;
- 95% (57 organisations) agreed that the technology industry has a role to play in supporting children develop their digital literacy skills.

We have taken into account these views as we have developed the policies which are set out later in this paper.

What stakeholders told us

We talked to teachers from primary and secondary schools, children who regularly use social media, and a number of different charities who represent the views of parents, children and vulnerable users. In addition, we held a series of roundtables with major technology companies so that we could learn about their safety work to date and the opportunities for using technology to prevent online harms. These discussions covered a wide range of topics including screen time, the enforcement of age restrictions on social media and ways of effectively tackling bullying online.

We have also had related discussions with social media and technology companies as part of a joint working group with the Department of Health and Social Care (DHSC), which focused on the mental health impacts of social media. Through the group we received feedback on the challenges around age verification and children spending hours online, and learnt of existing work they have in place. The Government welcomes the companies' engagement within this forum, including the letters companies wrote to the Secretary of State for Health and Social Care following the working group meetings, outlining the positive steps many of them are taking towards addressing these important issues. However, it is clear that there is further to go and more that could be done to protect children and young people from the potential harms to their mental health from social media.

In parallel to the main consultation, we worked with the British Computing Society (BCS), the Chartered Institute for IT, who carried out a survey of over 6,500 children and young people

about online safety.[4] These responses highlight that children feel that there is a gap in their digital resilience education. They have low expectations of social media platforms in relation to their privacy, safety and security online, and younger children in particular would like to be better protected from abusive content. As we take our work forward, we will ensure that we continue to take children's views into account and put a greater expectation on companies to address all users' needs.

We also received responses from regulators, trade bodies, libraries, members of the Open Rights Group, educators, the police, political parties, technology companies and charities who support different types of vulnerable users including children and young people, as well as victims of domestic abuse, hate crime and bullying.

We consulted, and continue to draw on, the expertise of others who are already making progress in this area. The Royal Foundation's Taskforce on the Prevention of Cyberbullying published its action plan in November 2017 and we look forward to learning from the innovative pilots which they are currently undertaking. The EU ICT Coalition for Children Online is a voluntary self-regulatory principles based code for child internet safety which was established in 2012 and a number of social media providers, Internet Service Providers (ISPs) and broadcast providers remain signees. More generally, we will continue to ensure that we seek out and learn from the ever-growing pool of research into this topic.

What we learned

There was strong support across all sectors, including technology companies and charities, for the three key principles underpinning our work:

- What is unacceptable offline should be unacceptable online;
- All users should be empowered to manage online risks and stay safe; and
- Technology companies have a responsibility to their users, and for the content they host.

Our suggested collaborative approach and commitment to working with a wide range of stakeholders was also welcomed.

The majority of the responses stressed the importance of taking the right steps to ensure that creativity, innovation and free speech are safeguarded, while also protecting users from online harms. We must protect users' rights while at the same time ensuring their safety. Consultation responses also emphasised the need to ensure that our work is future-proofed so that any rules we create or initiatives we start are adaptable for new technologies.

Our research has shown significant gaps in existing evidence, not least because online harms can change rapidly, and many key trends are too new to have been the subject of longitudinal studies. Our upcoming programme of work on internet safety will include undertaking new research, on which we will be working closely with UK Research and Innovation.

---

[4] https://www.bcs.org/category/19271

Regulatory approach

A number of responses, particularly those from charities, suggested that Government should make the proposed code of practice legally binding, underpinned by an independent regulator and backed up by a sanctions regime. The NSPCC's response said that successive voluntary codes of conduct and guidance adopted by industry in the past have not delivered significant, long-lasting impact. The Children's Charities' Coalition on Internet Safety (CHIS) said that measures such as the code of practice must be linked to a regulator with clearly defined legal powers to describe minimum standards, and to enforce those standards using a range of tools including an ability to levy substantial fines.

Other charities, including 5Rights, expressed concern over the existing self-regulatory approach. The British Computing Society, in their consultation response, said that the potential for further formal legislation was a reasonable way of encouraging industry buy-in and collaboration between industry and Government. The Children's Media Foundation pointed to the number of underage children on platforms as proof that voluntary self-regulation does not work.

Meanwhile, the Internet Watch Foundation (IWF), who remove child abuse images from the Internet, said that their self-regulatory approach, in partnership with the Internet industry, has been hugely effective. The technology companies who responded to our consultation were also very supportive of a continued self-regulatory approach and pointed to successful voluntary actions in relation to a range of online harms as evidence that this approach can deliver improvements.

Code of practice and transparency reporting

Google, Twitter and Facebook stated that they would work with Government to establish the social media code of practice and transparency reporting. Google suggested that the code of must not reduce the incentive for platforms to make their own sites as safe as possible in the most effective ways possible which can be very relevant and specific to their sites. Facebook referenced the priority they give to a number of existing self-regulatory initiatives, including the European Commission's Alliance to Better Protect Children Online. In August 2018, an independent evaluation will take place to review the output of all signatories to the Alliance. Twitter suggested that the code should cover the full spectrum of communications, content and information society services used by people in the UK.

ISPs including BT, TalkTalk and Sky were all supportive of transparency reporting as long as reports had clear and understandable metrics in place to ensure easy comparison. Sky felt that for this to work some basic information-gathering powers would be needed in much the same way that Ofcom has powers to request information of other communication providers, underpinned by a sanctions regime for non-compliance.

Social media levy

The consultation responses to questions about the levy produced a mixed response. Some respondents such as Sky believed there was value in establishing a more strategic approach to the online safety funding landscape. A number of charities were positive about the benefits of using a levy to support peer-to-peer online safety schemes for children and to provide online safety resources for parents, professionals and other vulnerable users online.

However many companies, including Facebook, Google and Twitter and some charities, including the Safer Internet Centre, were keen to avoid a fundamental change in how internet safety funding for existing activities is currently delivered. Many companies and charities have already established funding programmes and were keen not to see these disrupted. The NSPCC also raised concerns about the impact of any levy, given the potential for 're-badging' existing programmes. TalkTalk suggested that a review was needed to incentivise contributions given the uneven funding model for industry-wide initiatives. They also suggested that the forthcoming UK Council for Internet Safety (UKCIS) could be responsible for distribution of the levy.

There was strong feedback that the Government needed to build a robust evidence base to inform our approach in this area.

Supporting users

The consultation responses highlighted strong support for the further development of technical solutions to tackle online harms. However, respondents stressed the need for this work to be accompanied by the further development of online safety materials and education for children, parents and adult users, as technology alone can't solve online harms.

Since the publication of the Green Paper, our 'secure by design' work has progressed and as part of our UKCCIS remodelling, we remain committed to creating a Technical Network - bringing together engineers and innovative technology businesses to discuss best practice and develop new ideas. This will support our 'think safety first' work which we will set out in more detail in our upcoming White Paper.

Since our consultation, the UKCCIS Education Working Group have published new materials to support schools in teaching online safety and the Department for Education (DfE) has conducted a public call for evidence and a wider stakeholder engagement exercise on the scope and content of Relationships Education, Relationships and Sex Education (RSE) and Personal, Social, Health and Economic (PSHE) education, including the online safety aspects of all these subjects. We remain committed to working with a wide range of partners to ensure that online safety messages are delivered to all users and parents through a range of communication channels. This will involve working closely with technology platforms, civil society groups, libraries and schools.

Working with industry

It is important to recognise that the leading social media companies are already taking steps to improve their platforms. They have developed important technical tools and successful partnerships with charities to deliver online safety initiatives - with plans to do more in this area. The growth of AI and machine learning means that algorithms are used to remove harmful content more quickly. These measures are having a positive impact. For example, Google highlighted in their consultation response that 98% of the videos they removed for violent extremism were flagged by machine-learning algorithms, and they have begun to use this technology in other areas such as child safety and hate speech.

Throughout the consultation period, we worked closely with technology firms and we have seen progress in relation to online safety in the past year. In particular, responses from the technology industry, including trade groups, flagged their existing work relating to:

- Partnerships with UK charities to deliver online safety education;
- Work with the Royal Foundation's Taskforce on the Prevention of Cyberbullying;
- Participation in existing self-regulatory initiatives such as the ICT Coalition for Children Online and the European Commission's Alliance to Better Protect Children Online;
- Terms and conditions and community rules against bullying and other types of unacceptable behaviour;
- The ability for users to report unacceptable behaviours and consequences for those who participate in this behaviour;
- Tools and features relating to privacy, security and blocking which enable users to control their experience;
- Safety centres online which provide guidance to users.

The consultation responses highlighted pockets of best practice including:

- Facebook told us that anyone who reports content is told what action has been taken and may receive additional resources to help them resolve their concern. People can also feedback on how they think Facebook did, or can appeal decisions.
- Google said that they have been working on technical solutions which can be shared across the industry. For example, in March 2017, Alphabet released a new tool called Perspective - an API that gives any developer, harassment and comment moderation tools. These tools work to tackle abusive communications from both named and anonymous accounts.
- Twitter described the tools it has specifically designed to detect and remove repeat offenders on its platform and those attempting to return following a permanent suspension.

Initiatives such as these should be evaluated and effective best practice shared so that other platforms can decide whether to introduce similar technology. We are currently considering how Government can facilitate this through our 'think safety first' work and UKCIS. Alongside this, we would also like to see the largest platforms taking this work forward and smaller platforms actively seeking out advice on best practice.

Concerns

We welcome the efforts that these companies have taken to protect users and they have learnt from feedback about online harms taking place on their platforms.

However, the range of industry responses identified three main concerns:

1. Only a small group of the largest companies are engaged with our work on online safety;
2. Companies present a strong track record on online safety but this appears to be at odds with users' feedback on their experiences;
3. Government needs to create a level playing field so that all companies are meeting consistent standards.

The NSPCC's NetAware programme identifies the main sites, apps and games that children use the most.[5] Of the 39 platforms that were identified by the charity in 2017, only five companies responded to our consultation (Facebook, Google, Oath, Microsoft and Twitter), representing 12 of the platforms. This presents a major concern - we want all platforms, particularly those popular with children, to be engaged with our safety work.

Mental health

It is clear that, while the evidence around the impact of social media and internet use is not yet conclusive, there are potential negative impacts. These include, but are not limited to, social isolation, competitive pressures, increased vulnerability, increased exposure to abusive content, increased likelihood of cyberbullying and the risk of grooming for exploitation.[6]

To discuss and tackle the issues around social media and mental health, the Department for Digital, Culture, Media and Sport (DCMS) and DHSC convened a series of roundtables with a working group of social media and technology companies (including Google, Facebook, Twitter, Oath, Microsoft, Apple and Snap Inc). These meetings discussed children and young people's online safety, with a particular focus on the impact that social media products have on children's mental health. The work focused on the themes of age verification, screen time and cyberbullying/harmful content. The Government welcomes the companies' engagement within this forum, including the letters companies wrote to the Secretary of State for Health and Social Care following the working group meetings. However, while some companies are taking steps towards addressing some of these important issues, we are clear that there is further action they could take in this area.

DCMS will therefore continue to work with DHSC to explore a range of options to take this forward, as part of our Internet Safety Strategy.

Linked to the issue of long periods of time spent online, and to better understand the relationship between social media and the mental health of children and young people up to

---

[5] https://www.net-aware.org.uk/

[6] Best. P, Manktelow. R, Taylor. B 'Online Communication, Social Media and Adolescent Wellbeing: A Systematic Narrative Review', Children and Young Services Review (2014)

25 years old, the Chief Medical Officer will be leading a systematic review to examine all relevant international research in the area. The review will inform a report in this area, due for publication next year.

Our response

The consultation responses set out a broadly common view on the problems we need to tackle. Responses from users and charities that represent children and other vulnerable users note that standards online too often fail to meet the expected behaviours set out in platforms' terms and conditions.

The Government has made clear that we require all social media platforms to have:

- Terms and conditions that provide a minimum level of protection and safety for users;
- Clear rules on unacceptable content and conduct;
- Robust enforcement of their standards.

The companies' responses suggest they already meet these expectations. However, the disconnect between user and industry responses strongly suggests that companies need to do more to manage the content and behaviours on their platforms.

The consultation has reinforced the Government's view that we are right to bring forward the social media code of practice and transparency reporting which the Prime Minister announced in February 2018.[7] The code will set a higher bar in terms of the safety provisions and terms and conditions that we expect platforms to offer users, and transparency reports will enable us to establish which companies are meeting these standards.

We believe that companies must take a more proactive approach, pre-empting potential issues on their platform before they occur. Our 'think safety first' approach will therefore focus on companies embedding safety considerations into their product development. As technologies such as machine learning become more sophisticated, we expect companies to use these to identify and remove harmful content more quickly.

The Government is also clear that we need a new, more strategic and coordinated approach to online safety funding: current approaches to funding lead to duplication of effort and gaps in provision. Nevertheless, given the mixed responses to the issue of a social media levy, we believe there is value in taking more time to gather evidence and analysis from users, companies and charities.

We will continue to ensure that comprehensive online safety education is available to all children, as well as considering how we can best support parents in tackling internet harms. This work fits into our wider activities considering online video games, gambling and the work of civil society in supporting everyone being able to access the benefits of the Internet while also staying safe. We are reforming UKCCIS and will continue to promote a 'think

[7] https://www.gov.uk/government/speeches/pm-speech-on-standards-in-public-life-6-february-2018

safety first' approach for all companies. Further details on these activities will be set out in our forthcoming White Paper.

Online safety forms just part of the work which we're taking forward under our Digital Charter. Our Charter will address wider issues such as tackling disinformation and considering innovations in digital advertising.

One of the other issues raised by the NSPCC in the consultation was the border between legal and illegal conduct online. The Green Paper focused on harmful but potentially legal content and conduct, but the initiatives which we are taking forward will also support the work being taken forward to tackle illegal harms. In addition, DCMS and Home Office will continue to work closely together to ensure that we are jointly addressing activities which could escalate to become illegal.

We are concerned that, especially for children and young people, being exposed to harmful content can have negative impacts on mental health and wellbeing. We are therefore clear that there needs to be greater focus on preventing such online content from being published in the first place. This requires companies to proactively deny access to those who abuse their services; to develop response mechanisms and apply advances in technology to automate these approaches; and for the larger companies to share these tools and techniques with other companies.

We have seen some success through the voluntary online safety approach. For example, we have seen real value from our partnerships with voluntary sector organisations such as the IWF, the UK's global leadership in the WeProtect Global Alliance, and our strong cooperation with the tech sector through the industry-led Global Internet Forum to Counter Terrorism. But we have also made clear that we are prepared to legislate where necessary. As the Prime Minister announced in January 2018, we are looking at the legal liability that social media companies have for the illegal content shared on their sites. The status quo is increasingly unsustainable as it becomes clear many platforms are no longer just passive hosts.

Whilst the case for change is clear, we also recognise that applying publisher standards of liability to all online platforms could risk real damage to the digital economy, which would be to the detriment of the public who benefit from them. That is why we are working with our European and international partners, as well as the businesses themselves, to understand how we can make the existing frameworks and definitions work better, and what a liability regime of the future should look like. This will play an important role in helping to protect users from illegal content online and will supplement our Strategy.

A global leader

The UK is not the only country affected by these issues. We know there are a wide range of countries, including Ireland, Australia, France and Germany, who are tackling the same challenges on some of the same platforms. We aim to develop a defined set of responsibilities for social media companies to provide clarity on the safety measures we

expect within a well-functioning digital economy. In doing so, we will continue to work closely with allies, including in the OECD, EU and G7, on this important work. By taking a leading role globally, we will encourage others to align with our approach - we will demonstrate the advantages of promoting online safety within a framework that also protects human rights, in particular freedom of expression.

Moving forward

As we continue to develop the Digital Charter, we remain positive about the enormous benefits the Internet brings to our society and economy. But Government has an important role to play in helping to shape an online world that works for everyone, and one that reflects the values we live by and the behaviours we expect in the offline world. As problems such as cyberbullying, abuse, trolling and sexting continue to cause harm to citizens' mental health and wellbeing and issues such as disinformation, the mass misuse of personal data, screen time and lack of age verification for social media platforms grow in prominence, it is clear that we need to continue to tackle these issues head-on and evolve our work on online safety.

That is why we are announcing our intention to publish a White Paper before the end of this year to set out more definitive steps on online harms and safety. DCMS and Home Office will jointly work on a White Paper which will set out our proposals for future legislation. It will give us the opportunity to draw together a number of different aspects of Government work, including: reporting on progress of our review of platform liability for illegal content; responding to the first stage of the Law Commission Review of abusive communications online; and working with the Information Commissioner's Office on the age-appropriate design code which is part of the Data Protection Bill. It will also allow us to draw existing work on safety together with work on the new, emerging issues, including disinformation and mass misuse of personal data and work to tackle online harms.

The White Paper will also set out plans for upcoming legislation that will cover the full range of online harms, including both harmful and illegal content. Potential areas where the Government will legislate include the social media code of practice, transparency reporting and online advertising. We believe that these measures will bring about significant benefits for all users by setting clear rules on how harmful and illegal behaviour and content should be dealt with. The code and transparency reporting will also support platforms by creating a level playing field and ensuring that all companies are contributing to safety improvements, not just the largest providers.

We will be considering new policy areas on safety that have been identified during the consultation process that warrant further work, including:

- age verification to assist companies to enforce terms and conditions;
- policies aimed at improving children and young people's mental health, including the impact of screen time;
- tackling issues related to live-streaming; and,
- further work to define harmful content.

Through this process, the Government remains firmly committed to collaborating with industry to improve online safety, in particular looking to them for answers to technological challenges, rather than Government dictating precise solutions. We are very grateful to all of the companies who have spoken to us so far in relation to online safety issues. We will continue to seek their views on our policies through a series of workshops, focus groups and consultation events ahead of the publication of our White Paper. We know that many companies are already spending time thinking about how best to tackle online harms and have partnered with experts to understand the problems in more detail. We want to continue to learn about ongoing work and will use the convening power of Government to ensure that best practice is widely shared.

We plan to work closely with industry, academia, civil society, charities and other interested stakeholders ahead of the publication of the White Paper. We will continue to work with interested parties to refine our policies where we already have a clearly defined direction of travel, including the code of practice and the transparency reports, and to progress areas of work which need further development. We will ensure that vulnerable users, particularly children, remain a central consideration in our policies.

As we take this work forward, we want to create a policy landscape where our proposals effectively tackle online harms in a changing digital landscape whilst ensuring the Internet is free, open and accessible. We are determined that the UK should lead the world in innovation-friendly regulation that protects users and enables the digital economy and new technologies to thrive.

Actions for Industry

As set out in the Internet Safety Strategy Green Paper, working closely with industry is critical to improving users' experience online. Our objective is for users to feel safer online with the freedom to explore opportunities, free from fear of abusive or harassing behaviours and harmful or illegal content.

Digital Charter

The Prime Minister's speech in January 2018 set out the importance of the Internet working for everybody.[8] The Digital Charter is a rolling programme of work to agree norms and rules for the online world and put them into practice. In some cases this will be through shifting expectations of behaviour; in some we will need to agree new standards; and in others we may need to update our laws and regulations. Our starting point will be that we will have the same rights and expect the same behaviour online as we do offline.

The Internet Safety Strategy is part of our Charter online harms work to protect people from harmful content and behaviour, through building understanding and resilience, and working with industry to encourage the development of technological solutions.

The Charter also brings together a broad, ongoing programme, which will evolve as technology changes. In addition to online harms, our current priorities include:

- Digital economy – building a thriving ecosystem where technology companies can start and grow;
- Liability – looking at the legal liability that online platforms have for the illegal content shared on their sites, including considering how we could get more effective action through better use of the existing legal frameworks and definitions;
- Data and AI ethics and innovation – ensuring data is used in safe and ethical way, and when decisions are made based on data, these are fair and appropriately transparent;
- Digital markets – ensuring digital markets are working well, including through supporting data portability and the better use, control and sharing of data;
- Disinformation – limiting the spread and impact of disinformation intended to mislead for political, personal and/or financial gain;
- Cyber security – supporting businesses and other organisations to take the steps necessary to keep themselves and individuals safe from malicious cyber activity, including by reducing the burden of responsibility on end-users.

The Charter will not be developed by Government alone. We will look to the technology sector, businesses and civil society to own these challenges with us, using our convening power to bring them together with other interested parties to find solutions. This collaborative

[8] https://www.gov.uk/government/speeches/pms-speech-at-davos-2018-25-january

approach will ensure that the UK is both the safest place to be online and the best place to start and grow a digital business.

Taking responsibility

Platform liability and illegal harms

Online platforms need to take responsibility for the content they host. They need to proactively tackle harmful behaviours and content. Progress has been made in removing illegal content, particularly terrorist material, but more needs to be done to reduce the amount of damaging content online, legal and illegal.

32% (156 individuals) of those that answered the question in our online survey agreed that social media platforms have a duty of care to remove and reduce inappropriate behaviour or content on their platforms.

We are developing options for increasing the liability online platforms have for illegal content on their services. This includes examining how we can make existing frameworks and definitions work better, as well as what the liability regime should look like in the long-run.

This is a complex issue covering all types of illegal material and we will be carefully considering the options and consequences of change. We need to tackle illegal content and ensure the digital economy can continue to thrive. To do that, we will be working closely with the full range of stakeholders who have an interest in this area, including technology companies and international partners. We will set out more detail on our approach in our White Paper.

BCS, the Chartered Institute for IT's survey of 6,500 children highlighted that in general, children are keen for offensive or abusive to be removed by platforms without the need for a complaint to be made about them.

In addition, the survey showed that there is a strong consensus among most children (up to 83% among 11-12 year olds) that social media platforms should be automatically removing abusive or offensive posts.

Terms and Conditions

Platforms use their terms and conditions to set out key information about who can use the service, what content is acceptable and what action can be taken if users don't comply with the terms. We know that users frequently break these rules. In such circumstances, the platforms' terms state that they can take action, for example they can remove the offending content or stop providing services to the user. However, we do not see companies

proactively doing this on a routine basis. Too often companies simply do not enforce their own terms and conditions.

Government wants companies to set out clear expectations of what is acceptable on their platforms in their terms, and then enforce these rules using sanctions when necessary. By doing so, companies will be helping users understand what is and isn't acceptable.

Our consultation response indicated strongly that anonymous abuse is a particular problem online. 22% (108 respondents) of those who answered the question in our online survey thought that companies should encourage people to use their real identity when using social media. Companies need to pay particular attention to taking actions against users that hide behind accounts to abuse others.

Clear Standards

We believe that it is right for Government to set out clear standards for social media platforms, and to hold them to account if they fail to live up to these. DCMS and Home Office will jointly work on the White Paper which will set out our proposals for forthcoming legislation. We will focus on proposals which will bring into force real protections for users that will cover both harmful and illegal content and behaviours. In parallel, we are currently assessing legislative options to modify the online liability regime in the UK, including both the smaller changes consistent with the EU's eCommerce directive, and the larger changes that may be possible when we leave the EU. This legislative work will help the industry understand exactly what Government and the UK public expects in relation to safety and provide better consistency across a wide range of companies. As a first step, we will be introducing our statutory social media code of practice and transparency reporting.

Our code of practice will tackle abusive and harmful conduct and content on social media, by setting a clear, common approach to online safety. And the internet safety transparency reports will allow us to track company performance on safety and benchmark companies against each other. Taken together, the code and the reports will allow Government to monitor social media companies' online safety efforts and evaluate their success.

This work aligns with the recommendations set out in the Committee for Standards in Public Life's report on Intimidation in Public Life.[9] We have already had commitments from the major social media platforms that they will publish transparency reports in the coming weeks and months.

Scope

We want to see greater consistency across platforms so that users understand what standards of behaviour are acceptable across the whole online ecosystem and what can be

[9] https://www.gov.uk/government/publications/intimidation-in-public-life-a-review-by-the-committee-on-standards-in-public-life

done to tackle content which falls short of this. The response to our consultation showed that individual companies have made progress and the majority of industry respondents have terms and conditions relating to online safety in place already. There are also a number of voluntary initiatives and pieces of guidance that have helped to set direction for online safety. But the consultation revealed that there's a gap between users' experiences online and the response from the companies.

Only 25% (121 respondents) of those who answered the question in our online survey agreed that online safety policies are consistent across different platforms.

Key to this discrepancy is whether the measures that have been taken are consistent across technology firms of all sizes. To date, it's been the largest platforms who have taken the biggest steps forward in relation to online safety. This is understandable as they have the largest user bases and the greatest amount of resource to invest in safeguarding their users. It was also these larger, more established technology companies that provided responses to our consultation and highlighted their achievements in this area.

We know that the technology sector isn't static and that children in particular, often seek to join the latest, innovative, smaller platforms. These tend to be the platforms which haven't yet developed a full range of protections which leaves users vulnerable. In recent years, we have seen a number of platforms grow significantly in a very short space of time and safety features are often only added at a much later stage.

In November, **Ofcom published their 2017 report, 'Children and parents: media use and attitudes'**. The report looks at children's media literacy and includes detailed evidence on media use, attitudes, and understanding among children and young people aged 5 - 15, as well as media access and use of young children aged 3 - 4. The research showed that almost a quarter of 8 - 11s and three-quarters of 12 - 15s have a social media profile and although these figures haven't increased since 2016, the apps being used are changing. The study also showed that almost all 8 - 11s and 12 - 15s who go online say they have been told how to use the Internet safely. However, 45% of 12 - 15s who go online say they have seen hateful content online in the last year.

This presents a challenge for Government as we want all aspects of the sector working towards our objectives. It should not just be left to the largest companies to drive forward improvements. And while recent media attention, focused on the most recognisable social media platforms, demonstrates that all companies still have some way to go, it's not right that initiatives should only focus on the biggest technology brands. In order to really improve the user experience across the whole digital ecosystem, we need to work with a much wider range of platforms. It is right that Government clearly sets out its expectations for all companies to tackle harms, particularly those which affect children and other vulnerable users. Therefore, to safeguard users and enforce consistent standards, we will encourage all social media platforms to sign up to our code of practice and transparency reporting. Where relevant, we will also encourage gaming platforms which enable social interactions between

players and other types of platforms which promote social interactions to sign up to the code and transparency reporting.

Ahead of the publication of our White Paper, we will be consider suitable definitions and will look at how we can avoid creating burdens on the smallest start-ups. In the interim however, we expect the guidance within our code of practice and transparency report template to be most relevant to those platforms which meet the following criteria:

- Have more than 250,000 users in the UK;
- Act as a commercial provider;
- Provide services to UK users online either through a website, app or similar technology;
- Have the majority of their content created by users; facilitate social networking functions, messaging or comments; and, encourage interaction between users.

We particularly expect platforms which have users under the age of 18 to demonstrate their commitment to online safety by adhering to the code and transparency reporting. The NSPCC's NetAware list of apps highlights those platforms which are popular with children.[10] These include the following:

- Dubsmash
- Facebook
- Flipagram
- Instagram
- Kik
- Musical.ly
- Omegle
- Pinterest
- Popjam
- Reddit
- Sarahah
- Snapchat
- Soundcloud
- Tumblr
- Twitch
- Twitter
- Wattpad
- YouTube
- Yubo

This is not an exhaustive list and we look forward to engaging with a wide range of companies ahead of the publication of our White Paper. We expect that growing companies will move into scope as their UK user base increases.[11]

---

[10] https://www.net-aware.org.uk/networks/?order=title

[11] If your company is within scope of our proposals, please email internetsafetystrategy@culture.gov.uk for further information.

In advance of the White Paper, we will be commissioning research to establish more detail on UK user numbers to understand the pattern of growth and decline in popular platforms. We will use this information to inform our legislative proposals. We will also assess how successful the take-up of the code and report is on a voluntary basis over the next six months to identify the types of actions which may be required to secure compliance.

Evaluation

It is Government's firm view that the code and transparency reports are a means to an end, and not an end in themselves. Our policy cannot be considered successful on the basis that a particular number of platforms have signed up to the code of practice. We instead need to focus on how these initiatives and others create a more positive user experience online. The transparency reports are therefore intended to be an evaluation tool, providing data related to the extent of users' awareness and use of reporting tools, and the levels of different types of complaints about behaviours and content online.

In the coming months we intend to work closely with platforms and 'trusted flaggers'[12] to refine the transparency reports, and evaluate the successful uptake of the code and its impact on industry and user behaviours, ahead of the publication of the White Paper. In particular we will consider any additions or changes to the code to ensure it's achieving its aim of raising the bar on safety online.

Social media code of practice

The draft code of practice sets out the principles to which social media providers should adhere in order to tackle harmful content and conduct online. By establishing common standards, companies will understand how they should promote safety on their platforms, and users will know what to expect when things do go wrong.

While the majority of major technology platforms already have terms and conditions which set out rules on the types of material and behaviour which are allowed on their platform, our survey found that 60% (296 individuals) had seen inappropriate or harmful content online, of which 67% had witnessed online bullying, 53% racial abuse and 50% online misogyny. These figures imply that these terms and conditions are either not enforced by platforms, or are out of line with what the UK public expects on safety provisions.

Girlguiding's Girls' Attitudes Survey 2017 gathered the views of over 1,700 girls and young woman in the UK aged from 7 to 21, and is the largest survey of girls and young women in the UK. Their 2017 survey included questions on their experiences of being online and showed that only 47% of girls aged between 11 and 21 think their parents understand the pressures they face online. In addition to this, 54% of girls aged 11 - 21

[12] 'Trusted flaggers' include independent organisations that have a trusted relationship with the platforms that flag content that they believe violates terms and conditions.

said they had come across unwanted violent or graphic images online that made them feel upset or disturbed.

A number of different voluntary codes of practice already exist and we have carefully considered these initiatives before drafting the Government's approach. We have also considered the impact of industry-developed guidance, including the UKCCIS practical guide for providers of social media and interactive services.[13] Given the responses to the Green Paper consultation, we believe there is value in the UK Government setting out its expectations of companies, and taking steps to ensure that all providers are complying with these measures.

Principles

Given the differences between platforms, we have developed a principles-based code that focuses on preventing harm. We do not intend to be overly prescriptive about exactly how companies should meet their obligations under the code but do expect them to take appropriate action to protect their users.

BCS's survey of 6,500 children highlighted that there is a strong consensus among most children (up to 83% among 11-12 year olds) that social media platforms should be automatically removing abusive or offensive posts. By providing guidance on privacy and controls through the code of practice, we will ensure that users have more opportunity to control who can contact them.

The draft code of practice covers the following broad areas:

- Clear and transparent reporting practices;
- Processes for dealing with notifications from users;
- Clear and understandable terms and conditions and the expectation that these will be enforced, including the action taken to prevent anonymous abuse;
- Clear explanations to the complainant about the action taken in response to their complaint ('comply or explain');
- Information about how to report potentially illegal content and contact, to the relevant authorities;
- A commitment to signpost users to useful information when they experience harmful content, as appropriate;
- Use of technology to identify potentially harmful online content and behaviours.

Our online survey consultation responses demonstrated support for our code of practice to include guidance relating to privacy and controls; reporting mechanisms with policies and metrics on take down; and information about how to identify and report illegal content to

[13] https://www.gov.uk/government/publications/child-safety-online-a-practical-guide-for-providers-of-social-media-and-interactive-services/child-safety-online-a-practical-guide-for-providers-of-social-media-and-interactive-services

the relevant authorities.

Bullying online

The code is intended to make it easier for people to report bullying content by providing guidance to social media providers as to policies they should have in place for removing this content. The Digital Economy Act 2017 section 103 sets out that the code of practice should only cover conduct which is directed towards an individual. However, we have set out additional guidance, not required under section 103, stating that the code of practice should also apply to conduct directed at groups and businesses, as users can be upset by content even if it's not directed towards them individually.

Examples of online bullying that will be addressed by the code include, but are not limited to:

- Threats of harm made to individual(s);
- Threats to share images ('outing');
- Impersonation;
- Posting personal information including information that can locate an individual(s);
- Posting text or images to bully, insult, intimidate or humiliate an individual(s);
- Posting an image of the individual(s) used without consent;
- Posting false information about someone;
- Nasty or upsetting comments;
- Sending repeated unwanted messages to an individual(s);
- Trolling - deliberately offensive or provocative online posts;
- Flaming - brief, heated exchange between two or more people;
- Dog-piling - where large communities of people target abuse at a single individual.

The code of practice does not affect how unlawful conduct is dealt with. However, it does set out that providers should provide guidance for users to report content or conduct which may potentially breach UK law to the relevant authorities.

The full draft code of practice is set out in **Annex B**.

The Government is also taking steps to tackle online intimidation and abuse in relation to elections. The Government's response to the Committee on Standards in Public Life Review of Intimidation in Public Life set out that all those in public life have a responsibility to challenge and report intimidating behaviour wherever it occurs.

The **South West Grid for Learning Trust** (SWGfL) has been working with internet companies to keep people safe online for many decades, as well as working with similar organisations around the world including the Australian E-Safety Commissioners Office, Netsafe in New Zealand and the Insafe Network of European Safer Internet Centres.

They have developed a new initiative which aims to assist internet users with the removal of certain types of online harmful content. This innovative new project builds on the

established relationships held with industry partners, and complements the work of their partners the IWF, who remove child abuse images from the Internet.

The national reporting hub will provide advice and step by step guidance on how to report different types of content, host industry partners transparency reports and, where appropriate, will provide some mediation with social media providers to ensure swift takedown of content which breaches a sites terms and conditions. The new website will be launched later this year and there will be an awareness campaign to coincide with the launch.

Annual transparency report

The annual transparency report will provide insight into how users are using reporting tools, and the support they receive from the most popular social media platforms to protect their mental health and wellbeing. By setting common metrics, we will be able to benchmark companies against each other and review progress over time. Our online survey consultation highlighted that users were particularly keen to understand what moderation policies each site has in place and how are these reviewed, as well as the number of complaints, how they've been dealt with and volume of content taken down. We will be requesting all of this information as part of our transparency report.

Eventually the transparency reports will form a key part of how we evaluate the success each platform has made towards our overall aim to raise the level of safety online. This level of data will be invaluable as Government develops future policy and interventions on online safety. We hope that these reports will be valuable for the companies too, enabling them to more easily identify and share areas of best practice.

BCS's survey of 6,500 children highlighted that there is widespread agreement that the ability to view how much bullying happens on social media platforms would be useful, and this consensus is strongest between 9-14 year olds (averaging 72% agreement in that age bracket).

We have set out in **Annex C**, a template that details the metrics that we expect companies to report on. The template includes basic, but vital and hitherto unavailable, information on the total number of UK users, total number of UK posts and total number of reports, as well as what information companies signpost users to when they have reported an issue. These figures will help us understand the context each company is working within. We are also seeking information about the company's processes for handling reports, as well as specific information relating to the types of reports which are made and how quickly they are resolved. We will include qualitative metrics to allow companies to provide additional information on trends and the handling of reports.

The transparency template requests UK-level data from social media platforms who provide services here. We plan to draw all of the company reports together to produce the first annual transparency report, to be published alongside our White Paper. This will set out, for

the first time, not just valuable data that will help us understand harm and what companies are doing to take action against it, but which companies have complied with our request.

To support the publication of our first report, we expect companies to initially supply data, covering July - September 2018, by the end of September. We will use these initial reports to further refine our transparency template. The first full transparency report will be published next year.

Google and Facebook have published initial transparency reports relating to content removed from their accounts. Twitter has also committed to publishing a transparency report in due course. However, we believe that there is significant value in Government requesting and publishing information from all companies in a consistent format so that users and other interested parties have access. We understand that, for some companies, drawing together data for the reports will require investment in their reporting systems. That is why we are publishing a draft template at this stage - so that companies can start to prepare their first return and meet with us to discuss any difficulties which they may have.

37% (158 individuals) of those that answered the question in our online survey confirmed that they had reported potentially illegal or upsetting online content on social media. Only 41% felt that their reported concerns had been taken seriously by social media companies.

Data privacy

We are conscious that, in some cases, companies will need to increase the amount of data that they gather about users and reports, to complete the transparency template. Ahead of the publication of our White Paper, we will work with companies, user groups and the Information Commissioner's Office to ensure that this can be done in a way which does not invade individuals' privacy nor make the reporting process more burdensome. When the transparency report is published, figures will only be presented at an aggregated level, and no individual user will be identifiable. While we recognise that some particularly sensitive reporting requirements, such as users' gender, sexual orientation or age, would be useful to understand bullying aimed at particular individuals with protected characteristics, at this stage we do not propose to request the information. Instead, we are requesting that reports of abuse are categorised based on which attribute they relate to as part of the moderation process. We will however, keep this under review ahead of the publication of the White Paper.

Social media levy

The Green Paper asked for views on a social media levy that would support greater public awareness of online safety and enable preventative measures to counter internet harms, including both new initiatives and existing programmes.

The consultation responses show that there are already significant equities at play in terms of online safety funding. Social media companies highlighted the benefit of Government

support for companies coming together to pool resources and tackle specific harms: charitable organisations were broadly supportive but noted the complexity and the value of existing partnerships with industry. There is no singularly agreed proposal for preserving and improving this landscape, and we are aware that companies and charities are undertaking a wide range of work to tackle online harms.

Only 15% of individuals who responded to our online survey consultation agreed that a centralised social media levy would be an effective way for industry to provide a contribution to tackling online harms. Therefore it's important that we hold further discussions to understand these concerns and collaborate with our key stakeholders to agree an effective approach.

Reallocating resources without disturbing the status quo will be challenging, but the current system leads to duplication of effort, some vulnerable users aren't adequately supported and users can receive conflicting messages which leads to confusion. We strongly believe that there is definite value to be added from the convening power of Government to ensure that resources and funding are maximised across the digital ecosystem. However, before we disrupt any existing initiatives, we believe that it is right that we take the time to agree the best approach to realise sustained, significant investment to counter online harms.

By providing clear direction, Government will be able to efficiently direct investment to cover a range of user needs and ensure consistent safety messaging across platforms. By working collaboratively we will ensure that safety work has a greater impact than ever before and we can ensure that initiatives are appropriately evaluated and their success measured. This will help us generate additional evidence about how users can be best supported and how positive online behaviours can be encouraged.

We want Government to be at the centre of setting a new, strategic approach to online safety funding, while maintaining the benefits of current funding streams from the major technology companies. We have convened a working group of online safety and children's charities to provide input on this issue and we welcome the positive engagement that we've received from these organisations. Moving forward, we will be holding a series of roundtables with industry and charities to identify the best way forward. In parallel we will commission further research to identify what the costs of online harms are and which harms have the greatest negative impact on society. We will draw these pieces of work together in a meeting chaired by our Secretary of State before summer to identify how to achieve a more strategic approach to funding. We will use these discussions to inform our approach which will be set out in our forthcoming White Paper.

As we carefully consider plans for the levy's delivery, we will ensure that it is proportionate and does not stifle growth, investment or innovation in the UK with particular steps taken to protect start-ups and smaller businesses from undue burdens. We will be considering any levy in the context of existing work being led by HM Treasury in relation to corporate tax and the digital economy.

Respondents to our online safety survey suggested that the levy could be used to fund education programmes and resources for children and parents, alongside peer-to-peer support networks to help children and young people. As set out in the Green Paper, we are aware of some excellent schemes which are already benefiting users and we will be looking at how we can support these further.

'Think safety first' and links to 'secure by design'

In order to create a safer digital ecosystem in the future, we need to influence the development of new and emerging platforms. Critical to this work is persuading developers and designers to include safety features in new applications and platforms from the start.

BCS's children's survey highlighted that only 30% of the 12 year olds surveyed agreed that "most companies think about the online safety of people your age when they are making their websites or apps".

To achieve this, we will build on the *Secure by Design* model[14] and establish new safety baselines for digital products and platforms. We will partner with consumer groups and retailers to agree standards and promote best practice which will help to protect users' safety and wellbeing.

The ***Secure by Design*** report advocates a fundamental shift in approach: moving the burden away from consumers having to secure their devices and instead ensuring strong security is built into consumer "internet of things" (IoT) products by design. It also sets out the need for greater action by Government and industry, and proposes a range of measures to better protect citizens and the wider economy.

The central proposal of this report is a draft Code of Practice aimed primarily at manufacturers of consumer IoT products and associated services. It has been developed through extensive engagement with industry and subject matter experts and sets out thirteen practical steps to improve the security of consumer IoT.

This work will also closely align with the age appropriate design code that is included within the Data Protection Bill that is currently before Parliament.

As set out in the Green Paper, we will also create a technical network, bringing together specialists from a wide range of technology companies to anticipate future online harms and

[14] DCMS, 'Secure by Design: Improving the cyber security of consumer Internet of Things' (March 2018) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf

take steps to prevent them. We will build the network using our UKCCIS associate member contacts and partners.[15]

48% (189 individuals) of those that answered the question in our online survey agreed that more safety information about digital products and platforms should be available to consumers/ users.

Update on remodelling of UKCCIS

The Green Paper set out objectives for remodelling UKCCIS. Although UKCCIS is generally seen as a model of global good practice, the Council's Executive Board has recently lacked strategic direction, hampering its ability to set and deliver key objectives. The proposals set out in the Green Paper included widening the scope of the Council to cover all users, not just children, and changing its name to the UK Council for Internet Safety (UKCIS); establishing a smaller, higher-profile Board and reconsidering the role of the Council's working groups.

Council members such as Childnet International were supportive of our desire to improve the Board's agility and its ability to deliver against strategic priorities. TalkTalk also said that they were supportive of reforming existing processes to give a greater degree of coordination and accountability. As we remodel the Council, we will introduce a smaller Executive Board which will help to drive the strategic agenda for the Council, work to clearly defined objectives on safety, and provide a direct link between Ministers and the working groups. In addition, we recognise that there are differences in the education systems, legal frameworks and third sector support networks between the devolved nations so we will take steps to ensure that UKCIS's work reflects this.

As we remodel UKCCIS, we will also:

- improve the mechanism for gathering views on emerging issues,
- increase accountability for working group projects and strengthen links between the working groups and Board, and
- establish a clearer role for associate members.

We will formally launch the remodelled UKCIS with updated priorities, alongside our White Paper. This will ensure that the Council fully aligns with our strategic objectives and wider work relating to online safety.

In the meantime, the Council and its working groups will continue to play an important role in gathering evidence relating to online harms, technology changes, building digital resilience and supporting educators and parents.

Expanding remit

[15] Individuals or organisations that would like to contribute to this work should contact internetsafetystrategy@culture.gov.uk.

A number of the consultation responses from children's charities and campaigners flagged concerns about expanding the remit of UKCCIS to cover all users. As set out in the Internet Safety Strategy Green Paper, we believe that expanding the remit of UKCCIS to cover adults, as well as children, will bring significant benefits and it's important that the Council is aligned to the scope of the Strategy. We will maintain a focus on children's needs by:

- Ensuring children have the opportunity to share their views with the Executive Board;
- Maintaining at least one working group which will focus on children's online safety;
- Ensuring that children's charities continue to be represented on the Executive Board;
- Setting priorities relating to children's online safety and monitoring the Council's progress on these.

Putting these provisions in place will take time as we are aware that establishing a forum through which children's views can be gathered needs to be properly resourced and structured. We are currently working with children's charities who already have young people advisory boards so that we can learn from their experiences and take decisions based on established best practice.

4. Supporting children and parents

Education

Safer Internet Day (SID) 2018, is organised in the UK by the UK Safer Internet Centre - over 1700 organisations delivered activities across the UK including schools, businesses, charities, Government and police services. 45% of UK children aged 8 - 17 and 30% of UK parents heard about SID.

To coincide with SID events, the UK Safer Internet Centre published findings from new research which surveyed 2,000 8 - 17 year olds: 'Digital Friendships: the role of technology in young people's relationships'. The report revealed how central technology is to young people's relationships, as well as highlighting the positive and negative role it can play in their friendships. The findings showed how young people are proactively helping to build a better Internet and that they want support from adults to do so, with 77% of 8-17s saying they wanted their parents or carers to be there for them if something worries them online.

In response to the Green Paper, we received a number of written consultation responses from individual teachers as well as organisations which represent schools. These highlighted a range of online safety activities taking place at both a local and national level. For example, the Independent Schools Council highlighted that the Headmasters' and Headmistresses' Conference (HMC) has been running a "Tech Control" campaign working with Digital Awareness UK. The resources, which were tested with heads, teachers and pupils, have been shared with over 18,000 schools and one embedded video received over one million views.

BCS's survey of 6,500 children highlighted that children aged 8-13 would welcome more education in schools about online safety (with an average of 72% believing this, including 87% of 9 year olds).

The Government wants to help all schools to deliver a high-quality education that ensures all young people are equipped to have healthy and respectful relationships in both the online and offline world, and leave school with the knowledge to prepare them for adult life. This is why we have introduced a new national computing curriculum for key stage 1 to key stage 4, which includes content on online safety including how to use technology safely, responsibly, respectfully and securely. It is compulsory in all state-maintained schools and free schools and academies can use it as a benchmark.

The UK Safer Internet Centre's **Professionals Online Safety Helpline** was set up in 2011 to help the children's workforce with online safety issues. The helpline supports all professionals who work with children and young people and can help with any online

safety issues, including privacy, cyberbullying and gaming. The Professionals Online Safety Helpline also has direct channels to escalate concerns to social media companies and many websites. Further information can be found here: https://www.saferinternet.org.uk/professionals-online-safety-helpline

The Children and Social Work Act 2017 places a duty on the Education Secretary to make Relationships Education at primary and Relationships Sex Education (RSE) at secondary compulsory through regulations. The Act also provides a power for the Secretary of State to make PSHE, or elements therein, compulsory in all schools in England, subject to careful consideration.

DfE have conducted a thorough engagement process on the scope and content of the subjects, involving a wide range of interested stakeholders, and a public call for evidence exercise. In particular, one of the questions in the call for evidence sought views on the important aspects of ensuring safe online relationships that should be covered in Relationships Education and RSE. DfE are currently assessing responses to the call for evidence and the findings will be combined with evidence from the engagement process to support decisions on the content of the subjects and on the status of PSHE.

The preliminary findings from the engagement process have shown that some stakeholders highlighted the need for young people to be aware of some of the negative risks from social media, including what constitutes online bullying and its negative effects, and how this might impact their mental health and wellbeing. It is vital that children and young people of current and future generations understand that cyberbullying and equivalent negative activity online is not the norm and will not be tolerated. Some also mentioned the importance of learning about privacy settings, including the dangers of sexting and talking to strangers online.

Following a full analysis of the responses to the call for evidence, the Department will develop regulations and accompanying statutory guidance for the new subjects and both will be subject to public consultation followed by a debate on the regulations in Parliament.

As part of Safer Internet Day, the UKCCIS Education Working Group published its framework '**Education for a connected world**'.[16] The framework describes the digital knowledge and skills that children and young people should have the opportunity to develop at different ages and stages of their lives. It highlights what a child should know in terms of current online technology, its influence on behaviour and development, and what skills they need to be able to navigate it. The framework will enable teachers to develop effective strategies for understanding and handling online risks.

UKCCIS are seeking feedback on this document from education professionals and will use this information to inform our ongoing safety education work. The Education Working

16 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/683895/Education_for_a_connected_world_PDF.PDF

Group are continuing to develop further resources which will support the teaching of online safety in schools.

DfE recently also consulted on revisions to the statutory safeguarding guidance for schools in England, *Keeping Children Safe in Education* (KCSIE). This included considering how to strengthen guidance and support for schools and colleges to keep children safe online. Revised guidance will be published later this year. UKCCIS resources will be highlighted/ referenced in the upcoming statutory safeguarding guidance. These include: guidance on how to respond to a sexting incident and guidance for the Governing Board on checking a school's online safety approach. KCSIE is very clear that schools and colleges should ensure their staff receive safeguarding training, including online safety.

In partnership with the BCS, The Chartered Institute for IT, BT is upskilling primary school teachers to deliver the computing curriculum through the Barefoot Computing programme providing free resources and volunteer-led workshops to take teachers through the materials available. Over 1.5 million children have been reached through 50,000 teachers across the UK. Barefoot Computing is now used in over 50% of primary schools in England and Scotland and 40% in Wales and Northern Ireland. A campaign which started in January 2018 will encourage further uptake through a new lesson plan for 5-7 year olds to get them discussing online safety while playing a fun 'Safety Snakes' game with a programmable Beebot.

The DfE are investing £84m of new funding over the next four years to deliver a comprehensive programme to improve the teaching of computing and drive up participation in computer science, particularly amongst girls. This will include a national training programme to upskill up to 8,000 existing teachers and a new National Centre for Computing Education that will provide free resources that cover the whole curriculum, including online safety.

In **Scotland**, there is a similar commitment to delivering an educational experience which ensures all children and young people develop the knowledge and understanding, skills, capabilities and attributes which they need for mental, emotional, social and physical wellbeing.

Curriculum for Excellence is the national approach to learning and teaching for young people aged 3 to 18 in Scotland. It provides significant flexibility, within broad national guidelines, for teachers to develop lessons which best meet the needs of individual learners. Teachers, head teachers and other professional educational practitioners are best placed to decide what is taught in Scotland's schools. The flexibility afforded to educational practitioners means Scotland does not have a statutory curriculum.

In 2017 the Scottish Government published refreshed anti-bullying guidance 'Respect for All: The National Approach to Anti-Bullying for Scotland's Children and Young People'. This approach forms part of wider attempts to improve the health and wellbeing of children

and young people. It fits in with ongoing work to ensure children and young people feel safe and secure and are able to build up strong and positive relationships with their peers and with adults as well as our work to promote positive behaviour. This approach also sets out a common vision and aims to make sure work across all agencies and communities is consistently and coherently contributing to a whole school approach to anti-bullying in Scotland. It makes clear online bullying should not be treated differently to face-to-face bullying, and that all policies and practice should therefore include advice on online bullying. Scottish schools may use the Guidance on Developing Policies to Promote the Safe and Responsible use of Mobile Technology in Schools or the 360 Degree Safe e-safety self-review tool.

To support the roll out of the anti-bullying guidance, the Scottish Government funded anti-bullying service 'respectme' will continue its work with local authorities and other organisations to build confidence and capacity to address bullying effectively.

In addition, relationships, sexual health and parenthood (RSHP) education is an integral part of the health and wellbeing area of the school curriculum in Scotland. This aspect of the curriculum is intended to enable children and young people to build positive relationships as they grow older and should present facts in an objective, balanced and sensitive manner within a framework of sound values and an awareness of the law on sexual behaviour. A new online teaching resource is being developed which will seek to fill emerging gaps such as gender roles at transition from early years to primary and factors that are affecting the lives of young people such as social media; sexting; online grooming; easier access to pornography; peer pressure; Child Sexual Exploitation; consent; and, healthy relationships. This new resource is expected to be finalised during 2019.

The Parent Zone section of the Education Scotland website includes information for parents on, amongst others, internet safety.

Education in **Wales** is currently going through a major reform programme. The new curriculum looks to equip all our young people for life. It has four key purposes to support all learners to become ethical, informed, healthy and confident individuals who are ready to learn throughout their lives as they become citizens of Wales and the world.

The new curriculum will have six 'Areas of Learning and Experience (AoLE) one of which is Health and Well-being. This will draw on subjects and themes from mental, physical and emotional well-being and will also consider how the school environment supports children and young peoples' social, emotional, spiritual and physical health and well-being.

Digital Competence will also be a cross curricular theme, together with literacy and numeracy, within the new curriculum. The Digital Competence Framework (DCF) is the first element of the new curriculum and was made available in September 2016. The Framework has four strands of equal importance (Citizenship, Interacting and collaborating, Producing, and Data and computational thinking).

The Citizenship strand focuses on learners developing the skills and behaviours to contribute positively to the digital world around them which includes protecting themselves on-line. The strands includes the elements of 'Identity, image and reputation', 'Health and well-being', 'Digital rights, licensing and ownership', and 'Online behaviour and cyberbullying'. These skills will help learners to critically evaluate their place within the digital world, so that they are prepared to encounter the positive and negative aspects of being a digital citizen.

The interacting and collaborating strand also allows learners to explore both formal and informal methods of communication including social media and instant messaging. Learners will not only look at how to store data, but also the implications of data laws and how to share information appropriately.

The Welsh Government is committed to safeguarding and promoting the well-being of all children and young people in Wales. We expect all staff and volunteers working with children to share this commitment. We have published statutory guidance, Keeping learners safe, which sets out the role of local authorities, governing bodies and proprietors of independent schools to ensure they have effective systems in place to respond to safeguarding concerns.

There is an extensive online safety programme which builds on existing expertise and activities to develop sustainable online safety activities across Wales – as well as increasing the amount of resources available in Welsh. The project includes the following online safety activities:

- development and publication of a range of bilingual teaching resources focused on specific issues in online safety;
- development and publication of a range of resources to support learners and carers;
- provision of a self-evaluation tool - 360 degree safe Cymru and targeted support and promotion of its use;
- provision of a broad programme of online safety training to up-skill education practitioners;
- development of content and news features on online safety issues;
- development of an online safety training module for educational practitioners and governors.

The Online Safety Zone is a dedicated area on Hwb which has been designed and developed to support online safety in education across Wales. In addition to news articles and features, the Online Safety Zone hosts a range of teaching resources on various online safety issues to help keep learners safe online. It provides access to sources of guidance and advice to learners, education practitioners, education professionals, governors, parents and carers and links to training and further expert support.

Schools response to cyberbullying

All schools in England are legally required to have a behaviour policy with measures to prevent all forms of bullying (including cyberbullying) among pupils. We recognise that bullying online is just as prevalent as face-to-face, and it is increasingly becoming a means by which face-to-face bullying is extended beyond the school day.

YoungMinds and **The Children's Society**, in partnership with Alex Chalk MP, set up an inquiry into the impact of cyberbullying on social media on children and young people's mental health. To inform the inquiry, YoungMinds and The Children's Society carried out a survey of 1,089 children and young people aged 11 - 25 to hear about their views and experiences of bullying online. The survey showed that 61% of young people had their first social media account at age 12 or under, despite the guidelines stating you must be 13 years old to have an account. In addition to this, 60% of young people reported having seen somebody be harassed or bullied online and 83% said that social media companies should do more to tackle cyberbullying on their sites.

Government have already put in place a number of powers and a range of support to enable schools to prevent and tackle cyberbullying, including giving head teachers the power to regulate pupils' conduct when they are not on school premises and are not under the lawful control or charge of a member of school staff. Where bullying outside of school is reported to teachers, it should be investigated and acted on.

DfE are also providing £1.75 million, over 2 years, for four anti-bullying organisations to support schools tackling bullying. This funding includes projects targeting bullying of particular groups, such as those with special educational needs and disabilities (SEND) and those who are victims of hate related bullying, along with a project led by Internet Matters to report bullying online. The project led by the Anti-Bullying Alliance is focused on tackling bullying related to SEND. It includes face-to-face training for teachers along with helplines and online information for parents.

In December 2017, **5Rights** published their report **'Digital Childhood'** which addresses childhood development milestones in the digital environment. The paper describes the narrative of children and the digital environment and defines their needs as a series of opportunities and requirements that align with their age and meet their development goals.

Schools can help to prevent cyberbullying by educating their pupils about acceptable ways to behave online. DfE is working to address the manifesto commitment to *"educate today's young people in the harms of the Internet and how best to combat them, introducing comprehensive RSE in all primary and secondary schools to ensure that children learn about the risks of the Internet, including cyberbullying and online grooming",* taking into account the responses from the recent call for evidence on Relationships Education, RSE and PSHE.

In December 2017, **Brook** (a young people's sexual health and wellbeing charity) and the Child Exploitation and Online Protection command within the National Crime Agency (CEOP), published **'Digital Romance'** - a report that set out to explore how young people

are using digital technologies in their romantic relationships. The research provides an understanding of the way in which young people use technology to meet new partners, communicate in relationships and break up, alongside what they believe the benefits and risks to be - which often greatly differs from the assumptions of professionals and parents/ carers.

We are also working to identify how we can best help schools to create an atmosphere of respect, which will reduce bullying behaviour both offline and online. This work will help schools deliver on their range of existing equalities, behaviour, bullying and safeguarding duties in a way which minimises the burdens upon them.

Children in need, care and care leavers

Consultation responses from the Children's Commissioner, Childnet International and Guardian Saints all highlighted the particular needs of children in care and the need to support those who cared for them. The Office of the Children's Commissioner's research emphasises the importance of all young people living in the care of the state being kept safe from harm online as well as accessing the benefits.

The Government is clear that foster carers should get the training and support they need to meet the needs of the children they look after and this is reflected in the statutory framework. Currently all pre-approval foster carers complete the 'Skills to Foster' training and all foster parents complete the Training, Support and Development Standards within 12 months of approval as a foster parent.

The responsibility for providing training falls to the fostering agency supporting the foster carer. We know that there are numerous specialist training courses on internet safety available to foster parents. Some agencies have developed policies, which ensure that all young people have access to the Internet, and which promote the positive use of social media, for example, to keep in touch with friends and birth families and to stay safe online.

The recent reviews of foster care (conducted by Sir Martin Narey and Mark Owers, and the Education Select Committee) made a number of recommendations in relation to supporting foster parents and DfE are considering training as part of the wider package of support for carers. DfE will also consider whether there is more consistency needed in the approach that agencies take to training foster carers to help prepare and protect the young people in their care when they are online.

DfE published Quality Standards for Children's Homes in 2015. The guide to these standards states: "Children should have access to a computer and the Internet to support their education and learning, unless there are specific safeguarding reasons why this would be inappropriate. In such cases, the home should consider whether and how it can support the child to access a computer and the Internet safely."

We expect that all providers will take into account the Quality Standards when planning and delivering services – they set a benchmark for Ofsted inspections. DfE are considering whether similar Quality Standards would be of benefit in fostering services.

Although the majority of care leavers are over-18 and legally adults, we recognise that they remain vulnerable to a range of safeguarding risks, including risks associated with social media. Unlike children in care, care leavers do not have an allocated social worker or primary carer, as the majority of care leavers live independently or in some form of semi-independent accommodation. Care leavers are, however, supported by a Personal Adviser, whose role is to help the young person to make a successful transition from care to independent living.

Following changes introduced through the Children and Social Work Act 2017, the offer of Personal Adviser support is being extended to all care leavers to age 25. As a result of this, and other recent changes, DfE will be updating the statutory guidance that sets out what support local authorities are required to provide to care leavers and will take this opportunity to include guidance to Personal Advisers on how they can support care leavers to keep safe online.

Support for parents

In January 2018, **Internet Matters** published **'Parenting Digital Natives: Concerns and Solutions'.** The report provides insight on what parents of children aged between 4 – 16 think about their children's digital lives and what concerns they have about online risks. The research asked 2000 parents what concerns them most, and found there were two sorts of worries. The established concerns about online content conduct, and contact were still front of mind, and parents are also increasingly concerned about the potential influence of vloggers. Internet Matters will be publishing new research on vlogging and livestreaming in June.

Through its website**,** internetmatters.org, Internet Matters provides information and advice to parents to help them keep their children safe online. Of parents surveyed 88% said they would recommend the resource to others and 84% were better prepared to address future concerns with their children.

As highlighted in the Green Paper, we remain committed to equipping parents with the information which they need to help prevent future online harms, and will seek to deliver this information through a wide variety of routes.

Parents who completed our online survey highlighted that they would be interested in further online safety information relating to personal data protection, mental health impacts, cyberbullying, critical thinking and deception/ fraud online. We will be working with online safety charities to ensure that this information is easily accessible.

Departments across Government have strong links with online safety charities and initiatives which support young people online and their parents. The DfE will share messages relating to online safety through parent and community champion outreach programmes. We will continue to promote the materials which are available and commission UKCIS to identify any gaps in resources so that we can address these.

Parent Info (www.parentinfo.org) is a website for parents, covering all of the issues amplified by the Internet. Its newsfeed function enables schools and family-focused organisations to host and share expert advice and information through their own websites.

The aim is prevention; by preparing parents to effectively tackle sensitive issues, Parent Info is able to raise their confidence in their digital parenting and making informed decisions about addressing the risks their children face. To date, Parent Info has commissioned content from over 40 organisations specialising in topics such as sex, relationships, online safety, body image, peer pressure, radicalisation, extremism and mental health.

Since July 2015, over 4,500 schools and organisations have registered with Parent Info, allowing them to integrate this content into their websites and existing communication platforms, and promote articles to the parents and carers they support in a timely and sensitive way.

Parent Info is a collaboration between the National Crime Agency's Child Exploitation and Online Protection (CEOP) Command and Parent Zone, the leading provider of information, training and support, making the Internet work for families.

Between April 2017 - April 2018, the website had 502,217 visitors - a 14% increase compared to the same period 2016/17.

We are also ensuring that technology companies continue to support parents by developing technical solutions to online harms. In recent months, a number of recognised companies have launched new products for the UK market. For example, Google recently launched their Family Link app. The app allows parents to create and manage Google accounts for children under 13 years old and offers tools and information, including details on which apps their child is using and the ability to approve downloads.

The **Microsoft Family Account** is a free service which keeps children safer while using Microsoft's products and services. The service allows parents to schedule screen time for their children, determine what materials they can access on apps, games and web, and provides weekly email reports on their children's online activity. In addition to this, Microsoft's search engine Bing offers a SafeSearch setting for parents, which keeps sites that contain sexually explicit content out of the search engine through setting the filter to 'strict', 'moderate' or 'off'.

Mental health

The joint DHSC and DfE Green Paper on children and young people's mental health,[17] published in December 2017, contained three key proposals for improving links between mental health services and schools. The proposals are:

- to create new Mental Health Support Teams, supporting children and young people in or near schools and colleges;
- incentivising schools to identify and train a Senior Designated Lead for mental health; and
- piloting a four week waiting time standard for access to NHS mental health services for young people.

The Green Paper consultation closed on 2 March 2018 and received over 2,500 responses. The responses are currently being analysed and a response to the consultation, setting out further details around implementation of the proposals, will be published in due course.

To support the three key proposals, the Green Paper also included further activities to address wider mental health needs of children and young people, including around social media and children and young people's mental health.

In 2017, **Twitter** hosted a workshop to identify innovative campaigns that can leverage the platform to tackle mental health issues. When these campaigns are ready to launch Twitter's AdsForGood programme gives the organisations pro-bono advertising credits to test their ideas.

To discuss and tackle the issues around social media and mental health, DCMS and DHSC convened a series of roundtables with a working group of the main social media and technology companies (including Google, Facebook, Twitter, Oath, Microsoft, Apple and Snap Inc). These meetings discussed children and young people's online safety, with a particular focus on the impact that social media products have on children's mental health. The work focused on the themes of age verification, screen time and cyberbullying/harmful content.

The Government welcomes the companies' engagement within this forum, including the letters companies wrote to the Secretary of State for Health and Social Care following the working group meetings. However, while some companies are taking steps towards addressing some of these important issues, we are clear that there is further action they could take in this area.

DfE will therefore continue to work with the DHSC to explore a range of options to take this forward as part of our Internet Safety Strategy.

---

[17] DHSC and DfE, 'Transforming children and young people's mental health provision: a green paper' (December 2017) https://www.gov.uk/government/consultations/transforming-children-and-young-peoples-mental-health-provision-a-green-paper

Linked to the issue of long periods of time spent online, and to better understand the relationship between social media and the mental health of children and young people up to 25 years old, the Chief Medical Officer will be leading a systematic review to examine all relevant international research in the area. The review will inform a report in this area, due for publication next year.

The **British Board of Film Classification** (BBFC) take into account mental health issues relating to young and vulnerable in its classification decisions across websites and other audio-visual material. The BBFC draws on expert advice in order to do this, for example through maintaining a close relationship with the Samaritans and other suicide prevention experts in relation to classification policy on issues relating to suicide. In addition to this, BBFC have commissioned research to inform their classification policy, including into the potential effects of depictions of sexual, sexualised and sadistic violence in film and video.

The BBFC and the Dutch regulator, NICAM, have developed You Rate It (YouRi) in order to provide age ratings for user generated content (UGC), in recognition of its being an increasingly significant source of content online. YouRi is a tool that provides age ratings for UGC which is available on online video-sharing platform services, and takes the form of a simple questionnaire, designed to be completed by those uploading videos onto a platform, by the crowd, or by both. The tool was piloted by the Italian website 16mm.it with encouraging results: 81% of all videos available on the site received a classification during the pilot period. YouRateIt is available to video and social media platforms as part of their content compliance and age labelling mix and BBFC and NICAM are looking in 2018 to find a further partner, ideally in the UK or in continental Europe, to undertake a larger scale trial.

5. Wider Work

Government's work on internet safety covers activities with a wide range of stakeholders and draws on expertise from a number of different departments. We are continuing to promote a collaborative and joined up approach by partnering with technology companies, charities, civil society, academics and other research groups to establish the most effective ways of tackling online harms. This work falls under the umbrella of the Digital Charter, which enables us to draw the strategic links between policies and maximise their impact.

Disinformation

The UK Government takes the issue of disinformation, or 'fake news' very seriously. Disinformation is the deliberate creation and sharing of information known to be false. The motives for creating or sharing such material may be commercial, ideological or political – including to advance domestic and geo-strategic objectives.

A survey of 1,684 British adults aged over 18, conducted by YouGov in January 2017 for Channel 4, showed that concern about fake news is more acute among young people, with 57% of 18 - 34 year olds stating they are worried about fake news - compared to 49% of UK adults. The survey also found that in practice people find it difficult to distinguish fake news from real news stories. When those surveyed were shown six individual news stories, three of which were true and three of which were fake, only 4% were able to correctly identify them all. In addition, despite half (49%) of respondents to the survey stating they were either 'very or fairly confident' that they could tell the difference between a fake news story and a real news story, half of this group believed at least one of the fake news stories shown.

Our democracy is built on trust in electoral processes; confidence in public institutions; a free, open and accessible media; and free, open and trusted forums that allow different voices to contribute to the public discourse. These values and principles are at the heart of the UK's reputation and influence across the globe. But others may try to abuse these core facets of our democracy to manipulate and confuse the information environment to suit their own needs and undermine trust.

The **BBC website 'Own It'** was launched on Safer Internet Day this year and aims to help 9 - 12 year olds get the most out of their time online. Through providing information on online safety, the website helps children in taking their first steps online.

From March 2018, the BBC will offer all secondary schools across the UK resources to tackle the rise of 'fake news'. The scheme will build on the established networks of School Report and over 1,000 schools will be offered mentoring in class and online, aiming to equip children with the knowledge and tools they need to distinguish between responsible journalism and fabricated news.

Although robust mechanisms are in place to address the spread of disinformation in the broadcasting and press industry, we believe more work is needed - particularly in relation to information which is available online. Our focus is in four key areas:

- More research to better understand the problem;
- Education and guidance to ensure people have the skills they need to tell fact from fabrication;
- Developing technological solutions with industry partners, including reviewing algorithmic responses;
- Considering whether we have the right regulation in place.

This work forms part of the Digital Charter, which aims to ensure that the UK is the safest place in the world to be online. This will be a collaborative approach and we are actively engaging with industry partners to address this issue. In March 2018, DCMS and Demos jointly hosted a workshop with academics, media and representatives from the tech sector. This discussed potential uses of technology such as text analysis and machine learning to identify disinformation online. Going forward, we will continue to work with industry, civil society and international partners to tackle this problem.

Centre for Data Ethics and Innovation

Advances in the ways we use data are transforming our lives in profound and unexpected ways. These developments have the potential to be hugely positive, but they are also giving rise to new and unfamiliar ethical challenges. Increasingly sophisticated algorithms can glean powerful insights, which can in turn be deployed in ways that influence or even manipulate the decisions we make, or target the services and resources we receive in ways that may be unfair or discriminatory. Data use in these contexts raises fundamental questions for society around accountability, transparency and, ultimately, the level of control we retain over the decisions that shape our lives.

To ensure that we can maximise the benefits and minimise the risks associated with these new uses of data, we need a governance regime that is able to provide clarity and confidence to citizens and businesses alike. To this end, the Government has committed to establishing a Centre for Data Ethics and Innovation. Working in dialogue with industry, academia, civil society and the broader public, the Centre will advise Government and regulators on the measures that are needed to ensure and enable the safe, ethical and innovative use of data.

Digital markets

The digital era has led to a transformation in the way that consumers interact with business. This is a revolution of choice, convenience and affordability – people now have access to a global market in goods and services at the click of a button. This has sharpened competition in many markets, as well as providing significant rewards to innovation and entrepreneurship.

The nature of digital markets provides firms with access to a huge amount of data on consumers, enabling them to serve consumers in highly sophisticated ways. We want to make sure these markets work for everyone – for consumers, businesses and society as a whole. We want to make sure that the markets of the future are designed to encourage competition and innovation, and at the same time ensure that consumers are treated fairly, their data is held securely and used appropriately, and their privacy is respected.

We are consulting on these issues through the Consumer Green Paper as part of wider work to ensure that our regulatory environment accounts for the opportunities and challenges of an increasingly digital economy.

Online advertising

Online advertising is a crucial part of the digital economy - it is a major source of revenue both for major tech platforms and content creators (including the media and creative industries). And it has an impact on society more widely, for instance when used to influence political opinion.

There are a number of differences between online advertising and its traditional forebears. Most importantly, personal data is used in increasingly sophisticated ways to target ads to very specific demographics.

The **Advertising Standards Authority** regulates online as well as traditional media. Their remit and codes have evolved to take into account changing technologies and emerging platforms that have provided advertisers with new avenues to promote their products and services. For example, they have upheld complaints relating to Alpro (UK) Ltd where a Tweet from the television presenter AJ Odudu's Twitter account promoting an Alpro product was not identifiable as an ad, and Diamond Whites where reality TV star, Marnie Simpson advertised a tooth whitening product to her followers on Snapchat without making it identifiable as an ad.

In addition, the Committee of Advertising Practice has also published new guidance dedicated to children and age-restricted ads online. The guidance advises advertisers to use a range of interest targeting factors to complement and address some of the imperfections of self-reported age data. By doing so, advertisers of age-restricted products are better able to reach their target audience, while excluding children and young people who benefit from explicit protections under existing rules.

As part of the Digital Charter's work programme, Government will work with regulators, platforms and advertising companies to ensure that the principles that govern advertising in traditional media – such as preventing companies targeting unsuitable advertisements at

children – also apply and are enforced online.[18] We are also undertaking further work to understand the impacts which targeted advertising may have both on individuals and society as a whole.

The advertising industry helps fund **Media Smart**, a not-for-profit organisation that creates free educational materials for schools and youth organisations, for teachers, parents and guardians, to help young people evaluate the advertising they come across in their daily lives. The 22 supporting partners include Facebook, Google/YouTube, Sky, Viacom, ITV and Channel 4. Since its relaunch in 2015, the programme has focussed strongly on building digital resilience in 7 – 16 year olds by producing social media and digital resources that help them understand the different ways they are advertised to online. Recent work with the Government Equalities Office, PSHE Association, NSPCC and Childline has taken this a step further by looking at how young people's body image is impacted by the content they see online. Media Smart's most recent campaign, the Boys' Biggest Conversation, concentrates on young men, their body image and the effect it has on their mental wellbeing. Media Smart resources have been downloaded 30,000 times since 2015, and future resources on digital piracy are under discussion.

In recent months, we have seen advertisers withdraw from platforms they don't feel adequately protect their brand, when these platforms place their adverts next to harmful content. We hope that this action from advertisers will encourage platforms to embed safety considerations into every level of their business. We will look at ways in which we can encourage platforms to provide appropriate reassurances to the businesses who advertise with them, starting with a series of senior level DCMS roundtables with major brands to establish how best to take this work forward.

Industry has developed a cross-industry self-regulatory initiative, the **Digital Trading Standards Group** (DTSG) that is governed by the Joint Industry Committee for Web Standards in the UK and Ireland (JICWEBS). The DTSG has developed tools to provide transparency and enable buyers to actively manage campaigns and minimise the risk of ad misplacement, and has published good practice principles for all business models involved in buying, selling and facilitating digital display advertising. There are currently over 60 signatories, covering a significant proportion of the market. To minimise the risk of advertising funding IP-infringing content, for example, the industry has worked with the City of London Police's Intellectual Property Crime Unit (PIPCU) to develop and implement the 'Infringing Website List' (IWL), which functions as a 'blacklist' of sites that the Police have verified to be infringing copyright. This list enables the industry then to disrupt the ad revenue such sites receive. The DTSG provides a framework for the IWL to be used by the industry.

[18] The Advertising Association has published the following proposals relating to the Government's Digital Charter work: https://www.adassoc.org.uk/wp-content/uploads/2017/12/AA_Digital_Charter_2017_SinglePages_15.11.17.pdf

Law Commission review

In February 2018, the Prime Minister confirmed the launch of a Law Commission review of online abusive communications. As social media platforms did not exist when many of the relevant laws were enacted, it is important to review the current law to ensure that the criminal law remains fit-for-purpose in dealing with offences.

The review will take place in two parts and each will last for six months. The first part commenced in April 2018 and will require the Law Commission to analyse the framework of offensive communications legislation as it applies to online communication. Its report will set out the impact of any deficiencies identified in the current legal framework. This includes assessing whether the current law is effective in ensuring that what is illegal offline is also illegal online. The review will take into consideration the full range of work taking place across Government in relation to this topic - in particular, it will build on Home Office's initiatives relating to online hate crime and the Government Equalities Office (GEO) work on online misogyny.

In August 2017, the **Crown Prosecution Service** (CPS) published revised public statements on each strand of hate crime, following a full 13-week public consultation, alongside revised hate crime legal guidance. The CPS commits to treat online offending as seriously as offline offending. It has also published guidelines on prosecuting cases involving communications sent via social media, and these were revised in October 2016 following public consultation.

The CPS is currently revising its legal guidance and public statement on Crimes Against Older People and is working with the Home Office on this.

CSPL report on intimidation in public life

In December, the Committee for Standards in Public Life (CSPL) published their report on intimidation in public life.[19] The report highlighted the abuse which parliamentary candidates can receive online and the detrimental effect that this can have on our liberal democracy.

The Prime Minister welcomed the Committee's recommendations and the Government has set out how it will act on these.

DCMS and other Government departments are taking forward work relating to internet safety and the actions for social media companies including:

- Thinking carefully about what level of legal liability social media companies should have for content on their sites;
- Introducing a social media code of practice and transparency reporting;

[19] https://www.gov.uk/government/publications/intimidation-in-public-life-a-review-by-the-committee-on-standards-in-public-life

- Ensuring social media companies put in place specific support during election campaigns to ensure abusive content can be dealt with quickly, and ensuring they provide advice and guidance to Parliamentary candidates on how to remain safe and secure online.

We are holding regular discussions with technology companies about taking these initiatives forward, and are grateful to Facebook, Google and Twitter for their engagement to date. We are clear that social media platforms must take action against content or behaviours which involve the abuse of parliamentary candidates and/ or breach election law. During election periods, it is particularly important that reported abuse is reviewed quickly. Further information relating to the support which will be available to parliamentary candidates ahead of future elections will be detailed in our White Paper.

The Government's response to the CSPL report also highlighted a number of other actions in relation to intimidation in public life. These include:

- Consulting on the introduction of a new offence in electoral law of intimidating Parliamentary candidates and party campaigners. The Government will launch a consultation exercise in the summer.
- Removing the requirement for candidates standing as local councillors to have their home addresses published on the ballot paper. The Government will look to bring forward secondary legislation at a suitable opportunity.
- International engagement - Government is continuing to work with international partners to tackle online hate crime.
- The College of Policing deliver training entitled Researching Identifying Tracing Electronic Suspects, which equips officers to safely and lawfully gather information and intelligence on the Internet, and to trace and identify suspects online. The National Police Chiefs Council will continue to work with the College of Policing to ensure that the course context is current, in keeping with technological advances.
- The College of Policing has committed to revising Authorised Professional Practice on elections, through its electoral malpractice group, to ensure it is up to date and sets a clear standard for police officers which reflects the modern context, including offences relating to intimidation and those committed through social media.
- Police leaders are working to ensure that clear advice is available to Parliamentary candidates. The National Police Chiefs Council have put in place a lead for Elections who ensures all advice is shared among MPs and Parliamentary candidates and engages with Party Headquarters.

Data Protection Bill

The Data Protection Bill was introduced to Parliament in September 2017.[20] It will:

- Make our data protection laws fit for the digital age in which an ever increasing amount of data is being processed;
- Empower people to take control of their data;
- Support UK businesses and organisations through the change; and

[20] https://services.parliament.uk/bills/2017-19/dataprotection.html

- Ensure that the UK is prepared for the future after we have left the EU.

On Royal Assent, the Bill will replace the Data Protection Act 1998 with a new law that provides a comprehensive and modern framework for data protection in the UK, with stronger sanctions for malpractice. It will set new standards for protecting general data, in accordance with the General Data Protection Regulation (GDPR), giving people more control over the use of their data, and providing them with new rights to move or delete personal data. In addition, it will preserve existing tailored exemptions that have worked well in the 1998 Act, carrying them over to the new law to ensure that UK businesses and organisations can continue to support world leading research, financial services, journalism and legal services. It will also provide a bespoke framework tailored to the needs of our criminal justice agencies and the intelligence services, to protect the rights of victims, witnesses and suspects while ensuring we can tackle the changing nature of the global threats the UK faces.

The Bill sets the age from which parental consent is not needed to process data online at 13, which reflects the Government's view that online platforms present significant opportunities and benefits for children. However, the Bill also recognises that children require additional protections in relation to their online data and that is why we have also introduced a new requirement on the Information Commissioner to produce a statutory age appropriate design code for online services that are likely to be accessed by children. This code will help make sure that children in the UK are able to access online services in a way that meets their age and development needs. It will ensure that websites and applications are designed in a way that makes clear what data is being collected on children, how this data is being used, and how both children and parents can stay in control of this data. The code will also include requirements for websites and app makers on privacy for children.

In developing the code, the Information Commissioner will consult with a wide range of stakeholders including children, parents, child advocates, child development experts as well as trade associations. The Commissioner must also take into account the UK's obligations under the United Nations Conventions on the Rights of the Child and must pay close attention to the fact that children have different needs at different ages. We are in close consultation with the Commissioner, as well as Baroness Kidron who has been instrumental in the code's development, to ensure that this code is robust, practical and meets the needs of children in relation to the gathering, sharing, storing and commoditising of their data. The Commissioner will be required to finalise the code within 18 months of the Bill coming into force.

We recognise the importance of children's rights and wellbeing as they explore online and their particular needs. **5Rights** recently published a report **'Digital childhood: addressing childhood development milestones in the digital environment'** which

considers how growing up in the digital environment directly impacts on a child's development trajectory.[21]

Online video games

The Internet Safety Strategy Green Paper set out the statutory regulation for video games supplied in physical formats – the classification (Pan-European Games Information (PEGI) age ratings), labelling and sales restrictions that apply under the Video Recordings Act 1984. It also highlighted the self-regulatory approach taken by the industry for online games, in relation to providing parental controls on devices, offering advice on safe gaming to consumers, particularly those caring for children, and rolling out the International Age Rating Coalition (IARC) initiative which ensures that apps and games available from many online and mobile storefronts carry PEGI age ratings.

UK Interactive Entertainment (Ukie), the trade body for the UK's games and interactive entertainment industry, responded to our consultation setting out the actions which the industry is already taking to improve safety. We are working with the video games industry as they strive to make continuous improvements to their safety offer including:

- A relaunch and refresh of the AskAboutGames resource, the partnership between the Video Standards Council (VSC) and Ukie.[22] In the first three months of 2018, the re-launched website had 43,000 visits.

- An industry commitment to: increase awareness of the VSC Rating Board and their role as the designated body for classifying video games in the UK under the PEGI system; create more age rating-related content, promotion and web traffic; increase engagement with schools and partner organisations; host dedicated online safety information areas at national games shows; establish more AskAboutGames in-store pop ups, social campaigns and promoted content.

- A revamp of the VSC Rating Board website, including improved information about games and their PEGI ratings, with aims to link this to the websites of major retailers of games and the development of an app for consumers.

- Continued development of Nintendo, Microsoft and Sony by the parental controls on their games consoles, for example more recent features include giving parents the ability to schedule and limit playtime and to obtain weekly summaries of activity.

- Ongoing industry-led discussions on emerging evidence, issues and best practice in identifying and dealing with concerning behaviour in online games. Discussions have

[21] https://d1qmdf3vop2l07.cloudfront.net/eggplant-cherry.cloudvent.net/compressed/01972a9579924cbba7943c849bf159b3.pdf
[22] http://www.askaboutgames.com/

also included considering the industry response to the World Health Organisation's decision to potentially list "gaming disorder" as a health condition.

- Promoting player safety in games design and business development, to those working with video games start-ups and new games development talent. For example, DCMS is working with the UK Games Fund to include relevant knowledge-sharing in the support they give to their community of early-stage game businesses and graduates.[23]

- Looking at how interactive content can be used to make a positive impact on social problems such as loneliness and can support confidence and digital literacy. For example, initiatives like the Digital School House.[24]

In the coming months, we will work with Ukie and draw on the expertise of other UKCCIS members to:

- Tackle ongoing issues such as sexism, and build our understanding in relation to how this can be most effectively tackled;
- Examine emerging issues relating to augmented reality and other new types of gaming;
- Consider the evidence relating to how interactive content can support wellbeing and resilience.

Runescape case study

"*Jagex is a leader across the sector in online safety initiatives. Their commitment to the safety of their gaming community is clear. They implement such a vast portfolio of safety features we have asked Jagex to talk to others within the IWF membership to share their knowledge in this area*" - IWF

Cambridge-based games company Jagex is recognised by the IWF for the safety features of its popular Massively Multiplayer Online Role Playing Game, Runescape. Runescape has 250 million player accounts worldwide and over 2 million monthly users. Around a third of these are in the UK. To protect Runescape players, Jagex has developed an approach that includes a minimum age requirement, 24-hour live customer support in-game monitoring, robust procedures for identifying, reporting and escalating certain behaviours and a range of sanctions. Organisations they work with include the IWF, CEOP and local police forces.

Players must be at least 13 years old. With a gateway date of birth question and further barriers are created by the need to register with a credit card to fully access the game's features. Jagex monitors in-game chat to identify players who may be too young to be playing. Over the course of year this amounts to some 4.8 billion lines of chat. Additionally,

[23] https://ukgamesfund.com/
[24] http://www.digitalschoolhouse.org.uk/

proprietary software checks for unusual behaviour, inappropriate or worrying words or phrases. A customer service team operates 24 hours a day, 365 days a year and a volunteer group of mature Runescape players with a track record of accurate and responsible reporting act as additional live game moderators. The types of behaviour escalated through moderation and dealt with include: hate language, bullying or harassment, scamming, inappropriate websites, discussion of sexual deviancy, language intended to shock or trolling, discussion of recreational drugs and potential extremist terrorist activity.

IWF keywords and Jagex's historical knowledge are also used to scan reports for content that raises concerns about risk to life – for example where these relate to suicide, self-harm, real life threat or depression. Such reports are dealt with quickly and escalated to law enforcement or others where necessary. All chat is reviewed to identify high risk behaviour relating to possible child abuse and Jagex will escalate any issue where they feel there is a risk in relation to, for example, sexual conversations about minors, grooming behaviour or discussion about child abuse media or its distribution.

As well as reporting to law enforcement in serious cases, sanctions against players who behave inappropriately in Runescape include suspending their chat function, locking their accounts, blocking their IP for current or future access, or a complete ban.

After 17 years of operating in the online gaming market, Jagex is aware of the negative side of internet behaviour and believes it has a responsibility to its players to identify and address any toxic behaviour from a small minority.

Online gambling

Responses to our consultation raised a number of concerns relating to gambling and associated issues, including free-to-play gambling-style games, games or apps that may promote gambling-style behaviours, 'skins' gambling[25] and social media advertising.

The Government recently published the review of gaming machines and social responsibility measures across the gambling industry.[26] This included measures aimed at strengthening player protections related to online gambling products and advertising.

There are already strong protections in place to prevent underage gambling and to protect vulnerable people from gambling-related harm. All online gambling companies with UK customers, no matter where they are based, are required to obtain a licence from the

[25] Online gambling with virtual items deriving from video games.
[26] https://www.gov.uk/government/consultations/consultation-on-proposals-for-changes-to-gaming-machines-and-social-responsibility-measures

Gambling Commission and must comply with the licence conditions and codes of practice set by the Commission.

In March 2018, the Gambling Commission announced new proposals to make online gambling safer.[27] The proposals include improving the speed and effectiveness of age verification processes - so that age verification must be completed before a customer is able to deposit funds and gamble (rather than within a 72-hour window) - and strengthening requirements to interact with consumers who may be experiencing, or are at risk of gambling related harm.

The **Gambling Commission's annual Young People and Gambling Report**,[28] published in December 2017, found that children's participation in traditional forms of gambling continues to decline, with 12% of 11-16 year olds having gambled in the past week, down from 16% in 2016. The most common activities were gambling on fruit machines (4% having spent money on this in the past week), private bets with friends (3%) and National Lottery scratchcards (3%).

Children's participation in online gambling remained largely static compared to the year before. 1% of 11-16 year olds had spent their own money on online gambling over the past week, while 3% of 11-16 year olds had spent their own money on online gambling at least once or twice a year (compared to 3% in the previous year). A larger proportion (7%) had gambled online using their parents' accounts (either with or without permission) - the most common form being National Lottery games (5%).

The advertising codes of practice apply across all advertising platforms, including social media and online, and they aim to ensure gambling advertising is not targeted at children or young people and does not exploit vulnerable people.[29] Gambling advertising was considered as part of the Gambling Review, and a package of measures was put forward designed to strengthen protections around advertising, including online and on social media.

As part of this, the Gambling Commission consulted[30] on proposals to enhance requirements for the marketing and advertising of gambling products and services, including tougher sanctions for breaching the UK Code of Non-broadcast Advertising and Direct & Promotional Marketing (CAP code) and the UK Code of Broadcast Advertising (BCAP code), and the requirement that operators do not contact consumers with direct e-marketing without their consent.

---

[27] http://www.gamblingcommission.gov.uk/news-action-and-statistics/news/2018/Gambling-Commission-makes-online-gambling-safer.aspx
[28] http://www.gamblingcommission.gov.uk/PDF/survey-data/Young-People-and-Gambling-2017-Report.pdf
[29] The advertising codes covering non-broadcast gambling advertising can be found at https://www.asa.org.uk/type/non_broadcast/code_section/16.html
[30] http://www.gamblingcommission.gov.uk/news-action-and-statistics/Consultations/Closed-consultations-awaiting-response/Proposed-changes-to-LCCP-fair-and-open.aspx

The Commission will continue its work to encourage social media companies to develop user friendly guides which will explain how, using the platform tools available, consumers can limit their exposure to gambling advertising.

DCMS, as the department responsible for the digital and online agenda, recognises the important role it plays in bringing together work from across Government with industry initiatives. The Minister for Sport and Civil Society will co-chair a roundtable with the Minister for Digital and the Creative Industries, to bring together stakeholders from the gambling and technology sectors and move towards a wider roll-out of best practice. This will include helping to develop understanding of, and best practice around, online advertising and marketing.

Online gambling-style games are like real gambling games but are free to play and do not offer any prizes, which means they are not gambling products. In March 2018, the Gambling Commission announced proposals to further strengthen the protections currently in place by banning gambling operators from providing free-to-play gambling-style games until a consumer's age has been verified.

With regard to unlicensed 'skins' gambling,[31] the Gambling Commission has shown it will take action and prosecute unlicensed gambling with in-game items.[32] In addition to using its enforcement powers against these websites, the Commission is seeking to work with the video games industry to develop a joint approach to raise awareness of and explore solutions to this issue.

We note concerns that entertainment products, such as some video games, could encourage gambling-like behaviour and we will continue to look closely at any evidence around this issue. Microtransactions within apps and video games are subject to consumer protection legislation, including requirements on businesses not to subject anyone to misleading or aggressive marketing practices. This includes, for example, direct exhortation to buy products, such as in-game or in-app content.

Pictographic content descriptors supplement the PEGI age ratings on video games, and there is a descriptor for products that contain elements that may encourage gambling. Games with this type of content carry a PEGI 12, 16 or 18 age rating. The VSC Rating Board is working with PEGI to assess further steps to inform consumers about purchases in games.

In addition, the Competition and Markets Authority provides guidance[33] and advice for

---

[31] 'Skins' gambling is a term used to describe online gambling where virtual items deriving from video games are used as stakes or prizes. This type of gambling is typically offered by third-party websites in contravention of the terms and conditions of the video game platforms from which the virtual items derive.

[32] http://www.gamblingcommission.gov.uk/news-action-and-statistics/news/2017/Two-men-convicted-after-offering-illegal-gambling-parasitic-upon-popular-FIFA-computer-game.aspx

[33] https://www.gov.uk/government/publications/buying-features-in-online-games-advice-for-parents-and-carers/childrens-app-and-online-games-advice-for-parents-and-carers

parents and carers, in respect of children's use of online games. The advice includes information on checking device settings to prevent children from making in-play purchases, as well as guidance on game descriptors.

Libraries

Libraries offer a trusted source of information, both on and offline for many. The sector is inherently diverse with each library free to develop their own offer. A number of libraries and librarian organisations responded to the Internet Safety Strategy consultation. The responses highlighted a high level of activity in this area with librarians keen to upskill in a range of digital and online safety areas.

We are working with the Society of Chief Librarians (SCL) and the Association of Senior Children's and Education Librarians to explore the sharing of best practice and how online safety is integrated into:

- Educating parents/carers, adults, and children and young people;
- Training for library staff;
- Existing products and library services; and
- Bespoke new work.

In October 2017, the **Society of Chief Librarians** launched the first in a series of family learning and digital roadshows. Sessions were designed with the help of a group of digital enthusiasts from around the country who volunteered. Each event featured two Family Learning workshops (focused on a new activities pack and evaluation toolkit), plus hands-on demonstrations of the latest technology aimed at frontline staff who – with a little bit of training – could deliver digital taster events in their own areas. An evaluation following the roadshows indicated that 87% of the 200 plus delegates found the digital workshops 'very useful', with 82% saying they were going away to use the resources and what they had learned from the digital sessions within their own library services (and the remainder saying they intended to use some of this).

Loneliness Strategy

Loneliness and social isolation is endured by more than 9 million people in the UK; particularly the elderly, those with disabilities, carers and young parent. We know that online communities can provide a vital lifeline for many groups.

The Jo Cox Commission on Loneliness was a partnership of 13 charities and businesses with expertise, insight and reach into some of the communities most affected by loneliness in the UK. In December 2017 the Commission published a report of its findings and recommendations for how Government and the wider community can contribute to tackling loneliness. The Government has accepted most of the recommendations, including appointing Tracey Crouch MP as the ministerial lead for cross-government work on loneliness.

DCMS is hosting a cross-government team, which has a range of work planned, including developing a Strategy on loneliness in England, which will be published later this year. This will bring together Government, local government, public services, the voluntary and community sector and businesses to identify opportunities to tackle loneliness, and build more integrated and resilient communities. We will ensure that any links between the Internet Safety Strategy and loneliness are appropriately reinforced.

National Citizen Service

The National Citizen Service (NCS) will work with the Government to empower young people to stay safe online. The annual NCS Youth Report provides a valuable insight into teenage online usage and the issues that this presents from an educational and safety perspective. The 2017 report found 46% of LGBT teens surveyed would go to an online chat room for help with mental health, compared with 18% of non-LGBT teens. NCS will work with Governmental and civil society stakeholders to communicate these insights. NCS is exploring how its online "Opportunity Hub", open to the programme's 400,000 graduates can be used to signpost young people to support on issues, including those experienced online. NCS will consider how the challenges young people face online, as well as the benefits, can be addressed through its programmatic work.

6. Wider Government response to online harms

Government Equalities Office

The Government Equalities Office (GEO) continues to support the Revenge Porn Helpline which offers vital support to those affected by this crime. The Helpline has received over 10,000 calls since it opened in February 2015.

The GEO is also taking forward work on positive body image. These projects will build on the commitments made in the response to the recent Youth Select Committee report which highlighted that increased time spent online can lead to increased exposure to images of unattainable and unrealistic beauty.[34]

The GEO are also developing a package of work to tackle harmful gender norms which can occur both online and offline. This will include work with the advertising industry to encourage stereotype-free advertising.

Statistics from Girls' Attitudes Surveys 2016 and 2017 produced by Girlguiding:

- In the 2016 survey: 25% of girls aged 11-16 said that the fear that people will criticise their body stops them from using social media and 40% of girls aged 17-21 said that they have had an embarrassing photo of them shared without their consent online.[35]
- The 2017 survey showed that girls aged 11 to 16 relate most to YouTubers and are the most likely to see them as good role models. The oldest group (17 to 21 year olds) are more cynical and aware of YouTubers advertising brands or having a potentially negative effect on viewers.[36]

Home Office and the Ministry of Housing, Communities and Local Government

Online hate crime and hate speech

[34] http://www.byc.org.uk/wp-content/uploads/2018/03/2017-Youth-Select-Committee-Government-Response.pdf
[35] https://www.girlguiding.org.uk/globalassets/docs-and-resources/research-and-campaigns/girls-attitudes-survey-2016.pdf
[36] https://www.girlguiding.org.uk/globalassets/docs-and-resources/research-and-campaigns/girls-attitudes-survey-2017.pdf

The survey responses to the Green Paper consultation have helped us understand more about online abuse and who is targeted. The survey and written responses will be used to help inform the refresh of the Hate Crime Action Plan later in 2018.

The **All-Party Parliamentary Group Against Antisemitism** and **Antisemitism Policy Trust's** response to our consultation highlighted the work taking place internationally to combat internet hate, on which the UK has already taken a leading role. We will continue to collaborate with the Inter-Parliamentary Coalition for Combating Antisemitism and the EU Commission Initiative to remove illegal hate speech within 24 hours as we take forward our work in this area.

On 8 October 2017, the Home Secretary announced £200,000 of Home Office funding for a new national police hub to tackle the emerging threat of online hate crime. The hub, run through True Vision by Greater Manchester Police for the National Police Chiefs Council, will work to ensure that online cases are managed more effectively and efficiently. It will also help to provide better support victims and streamline the process for frontline officers. The hub became operational in January 2018.

Several of the written responses to our consultation refer to the national online hate crime hub. We are pleased that there is support for this and will ensure consultee's feedback is passed to the police online hub team.

The Ministry of Housing, Communities and Local Government (MHCLG) has provided £50,000 to Stop Hate UK in 2017-18 to support their Counter Narrative training for young people to address online hatred including a seminar to identify best practice. MHCLG has also supported the Society of Editors in delivering a guide to moderate online hate content.

Home Office

Child use of adult dating sites

The findings from the consultation highlight that industry needs to take more ownership of the activities on their platforms and do more to tackle the issue of children using adult dating sites.

There was general concern about dating sites' lack of ownership in preventing sexual exploitation of children, with only 27% (100 respondents) agreeing that dating websites were doing all that they can to prevent child abuse. Only 30% of respondents considered it to be a law enforcement responsibility to moderate children using adult dating sites**.** 68% of respondents thought that companies should better moderate and 60% of respondents thought where appropriate they should terminate children's accounts. 86% of respondents thought that parents should be responsible for ensuring that their children didn't access adult dating sites.

71% of respondents stated that adult dating site users should have a minimum age rating and 51% of respondents stated that 18 should be the minimum age. 79% of respondents considered age verification to be a useful mechanism to prevent young people from using adult dating sites. There was also general concern about the current lack of moderation by companies in relation to children using their sites. Under-age use of dating sites can lead to contact abuse therefore it's important that we take steps to address this. Overall, respondents were keen to see more investment from dating companies and greater use of new technology to protect users and verify user identity.

The Government will be engaging with adult dating sites, law enforcement agencies and other interested parties by holding roundtable discussions on the best way forward. Government will work with industry to explore voluntary options including preventive messaging on sites.

Fraud

The Joint Fraud Taskforce is still relatively young, but is making good progress. Over the next 18 months, the Joint Fraud Taskforce will develop and implement strategies that, alongside the Regulatory Technical Standards recently finalised at EU level, will bring about significant reductions in 'card not present' fraud as well as working to ensure that banks adopt the principles of the Code of Practice for victims of fraud financial abuse.

Cifas, a not-for-profit organisation working to prevent fraud in the UK, noted in their response to our consultation that 88% of identity fraud victims reported to Cifas in the first ten months of 2017 were under 65. They highlighted that young people aged under 21 are the fastest growing age group for victims of identify fraud. We will be looking at what more we can do to raise awareness of identity fraud issues amongst younger age groups.

In addition, the CPS is currently revising its legal guidance and public statement on Crimes Against Older People and continues to work with the Home Office on this.

Domestic abuse

On 8 March 2018, the Home Secretary and Justice Secretary jointly launched the public consultation on domestic abuse. The consultation seeks views on measures to be included in a future Domestic Abuse Bill, as well as non-legislative options to raise awareness, support victims and ensure perpetrators are stopped.[37] This consultation will build our understanding of online threats and the role of technology in abuse, as well as considering how we can make innovative use of technology to tackle domestic abuse and provide support to victims.

[37] https://www.gov.uk/government/consultations/domestic-abuse-bill-consultation

CHAYN is an open-source project that leverages technology to empower women against violence and oppression so they can live happier and healthier lives. Chayn started in May 2013, when Hera Hussain wanted to create a platform to inform women experiencing domestic violence in Pakistan. It continues to be run by volunteers and offers access to free materials such as "Do it yourself online safety".

The Tampon Tax Fund has provided £1.4m funding to Rape Crisis England and Wales to conduct a Digital Transformation Project across their 45 sites to enhance digital capacity in order to support survivors of sexual violence, reach marginalised women and girls, work with communities to address online sexual grooming and exploitation and prevent sexual violence.

Serious Violence Strategy

The Serious Violence Strategy, published on 9 April 2018, includes a commitment to continue to work with the police to support proactive action to address and take action against illegal material hosted and offences perpetrated online.[38] For example, the Metropolitan Police has been leading action through Operation Domain which started in September 2015 to take action against gang related videos encouraging violence.

Commission for Countering Extremism

In October 2015, we published the first ever Counter-Extremism Strategy to protect communities from the social harms caused by extremism. The Government is taking a comprehensive approach to tackling the evil ideology of extremism – whether violent or non-violent, Islamist or far and extreme right wing. The Counter-Extremism Strategy has four pillars: vigorously countering extremist ideology – making sure every part of Government is taking action; actively supporting mainstream voices - especially in our faith communities and civil society; disrupting the most harmful extremists - using all of the tools available; and building more cohesive communities - by tackling segregation and feelings of alienation which can provide fertile ground for extremists' messages.

In March 2018, to step up the fight against extremists, the Government formally launched the independent Commission for Countering Extremism and confirmed Ms Sara Khan as the Lead Commissioner. The Commission has a clear remit to identify and confront extremist ideology in all its forms. It will do this both across society and online, bringing new drive and innovative thinking to all our efforts to tackle extremism.

Attorney General's Office

[38] https://www.gov.uk/government/publications/serious-violence-strategy

Towards the end of last year, the Attorney General launched a Call for Evidence on the impact of social media on the administration of justice in criminal trials. The issues raised in the evidence received are currently being considered and a response will be published later this year.

Earlier this year, **Doteveryone** published their **'People, power and technology: the 2018 digital attitudes report'.**[39] The report highlights concerns that the Internet hasn't been beneficial for society as a whole; an understanding gap around technologies, how data is used and how companies make money; and the public demand for greater accountability from technology companies.

Further research

We have commissioned a rapid evidence assessment which considers the prevalence and impact of online trolling. The report will be published in due course, but the initial findings highlight that more research is needed to gain a clearer understanding of what trolling is, how it is affecting UK society and what needs to be done to effectively counter its negative impacts.

Therefore, in this coming year, we will be prioritising the funding of new research into adult harms and drawing on available knowledge about effective strategies for tackling this from across both Home Office's work on illegal harms and our wider work on the Digital Charter. We will be working with partners such as the Behavioural Insights Team to explore ways in which Government, companies and charities can encourage users to improve their online behaviour. In addition, we will focus on new research to tackle the current evidence gaps highlighted by the UKCCIS Evidence Group's literature review in relation to children's online activities, risk and safety.[40]

Research by the **Children's Commissioner** into the impact of social media on the lives on children aged 8 – 12 found children insufficiently prepared for life online, particularly at the critical point of transition to secondary school. In January 2018, she published **'Life in "likes"**, which included analysis from a series of focus groups with children. It explored how they use social media, how it influences their friendships and family relationships, and whether and how it has an effect on their general well-being.

The report found children experimenting with a variety of social media platforms, including many they were formally 'too young' to use. Children said that they were confused by how old you needed to be to use social media.

---

[39] http://attitudes.doteveryone.org.uk/

[40] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650933/Literature_Review_Final_October_2017.pdf

The report identified the benefits of social media, as younger children in particular said it made them happy and relaxed. However, it also found children ill-prepared for the emotional and social effects of social media use and warned of a ‘cliff edge’ as children transition to secondary school and their social circles, offline and online, rapidly expand.

Annex A – Consultation Activities

We would like to thank the following schools for participating in our focus group and roundtable discussions:
Oasis Academy Lister Park
Cheam Common Junior Academy
Parklands Infants School
Coppice Primary School
Marlborough Primary School
Earls Court Free School Primary
The Cedars Primary School
Chadwell Primary School
Gilmour Juniors
LIPA Primary
Fazakerley Primary
Our Lady Immaculate Primary
St Patrick's Primary
Whitefield Primary
Knotty Ash Primary
St Francis de Sales Catholic Juniors
St Sebastian's and St Cuthbert's Federation
Barlows Primary
The Innovation Centre, Bradford
Southfield School (SEND), Bradford
Bingley Grammar School

Consultation survey responses

We produced two versions of our online consultation survey - one for individuals and one for organisations. The survey for individuals included questions on both personal online experiences and our policy proposals, whereas the survey for organisations only included questions on our policy proposals. 528 individuals and 62 organisations responded to our survey. Where we have provided consultation result figures in this document, we have highlighted whether the results relate to responses from individuals or organisations.

As individuals and organisations completed our survey, they could choose to submit their responses without answering all of the questions. Therefore the number of respondents varies for each question. The result percentages provided through this document are calculated based on the number of respondents who answered that particular question.

For example:
In total, 528 individuals responded to the survey.
Question X - 360 individuals responded. 240 individuals selected 'yes' and 120 individuals selected 'no'. The percentage of individuals who responded 'yes' is calculated as follows:
(240/360) x 100 = 67%

Annex B – Draft code of practice for providers of online social media platforms

This code provides guidance as required by the Digital Economy Act 2017 section 103. It also provides additional guidance, not required by the Act.

[Code of Practice under section 103]
This code of practice applies to conduct which -
a. Is engaged in by a person online;
b. Is directed at an individual; and
c. Involves bullying or insulting, or other behaviour likely to intimidate, humiliate the individual (referred to as 'abuse' for the remainder of this document).

This code does not affect how unlawful conduct is dealt with.

The code of practice may be revised from time to time.

1. "Social Media Providers" should maintain a **clear and transparent reporting process** to enable individuals to notify providers of the use of their platforms for the conduct set out above. This should include:
   - Capacity for users to report content or conduct which breaches the service's terms and conditions;
   - Capacity for users to report abuse targeting gender, transgender identity, disability, race, sexual orientation, religion and political views;
   - Guidance for users to report content or conduct which may potentially breach UK law to the relevant authorities;
   - Capacity for reports by users who self-identify as under 18 to be handled appropriately;
   - Implement processes for reviewing user reports about images, videos, text and other content or conduct;
   - Making available, and visible to users, information on report and review procedures;
   - Tools to block or mute the user who has uploaded abusive content, so that they can no longer see posts or have a conversation with the victim;
   - Moderating processes which are resourced to match the platform's user base;
   - Links to reporting options in appropriate places on the platform so they are regularly seen by the user;
   - Clear age guidelines, including as standard, a mechanism for users to report underage use where they suspect it is taking place;
   - Scope for the testing and improving of reporting mechanisms based on user feedback and as new products/ features are developed;
   - Links for users to access appropriate off-platform support for a range of issues: crime, bullying, mental and physical health and wellbeing, suicide and self-harm;
   - Appropriate mental health and wellbeing training and support in place for all moderators.

   Best practice examples of the principle:

- A triage system to deal with content reports;
- Capacity to report multiple incidence of abuse;
- Capacity for non-users to report abusive content/conduct and potentially harmful content, for example parents and teachers to report on behalf of young people;
- The option of in-line reporting: reporting buttons on the actual content/ conduct that the user might want to report;
- Reporting streams for complaints where abuse targets one or more of the protected characteristics set out in the Equality Act 2010;
- Prioritisation of reports concerning: suicide or self-harm content or behaviour, credible threats and child safety (under 18 users);
- Flagging users to websites and public referral tools to report content or conduct which may potentially breach UK law so law enforcement and industry can take appropriate action. These include the Counter Terrorism Internet Referral Unit, the True Vision hate crime reporting website and the Internet Watch Foundation (IWF);
- Using a mix of human and machine moderation with minimum training standards and guidance for moderators of online content;
- Establishment of effective single points of contact within the company for law enforcement agencies;
- Tools to unsubscribe or "un-follow" accounts that produce or share offensive material;
- Inclusion of relevant professionals and users when designing new safety policies;
- Use of technological tools which prevent users who have been blocked from the platform from attempting to return.

2. “Social Media Providers” should **maintain processes for dealing with notifications** from users. This should include:
   - Providing information about how reports are dealt with and how the outcome will be communicated, including expected timeline;
   - The removal of content reported on a ‘comply or explain’ basis - processes should notify users about the outcome of a report, when action has been taken, if further information is needed and when no further communication will be provided;
   - Sending users an acknowledgement that their report has been successfully received within 24 hours. The acknowledgement should further information on the reporting process including: a commitment to act on reports relating to abuse within a certain number of hours and the expected resolution timescales;
   - Support information which is accessible and in one place for users, e.g in a ‘safety centre’ (or equivalent).

   Best practice examples of the principle:
   - Providers consider the most effective way of communicating with users about their reports - this may include using different communication channels or adapting the language used for younger users;
   - Providers work effectively with trusted flaggers including charities and other user support organisations such as the Revenge Porn helpline;

- Additional support including signposting to other sources of guidance is used to help users deal with complex issues, including mental health concerns;
- Flagging privacy options to users as part of the reporting process;
- Offering an appeals process to users who disagree with the platforms' decisions on content removal;
- Ability for non-users to report abusive content/conduct, for example parents and teachers to report on behalf of young people;
- Providers anticipate when increased reporting may occur, such as during election periods, and ensure that appropriate resources are available to deal with reports in a timely manner.

3. "Social Media Providers" should include **provisions about the above matters in their terms and conditions.**[41] Terms and conditions should:

- Be underpinned by the principle that what is unacceptable offline is also unacceptable online, with recourse to UK law;
- Be clearly written and easy to understand;
- Include consequences for users in relation to the violation of terms and conditions;
- Include or link to information on:
  - Acceptable user content and conduct examples;
  - Provision to tackle abusive behaviour;
  - Respecting the rights of others;
  - Actions taken to tackle anonymous abuse;
  - Action against content that is been removed and reuploaded;
  - Provision to terminate accounts which are used to abuse others;
  - Where behaviour may amount to a criminal offence;
  - Make reference/ link to an explanation of how community guidelines are developed, enforced and reviewed including information on performance metrics on take-down;
  - Provision for user privacy settings including the ability to make a profile not visible to the public.

Best practice examples of the principle:

- Policies, including the terms and conditions, are expressed in plain English and can be understood by users of all ages;
- Policies about acceptable user conduct and content are accessible and may be reproduced separately from the main terms and conditions of a platform, for example as part of community standards;
- Regular reminders of the policies should be presented in engaging formats across different typical user journeys.

4. "Social Media Providers" should give **clear explanations to the public about the action taken against the above specified conduct:**

- Users should be made aware of the prevention, identification and consequences of behaviour which is contrary to the policies of the platform. This should include strategies for users who persistently engage in abusive behaviour or behaviour which

[41] Also referred to as 'Terms of Use' by some providers.

may promote risky and dangerous behaviour, intentional self-harm or damage other users' mental health and wellbeing;
- Platforms should give users explanations on a 'comply or explain' basis if content remains after they have reported it;
- Platforms should consistently enforce the consequences of misconduct as detailed in their policies.

Best practice examples of the principle:
  - Platforms provide education on appropriate online conduct to all users, especially those who breach the platform policies;
  - Information about the consequences of misuse is incorporated in the regular reminders of the platform's policies.

[Additional Guidance not required under section 103]
The above code of practice also applies to conduct which is directed at groups and businesses. Examples of 'groups' include supporters of a football team, pupils of a school, people from a particular town, supporters of a particular political party.

In addition to the types of abuse detailed above, the code also applies to conduct which negatively impacts mental health and wellbeing. The code of practice will encourage the use of technology to identify potentially harmful online content and behaviours.

In addition to this code, other guidance relevant to "social media providers" includes:
- the Information Commissioner's existing and future guidance including the upcoming Age Appropriate Design Code;
- the UK Council for Child Internet's Safety *Child Safety Online - A practical guide for providers of social media and interactive services.*

Annex C – Draft transparency reporting template

TRANSPARENCY REPORT TEMPLATE	
Data relating to July - September 2018	
Company information	
Name of company	
Company headquarters address	
UK head office address (if applicable)	
Total number of UK users	
Total number of UK posts/ pieces of content published	
Process information	
Information in the UK terms and conditions and community guidelines regarding what content and behaviours are acceptable/ unacceptable on the platform	Terms and conditions state: Community guidelines state:
Information in the UK terms and conditions and community guidelines regarding the reporting process	Terms and conditions state: Community guidelines state:
Number of employees reviewing all types of UK reports	
Number of employees specifically reviewing UK reports of abuse	
Number of those employees with mental health training (either professional or awareness focused training)	
Details of support which users may be signposted to having made a report, for example a suicide-prevention helpline	

Number of users that are signposted to support	
Threshold for permanently terminating a user's account	
Reporting information	
Headline figures	
Total number of content items reported by UK users	
Number of UK users who made any type of report	
Total number of all reports made by UK users	
Percentage of reports made by UK users which led to action being taken eg content was removed, user was blocked, etc	
Average review time for all types of reports (ie time from the user making the report to the report being closed)	
Average time from content creation to take down	
Details of trusted flaggers contributing to the reporting process, if appropriate	
Number of pieces of content flagged by trusted flaggers and the percentage of content which is then removed	
Percentage of users who report content and receive feedback	
Percentage of trusted flaggers who report content and receive feedback	
Average time taken to send users a decision about a report	
Detailed figures	
Number of users who report content and are then signposted to mental health support	
Number of users who report content and are then signposted to other types of support	
Number of reports relating to content that has been removed and then re-uploaded	

Number of accounts of underage users that have been deleted	

Categories of complaints	**Number of content items proactively removed (ie not based on user reports)**	**Number of content items reported by UK users**	**Number of UK users who made a report**	**Number of reports made by UK users**	**Percentage of reports made by UK users which led to action being taken**	**Number of user accounts blocked due to reports**	**Average review time for reports**
Abuse							
Violent or graphic content							
Harmful or dangerous content - content which might lead to users harming themselves or others							
Nudity or sexual content							
Spam, misleading data, scams, fake news							
Copyright							
Impersonation							
Other							

<u>Reports relating to abuse</u>	
Percentage of reports made on behalf of somebody else	
Percentage of reports relating to anonymous accounts	
Percentage of reports made where the reporter claims they know the person they are reporting	

	Number of users	Total number of abuse reports made	Percentage of abuse reports leading to take down
UK users aged under 13			
UK users aged 13 - 15			
UK users aged 16 - 18			
UK users aged 19 - 25			
UK users aged 26 - 35			
UK users aged 36 - 45			
UK users aged 46 - 55			
UK users aged 56 - 65			
UK users aged over 65			
UK users - no age recorded			

Categories of abuse complaints[42]	Number of abuse reports made
Related to gender	
Related to transgender identity	
Related to disability	
Related to race	
Related to sexual orientation	

[42] Reports may be related to several categories of abuse so can be recorded under multiple categories.

Related to religion or belief	
Related to political views	

An opportunity to: • **highlight any trends or significant information relating to any of the above data;** • **provide further information on the companies' approach to reporting and any plans to make improvements to reporting processes**

HM Government