HM Government

Internet Safety Strategy – Green paper

October 2017

Contents

Table of Contents

1. Foreword

As the Secretary of State responsible for digital, I have the privilege of working with a sector which is constantly evolving and playing an ever increasing role in all of our lives.

Since its inception, the Internet has been an amazing force for good. It has had an extraordinary impact on people around the globe. It has created lines of communication; driven innovation, growth and new business models; and, it has connected and given a voice to the previously disenfranchised. For the first time ever, anyone, anywhere, with a smartphone and an internet connection can grow their own business and connect with people from around the world.

The Internet has evolved in this way because it is open and free. It is right that the technology that underpins the Internet is developed by the brightest technicians and engineers, not governments. But as the Internet has developed, risks have emerged online and behaviours that would not be tolerated in the real world are increasingly condoned online. As our manifesto sets out, we will act to ensure people are protected online – working with the sector to develop solutions wherever possible, while not ruling out legislation where it is needed.

We recognise that the Internet is challenging our society and that government needs to react to new social norms. This green paper will promote debate on what we think acceptable behaviours are online, and consider how the government can create strong frameworks that get to the heart of the problems we face. This Government believes that citizens' rights and wellbeing need to be protected online, just as they are in the offline world. We are committed to tackling online harms, by not only working with technology companies, but also focussing on how we can best support users.

As set out in our manifesto, this Government is committed to ensuring that Britain is the safest place in the world to be online. This is important as we want everyone to benefit from the opportunities presented by the digital age. This green paper takes forward a range of manifesto commitments including our promise to educate today's young people in the harms of the Internet and how best to combat them; introduce an industry-wide levy which could in the future be underpinned with legislation; and protect the vulnerable and give people confidence to use the Internet without fear through initiatives like a code of practice for social media companies.

The question and challenge of our age is how to reduce the risks posed by the Internet, while embracing its opportunities. This green paper sets out our objectives on online safety and we will work together with a wide range of interested parties to achieve these. In developing this work we will work closely with government departments, charities, academics and the tech community to take the action needed to make online communities safer and empower users to manage risks and stay safe online.

This Internet Safety Strategy is just the first part of our work on the Digital Charter. The Charter will ensure that every individual and every business can seize the opportunities of digital technology.

The Rt Hon Karen Bradley MP
Secretary of State for Digital, Culture, Media and Sport

2. Executive summary

This Government aims to establish Britain as the world's most dynamic digital economy. We want to make Britain the best place in the world to setup and run a digital business, while simultaneously ensuring that Britain is the safest place in the world to be online. This means developing an approach to the Internet that benefits everyone. It means embracing and maximising the opportunities that the Internet provides, while at the same time tackling the risks that it poses for its users. It means working together with a wide range of stakeholders to develop safer online communities and empowering citizens to manage risks and stay safe online.

Our Internet Safety Strategy green paper marks another step towards developing a coordinated, strategic approach to online safety. We recognise the enormous and unparalleled opportunity that the Internet has presented; it has provided us with new and faster ways to communicate, learn, travel, have fun and do business. At the same time, the power of the Internet poses risks that we all have a responsibility to address.

Through this green paper we will set out a high level of ambition on how we must all play our role in tackling issues of online harms. The government will address online safety by bringing groups across society together – including the voluntary sector, technology firms, schools, and the people of Britain – to establish a coordinated approach.

We recognise that no technology can be inherently good or bad and we acknowledge the value of a free and open internet that protects freedom of expression and the platforms that promote it. We believe that in order to improve online safety, government will need to harness the technical understanding and expertise of industry partners if we are to deliver thriving, safe and innovative online platforms.

In delivering these objectives, our work will be underpinned by three key principles:

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

We have consulted a wide range of stakeholders including charities, internet safety organisations, academic researchers and technology companies while developing the objectives and initiatives in this green paper.

This is an important step towards developing a safer online environment and we will need to carefully consider all our policy options before we bring them forward. This is why we are consulting on various aspects of online safety as part of the green paper.

Over the next eight weeks we hope to have a public conversation about the options included in our Strategy. Some of our ideas are ambitious - and rightly so. Problems created by new technologies need a new, innovative policy response if we are to correct online harms without hampering or restricting growth and innovation in the digital economy.

The Internet Safety Strategy green paper will form part of the government's Digital Charter. The Charter will deliver our manifesto commitment to establish a new framework that balances freedom with protection for users. Through the Charter, we will work with businesses, academics, charities and the wider public to build consensus on how technology should be used and how we act online.

The Internet Safety Strategy green paper

Our Internet Safety Strategy green paper is formed of five strands, summarised here and developed in more detail throughout the document.

Our strategic response

Government needs to create the conditions and set the framework for a collaborative, strategic approach to safety. This chapter will set out how government action will support the delivery of the Strategy and its ambitions. While the Department for Digital, Culture, Media and Sport (DCMS) will take a leading role in this delivery, we will work with a wide range of partners across government, including the Home Office, the Department for Education, the Department for Health and the Ministry of Justice.

The Strategy acknowledges the pioneering role that the UK Child Council for Internet Safety (UKCCIS) has played in promoting and championing improvements to child online safety in the UK. We plan to build on and augment the work of the Council and widen its scope to all internet users. We propose a number of governance changes to improve its accountability, strategic direction and responsiveness to the rapidly changing online landscape. These will be discussed with the online safety community as part of the delivery of the Strategy.

Our work on online safety will complement relevant upcoming areas of work across government, including the Department of Health's and Department for Education's Children and Young People's Mental Health green paper. The government's approach to the most serious online crimes relating to extremism, terrorist use of the Internet and child sexual exploitation will continue to be led by the Home Office. While these issues fall outside the scope of this Strategy, appropriate links will be made where the Strategy offers additional solutions to these problems, for example through online safety education.

Finally, we recognise that while the Strategy focuses on online safety in Britain, the Internet is a global technology and we will need to work with other partners and international institutions to support and deliver our objectives.

Working with industry to make online environments safer for all users

We recognise the government alone cannot keep citizens safe from online harms. The initiatives in this Strategy will be delivered in close partnership with industry, drawing on their technology and engineering expertise, to put in place specific technical solutions to make their platforms safer.

Alongside setting stretching objectives for industry on tackling online harms, this Strategy consults on a variety of initiatives aimed at improving industry's offer on safety, including manifesto commitments.

We are consulting on the social media code of practice provided for by the Digital Economy Act. The Act requires the code to address conduct that is bullying or insulting to users, or other behaviour that is likely to intimidate or humiliate. Through this code we hope to tackle some of the most pernicious, but legal, online behaviours, including trolling and abuse, that is often disproportionately targeted towards women.

We will also consider how the code can deliver the manifesto commitment for a reporting mechanism with a 'comply or explain' response.

To give effect to the manifesto's commitment to introduce a 'social media levy', the consultation will ask a number of initial questions about implementation, to guide early policy development.

We will also ask questions about how government can work closely with industry to produce an annual internet safety transparency report. This could include common metrics which would enable benchmarking of reporting mechanisms.

Finally, the green paper considers options for working with the online gaming industry to improve gaming safety.

How can technology improve online safety for all users

We know that technical solutions, developed by industry, can help keep users safe online. We recognise the benefit of current parental control filters. Technologies, including linguistics filters and artificial intelligence, have the potential to make a considerable difference to the safety of online communities. Government will consider what we can do to support and develop a world-class online safety industry in Britain, in line with our manifesto ambition to make Britain the best place in the world to start and run a digital business.

We will provide better information about how startups can deliver safety by design to raise their level of safety from the start, and will consider the role that individual technologies, including application (app) stores and operating systems can play in delivering safer services.

We will encourage app developers to 'think safety first', by working with established companies to share best practice and promote new and existing guidance on online safety to ensure that necessary safety features are built into apps and products from the very start. We will work with existing industry bodies and communities, for example Tech City UK, to improve our outreach to startup communities in order to disseminate and promote messages on online safety to developers.

Government also recognises the value of providing consistent messaging on online safety across platforms and operating systems. Building on the good work that Google and Apple have already done on their family classifications for apps, we will seek to work with them to improve this offer on safety, particularly in relation to children's services and apps.

Supporting children, parents and carers

The Strategy outlines the crucial role that education will play in raising the level of users' safety online, with a particular focus on children and parents. For children, we will consult on the role that online safety education will play in the new, compulsory subjects required by the Children and Social Work Act. Additionally, we will consider the role that peer to peer learning can play in delivering innovative education programmes to users.

Schools also play an important role in supporting children when they have suffered the impacts of online harms from cyberbullying and online abuse to sexting. Schools are increasingly expected to handle online issues that have taken place outside of schools hours. The Department for Digital, Culture, Media and Sport (DCMS), working closely with the Department for Education (DfE), will ensure support is in place for schools to handle these concerns, including signposting the range of materials that are available.

We will seek to support parents to address issues of online safety in the same way that they tackle other risks, like road safety, starting from birth. We know that there's already a lot of advice available for parents and carers on online safety but it can be confusing or overwhelming. We will ask the new UK Council for Internet Safety (UKCIS) to streamline and target education and advice on online safety for parents.

Responding to online harms

While the primary aim of this Strategy is to build safer online environments and reduce the harm experienced online, we cannot expect that things will not sometimes still go wrong for some internet users. This green paper explains the support that is in place for users when something does go wrong online and details existing work across government which seeks to support users.

The Home Secretary recently announced that an Online Hate Crime Hub would be established that will ensure that victims of online hate crime have their cases effectively and efficiently investigated. This will help the police to provide more tailored support to victims of online hate crime, through expert case management and detailed evidence collection. We hope that this will increase prosecutions and ensure that victims receive appropriate support and advice.

In addition, this Strategy clearly outlines the existing support for victims of online harms, including through the ending violence against women and girls (VAWG) strategy, the serious and organised crime strategy and the national cyber security strategy, the hate crime action plan and the support that government provides to older people who might be the victims of fraud online.

3. Introduction

The challenge

Technology is positively and rapidly transforming our economy and society. This pace of change has meant that society needs to catch up with the new challenges that it brings. In particular, there is growing public concern about online safety; this covers a diverse range of issues from online trolling and hate speech to location-sharing within social media platforms. Surveys show that for parents and carers, online safety concerns are becoming more prevalent than concerns about more traditional harms such as drinking or smoking. Many women have been subject to aggressive and sustained campaigns of abuse on social media. It is vital that collectively, we address these issues, so that the digital revolution continues to have the support of the British people, and that Britain can remain a world-leading digital economy.

The government wants Britain to be the safest place in the world to be online, as well as the best place in the world to start and grow a digital business. We are publishing this Strategy to set out how we plan to achieve this aim and to seek your views on how we should take forward our proposed online safety initiatives.

We firmly believe that to improve online safety, government needs to work with the technology sector to find solutions - from taking action against those who wish to use the Internet for criminal purposes, to tackling anti-social online behaviours and reducing access to harmful online content. Progress in these areas will take time, and we recognise that we won't be able to eliminate all risk of harm. This means it will also be vitally important that the government ensures that internet users - particularly children - know how to spot danger, understand what action they can take to keep themselves safe online and how they can support others to stay safe.

Our principles

The government will address online safety by bringing groups across society together – including the voluntary sector, technology firms, schools, and the people of Britain – to establish a coordinated approach.

Our work on the Internet Safety Strategy is underpinned by three principles:

What is unacceptable offline should be unacceptable online
One of the most common concerns about the Internet is that different rules apply there - acts that would be unthinkable in the physical world have become commonplace online. We reject this.

The government and police will protect citizens online in the same way that we do offline. Those who commit crimes online should understand that the law applies online, just as it does offline. And together we should establish that we expect standards of behaviour online to match those offline - it is no more acceptable to bully, insult and threaten on the Internet than it is in the street or the classroom.

All users should be empowered to manage online risks and stay safe
We all need to work together to give our citizens the knowledge and tools they need to stay safe online, so they can make the most of the opportunities that the Internet presents.

Technology companies have a responsibility to their users

Technology companies have a responsibility to promote online safety and protect the wellbeing and rights of all of their users. This means they have to be our partners as we work to prevent harmful behaviours and content.

Online harms

This Strategy seeks to address a wide range of harms, relating both to behaviours and content, which can be experienced online by users.

We know that too many people face online bullying, abuse and content that leads to anxiety, self-harm, eating disorders and even suicide. These harms are not new problems for society, but the Internet has increased the ease and frequency with which people can be exposed to these harmful messages.

We recognise that children in particular need to be supported to stay safe online. Our children are now introduced to technology at a young age. They are 'digital natives', and their natural comfort in using the Internet will be a great asset in a world where digital skills are ever-more essential. But we need to make sure they know how to use the Internet safely and responsibly. We want to help them build their digital literacy, to spot dangers, think critically about the content they are consuming, and to understand that actions have consequences online just as they do offline. We also want to make sure parents have the knowledge and confidence to understand how they can keep their children safe.

In addition, we are aware that adult users are concerned about harms such as online harassment and abuse. Certain groups within society are more likely to experience these types of issues. We need to tackle these problems to ensure that everybody can fully participate in life online without fear. To do this, we are looking at what support can be put in place for the vulnerable and those who are disproportionately likely to encounter harms online.

Our approach

Our work and the consultation questions set out in this document centre on four main priorities:

- Setting out the responsibilities of companies to their users;
- Encouraging better technological solutions and their widespread use;
- Supporting children, parents and carers to improve online safety;
- Directly tackling a range of online harms.

The government can best deliver these priorities and a safer online environment by working in partnership with others. Industry has to play a central role in helping us achieve this goal by improving online safety. Through safety by design, increased accountability and transparency, companies can take a leading role in supporting users.

We also recognise that no technology can be inherently good or bad. We value a free and open internet that protects freedom of expression and the platforms that promote it. What matters are the choices that we all make when we use these tools, the support and education that is provided, and the way these relate to the values we share as a society.

The government is uniquely positioned to highlight these issues and bring initiatives together to create a coherent strategy that is more than the sum of its parts – and to raise the bar in each individual area.

The government has made tackling online extremism a priority, and is also taking action on the most serious of crimes relating to terrorist use of the Internet, child sexual exploitation, cyber crime and online fraud. This vital work will continue to be led by the Home Office and will not be covered in this

green paper. These serious crimes require specific work with law enforcement and the security services, and well-established programmes of work are already tackling them.

Digital Charter

This Internet Safety Strategy is part of the Digital Charter. We are developing the Digital Charter, working with companies, civil society and others to establish a new framework that balances freedom with protection for users, and offers opportunities alongside obligations for businesses and platforms.

The Digital Charter has two fundamental aims: making Britain the best place to develop and deploy new technology; and making Britain the safest place in the world to be online.

This Internet Safety Strategy is part of the latter of these two aims - making Britain the safest place in the world to be online. It is the first strand of our Digital Charter work. This Strategy builds on and supports the government's broader work on cyber security, set out in the National Cyber Security Strategy published in November 2016. As the boundaries between technology and the physical world become increasingly blurred, cyber security and safety are now intrinsically linked. Cyber security measures and guidance help protect users from cyber risks, such as hacking and fraud, with a focus on making devices and platforms more secure. However, taking a robust approach to cyber security is not in itself sufficient in keeping users safe. The ambition of this Strategy is to detail what further steps need to be taken to keep individuals safe online.

Evidence

Alongside this Strategy, DCMS has published a literature review undertaken by Professor Sonia Livingstone, Professor Julia Davidson, Chair of the Evidence Group and Dr Joanne Bryce, on behalf of the UK's Council for Child Internet Safety (UKCCIS) Evidence Group. The report provides up to date evidence of how young people are using the Internet, the dangers they face, and the gaps that exist in keeping them safe. These themes are explored in more detail in Annex A, along with details of the online harms which adults can also experience.

This literature review is valuable in highlighting the gaps in our current knowledge. It also shows the importance of maintaining an up-to-date evidence base, so that we understand the pace at which online safety needs change. DCMS will now commission a literature review focusing on the online safety of adults. We anticipate publishing this review next year.

We will then be in a position to understand where further online safety research is required and will work with other organisations to address these gaps.

Consultation

This Strategy has been informed by a wide range of stakeholders including children's charities, internet safety organisations, academic researchers and technology companies. It also incorporates the views of a wide range of government departments and their partners.

This range of views has helped us decide which online safety proposals we should pursue. We are now seeking your views on these proposals, and how we should take them forward. Alongside this Strategy, we have published an online survey for adults to complete. This consultation represents important progress in our online safety work, and we want to seek as wide a range of views as possible.

As we have developed this green paper, we have drawn on the excellent work of The Royal Foundation Taskforce for the Prevention of Cyberbullying, convened by The Duke of Cambridge. The Taskforce's groundbreaking approach clearly aligns with the Strategy's intentions and will help inform our next steps. We look forward to the public launch of the Taskforce's work which is expected in the last quarter of 2017.

4. Our strategic response

As well as the direct action to provide better technological solutions and more support for children and their parents, we also want to make sure we have the right institutions in place. This section sets out our proposed strategic response.

Remodelling UKCCIS

This Strategy sets out a wide range of actions which will require cooperation between many different stakeholders.

Since 2010, the UK Council for Child Internet Safety (UKCCIS) has brought together organisations drawn from across government, industry, law, academia and charity sectors that work in partnership to help keep children safe online. UKCCIS has over 200 associate members. It works to share responsibility for online safety across all sectors while ensuring their buy-in. By providing a platform for communication in this way, it demonstrates the shared working approach we are taking in the UK, across all nations and sectors which is seen as good practice by other countries.

Through its working groups, UKCCIS has published guidance on handling sexting incidents for schools, in parallel with the police issuing revised guidance for officers.[1] It has also produced a guide for providers of social media,[2] parents and users of social media[3] and collated a large body of evidence on internet safety amongst other achievements.

We acknowledge the pioneering role that UKCCIS has played in promoting and championing improvements to child online safety in the UK. However, with a higher level of ambition not just for children but for all users, we want to make sure that the Council is aligned to the scope of this Strategy and able to hold government to account for our progress on online safety.

In order to do so, we will remodel UKCCIS to align with the Strategy so that it can take a leading role in this work. We propose:

- The Council will consider all users, not just children, and change its name to the UK Council for Internet Safety (UKCIS);
- A smaller, higher-profile executive board to set the Council's strategic direction and annual priorities;
- Reconsidering the role which the working groups undertake to ensure that we have flexibility to quickly respond to new issues. The important roles undertaken by the Education and Technical Working Groups will continue and we propose to expand the work of the Evidence Working Group to include adults;
- Based on the outcome of the consultation, we may decide to have an independent panel or working group which could support the government with arrangements for the social media levy;
- UKCCIS undertake a review of available online safety information and identifying gaps in resources.

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609874/6_2939_SP_NCA_Sexting_In_Schools_FINAL_Update_Jan17.pdf
[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/517335/UKCCIS_Child_Safety_Online-Mar2016.pdf
[3] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/490001/Social_Media_Guidance_UKCCIS_Final_18122015.pdf.pdf

Government's wider role

Action across central government and the wider public sector

DCMS is working closely with a wide range of partners in government to keep our citizens safe online, including the Home Office, Department for Education, Department for Health, HM Treasury, Cabinet Office, Ministry of Justice, the Government Equalities Office, and the National Cyber Security Centre.

In particular, in delivering this Strategy, DCMS will work closely with the Home Office, Department of Health and Department for Education. The upcoming Children and Young People's Mental Health green paper, which will be published before the end of the year, will reference improving the evidence base relating to the impact of the Internet on mental health and considering the role that technology has in affecting children and young people's mental health.

The Home Office is taking forward a wide programme of work to tackle illegal activity online, in partnership with the police, voluntary sector organisations such as the Internet Watch Foundation and industry, and at an international level through the WeProtect Global Alliance. It has established strong cooperation with the tech sector through the industry-led Global Internet Forum to Counter Terrorism, focusing on the threat from violent extremist content online.

The Internet Watch Foundation (IWF) is a not-for-profit organisation and self-regulatory body which is supported by the global internet industry and the European Commission. The IWF minimises the availability of online sexual abuse content, by predominantly focusing on the removal of child sexual abuse images and videos. The IWF offers a place for the public to report child sexual abuse images and video anonymously. They then have the images and videos removed.

While the Internet Safety Strategy does not cover illegal activities such as child sexual exploitation or violent extremist content, there will be clear benefits for these policies, derived from building users' digital literacy online and making it easier to tackle unacceptable online behaviour.

The **Committee on Standards in Public Life** is undertaking a review of intimidation experienced by Parliamentary candidates. They are also considering the broader implications for other candidates for public office and other public office holders. The Committee will produce a report for the Prime Minister, including recommendations for action and identifying examples of good practice by the end of the year.

To ensure the balance is right between freedom of expression and the integrity of the criminal trial process, the **Attorney General**, in his role as guardian of the public interest, has launched a call for evidence to analyse the impact of social media commentary on court proceedings in order to inform an assessment of whether any further guidance is required.

Engaging internationally

This Strategy focuses on online safety in Britain, but recognises that solutions and changes to behavioural norms are also needed at a global level. We will be talking about the challenges of online safety with leading tech companies and like-minded democracies as we develop our thinking on the Digital Charter. We will campaign to build a more robust international response to online safety and continue to focus on raising awareness with international bodies and our partners.

We will work through our network of diplomatic missions, to establish new support for our work, including through international institutions such as the UN, EU, Commonwealth, OECD and the Council of Europe. This will include steps to build relationships, share best practice and practical solutions.

This international effort will reinforce the leadership role that the UK has already established through the WeProtect Global Alliance.

We also believe that seeking a global leadership role on online safety will position Britain as a leader in technology that supports online safety. We will work closely with the Department for International Trade to ensure that the export potential for this technology is fully realised.

5. Working with industry to make online environments safer for all users

The government cannot keep citizens safe on its own, everyone has a role here: government, industry, parents, civil society and citizens. In particular, we need the technical understanding and expertise of the industry. This is why we will work in partnership with social media and other technology companies, working with them to provide safer online platforms for their users and providing support to do this where it is needed.

By working together and setting a clear level of ambition on safety, without prescribing exactly how companies should achieve this, we hope to build online safety without stifling creativity, innovation and growth in the Britain's digital economy. We are clear that our support for a free and open Internet remains undimmed, and that we do not want to restrict access to the Internet. But we do want to see a much more consistent approach to safety across the industry.

We will work closely with the technology industry to develop a framework that helps achieve that consistency, shares best practice, and agrees what will be expected of companies to protect their users from abusive behaviour and content online.

The issuing of the social media code of practice, as required under the Digital Economy Act 2017, will be the first step in this process. Alongside this, we are currently reviewing the existing regulatory framework. As outlined in the Conservative manifesto, we will consider further steps that may be required to continue to develop and uphold a robust regulatory environment that both supports digital service providers and delivers improved protection to users, including - if necessary - a sanctions regime to ensure compliance.

The manifesto also committed to introduce an industry-wide levy for social media companies and communication service providers to support awareness and preventative activity to counter internet harms. To assist with the introduction of the levy, we are using this consultation to ask questions about how it could be best implemented.

We want all internet users to be equipped with the right skills and digital resilience to stay safe online. But we also want to reduce the problems that users are currently encountering, and because a shift in the way users respond to threats will take time to achieve, it is critical that the technology industry takes action now to make products and platforms as safe as possible.

Leading companies are already advancing their commitments in this area. For example, Facebook has announced new machine-learning algorithms designed to help spot people at risk of suicide. Jigsaw (part of Alphabet), has released a new tool called Perspective, an application programme interface (API) that gives any developer access to comment moderation tools.

Tumblr is a microblogging and social networking website founded in 2007, and acquired by Yahoo in 2013. Tumblr displays targeted messages to users in response to searches containing certain trigger words relating to suicide, depression, eating disorders, self-harm and domestic violence. These messages interrupt the user experience and provide links to expert sources of advice. Tumblr also has 'safe mode' which filters sensitive content. 'Safe mode' is the default setting for all users.

While these sorts of efforts are a step in the right direction, the industry needs to ensure that available tools are more consistently available across different platforms, and better publicised to users. And as their technology evolves, so must the solutions they have in place to protect their users.

There has been significant recent public concern about acts of harm and self-harm playing out online, from the live streaming of suicides to anonymous public cyberbullying and the use of adult dating sites

and apps by children which have resulted in contact abuse. Leaked moderation guidelines have provoked much comment and debate, and shown the dilemmas that companies face when they try to tackle these issues.

The government wants to partner with industry to ensure these and other problems are taken seriously. We set out below the action that we intend to take.

1. Social media code of practice

This Government will work with the industry to secure a more coherent, joined-up approach to online safety across the range of major platforms. A key part of this will be issuing the voluntary code of practice, required by the Digital Economy Act 2017. We are consulting on what this will look like, with an aim of publishing the code of practice in 2018. The government will also consider the recommendations of the Committee on Standards in Public Life's review on the intimidation of Parliamentary candidates, which in due course may make recommendations on how online abuse should be tackled.

The code of practice will seek to ensure that providers offer adequate online safety policies, as laid out in the Digital Economy Act 2017, introduce minimum standards and metrics and ensure regular review and monitoring. The Act requires that the code addresses conduct that involves bullying or insulting an individual online, or other behaviour likely to intimidate or humiliate the individual (section 103(3)). This will be an important way for us to tackle pervasive issues such as trolling. The code will not cover unlawful content which the legal framework already addresses. We intend that the code of practice will be developed following this consultation.

The Digital Economy Act 2017 requires that the code of practice include guidance about (section 103(5)):

- Maintaining arrangements to enable individuals to notify providers of the use of their platforms for the specified conduct;
- Maintaining processes for dealing with notifications;
- Ensuring relevant matters are clearly included in the terms and conditions for using platforms;
- Information given to the public about action providers take against their platforms being used for harmful conduct.

As part of this green paper, we are consulting on whether guidance should also be issued on:

- Information on standards for user content and conduct, including how community guidelines are developed, enforced and reviewed;
- Information about the prevention and identification of abuse and misuse of services, including persistent abusers across a range of harms;
- Reporting mechanism for inappropriate, bullying or harmful content, with clear policies and performance metrics on take-down, including considering the manifesto commitment for content removal on a 'comply or explain' basis;
- Information about how to identify illegal content and contact, and report it to the relevant authorities in a local jurisdiction; and,
- Privacy and controls - policies, practices and communications.

Signing up and adhering to the code of practice provides an opportunity for industry to voluntarily demonstrate their commitment to improving online safety for the benefit and protection of all their users. This may require technical innovation or adjustments in the form of sharpening reporting mechanisms and privacy settings. We will also encourage better communication between industry and consumers, including on guidelines and terms and conditions.

This consultation asks questions about how you think social media providers are currently performing in terms of online safety and how you think we should take forward work on the code of practice.

2. Transparency

Social media companies are already undertaking significant steps to keep their platforms and sites safe for users through education, technological solutions and cooperation with civil society.

But not all users are aware of the tools available to them, or of the things they need to do to keep themselves safe on these platforms. One way of assessing both the problem and user awareness is through analysing the levels of reporting of abuse and inappropriate behaviour.

In this consultation, we have included questions on the possibility of working with industry to produce an annual internet safety transparency report. This could include common metrics which would enable benchmarking of reporting mechanisms. We believe this information would be valuable in understanding harmful content and conduct online and will help to underpin any future policy interventions in this area. In developing any such transparency report, we would avoid initiatives that might place disproportionate, additional burdens on either companies or users, that might discourage users from reporting, or that might lead to unnecessary delays in how companies respond to reports.

Depending on the outcome of our consultation, an annual internet safety transparency report could be used to show:

- the volume of content reported to companies, the proportion of content that has been taken down from the service, and the handling of users' complaints;
- categories of complaints received by platforms (including by groups and categories including under 18s, women, LGB&T, and on religious grounds) and volume of content taken down;
- information about how each site approaches moderation and any changes in policy and resourcing.

Regular annual reporting will help to set baselines against which to benchmark companies' progress, and encourage the sharing of best practice between companies.

3. Financing & industry structures

Some companies have already invested heavily to improve the online safety of their users, including through supporting end-user and civil society groups. However, we believe that more needs to be done and that it is right that all companies should be involved and encouraged to play their part. This is the reason we will introduce a levy, to help us combat online harms.

We have included in our consultation, questions about how to develop and deliver this. The objective of the levy will be to support greater public awareness of online safety and enable preventative measures to counter internet harms. These include both new initiatives proposed in this Strategy and existing programmes. As we develop plans for the levy's delivery, we will seek to ensure that it is proportionate and does not stifle growth or innovation, particularly for smaller companies and start-ups. And we will make sure it does not disincentivise tech companies investing in the UK.

Initially, we will look to secure contributions on a voluntary basis through agreements with industry, and we will seek industry involvement in the distribution of the resource. We will not seek to do this from scratch - we will consider existing safety initiatives that industry already delivers as part of our policy development. We may then seek to underpin this levy in legislation, to ensure the continued and reliable operation of the levy.

The levy will not be a new tax on social media. Instead, it will be a way of improving online safety that helps businesses grow in a sustainable way while serving the wider public good.

The manifesto likened this levy to the one that is set out in the Gambling Act 2005. While the Secretary of State has the power in legislation to bring forward a gambling levy, in practice the sector

provides voluntary contributions and support. The majority of these voluntary payments go to GambleAware, a leading charity in Britain committed to minimising gambling-related harm.

GambleAware funds education, prevention and treatment services and commissions research to broaden public understanding of gambling-related harm. The charity aims to broaden public understanding of gambling-related harm and help those that do develop problems, get the support and help that they need quickly and effectively. In 2015/16, GambleAware distributed £8.1 million: 15% was spent on research, 74% on education and treatment, and 11% on overheads.[4]

The idea related to the potential levies on gambling and social media will be similar as both ask industry to contribute funding to counter harms caused through their platforms and businesses. This could also be compared to industry funded charities like the Drinkaware Trust.

4. Advertising and social media

It is the user base of social media platforms that underpins their business model and allows them to generate revenue from advertising. While social media companies often do not make money directly from sales to users, they generate revenues by providing access to their user base for third parties or by advertising sales. The high levels of digital engagement in the UK, coupled with its economic strength, make this a key market globally.

In 2016, advertising provided over 95% of Facebook's revenue. While the USA and Canada prove to be the most profitable countries per user, Europe comes in second place, with the UK providing above average revenue compared to other European countries.[5] For 2016, eMarketer estimates the UK to have represented $1.8 billion of advertising revenue for Facebook alone.[6] A report by analysts OC&C suggests that collectively Facebook and Google's share of UK online ads is due to rise to 71% by 2020.

Recently, it has become clear that advertisers have become aware of how online safety issues and experiences on online platforms can reflect badly on advertising space that they have purchased. For example, Vodafone recently published new rules intended to prevent its advertising from appearing within outlets focused on creating and sharing hate speech and fake news. The government will explore, in an open and consultative way, how higher expectations of online safety from advertisers can be translated into a greater focus on safety from platforms.

5. General Data Protection Regulation

The government introduced a Data Protection Bill to Parliament in September 2017, which will include measures to protect children and provide individuals with increased control over how their personal data is processed. This, along with other measures in the Bill, will provide everyone with the confidence that their data will be managed securely and safely.

The government published a call for views in April 2017, on the various derogations (exemptions) in the General Data Protection Regulation (GDPR). On 7 August, government published the responses and the Statement of Intent for implementation of the Data Protection Bill. Under the plans, individuals will have more control over their data.

---

[4] https://about.gambleaware.org/about/
[5] http://www.telegraph.co.uk/technology/2016/11/03/how-much-money-does-facebook-make-from-you/
[6] http://www.campaignlive.co.uk/article/facebook-ad-revenue-rockets-57-26bn/1422945

There are three key changes, specific to the protection of data belonging to individuals, with additional protections offered for children. They are:

- A new requirement that privacy notices - which set out how an organisation plans to use the personal data it collects - be written in a clear, plain way that is understandable to the user, even if they are a child.
- A strengthened "right to be forgotten": individuals will be able to ask for their personal data to be erased. This will include provision to allow people to require social media platforms to delete information they posted during their childhood. In certain circumstances, individuals will also have the ability to ask social media companies to delete any or all of their posts.
- Parents or guardians will be required to give consent to information services (which include social media) where a child is under the age of 13. We will also make it simple for consent to be withdrawn.

6. Online games

More than half of all 8-11s (56%) and 12-15s (58%) play games online, making this an important focus for child safety in addition to social media.[7] There are risks in terms of age-inappropriate content, which might depict violent or sexualised scenes. There may also be risks of harassment and abuse as players interact with each other, which mirrors types of behaviour in online communities in general, including social media.

The government will work closely with online platforms, game publishers and developers, and with agencies such as the VSC Rating Board[8] to continue to improve online safety in games. Part of our work with industry will consider how to increase diversity and inclusion in gaming communities, and how to promote good practice in community management and technical player protection measures.

A major element of child protection for video games is ensuring that products are labelled to show their age-appropriateness and these age classifications can link to parental controls where they are available. Here, we benefit from the long-established, pan-European 'Pegi' age ratings for video games which are administered in the UK by the VSC Rating Board.

In the UK, games supplied as physical products (on discs and cartridges for example) must by law carry the appropriate Pegi 12, 16 or 18 ratings if they are unsuitable for children. It is an offence to sell or rent these products to anyone not old enough. On video games consoles, controls can be set by parents or carers to block access to games with certain Pegi age ratings, to block internet access and also to set limits on the amount of time children can play each day.

The market for online games, and those games available as apps for mobile or tablet devices, is global. Protections focus on self-regulation by games developers, publishers and platform providers and we welcome their collaborations in recent years. Administered in collaboration by a number of the world's games rating authorities, the International Age Rating Coalition (IARC)[9] for example is a key initiative in this area and ensures games and apps available through many online and mobile storefronts (such as Google Play and Microsoft Windows) have Pegi age ratings. Microsoft, Sony and Nintendo also require Pegi ratings for games content that can be downloaded from the stores on their consoles.

[7] Ofcom (2016), Children and parents: media use and attitudes report.
https://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf
[8] VSC Rating Board - http://videostandards.org.uk/Home/
[9] https://www.globalratings.com/

The industry initiative, AskAboutGames,[10] which is supported by trade body Ukie and the VSC Rating Board, aims to help educate parents and players about how to play video games safely and responsibly, about age ratings and the parental controls available across consoles and devices.

We will work with industry and others on:

- further promoting awareness and understanding of Pegi age ratings, parental controls and advice on safe gaming;
- considering what evidence there is of existing issues - including sexism - and also opportunities and thinking about issues that may emerge, particularly as new types of games (such as Augmented Reality) develop;
- developing understanding of the various safeguards, techniques and protocols that games companies use to manage their consumers' online game experience with a view to highlighting best practice;
- sharing guidance and best practice for games businesses to help them ensure their consumers - particularly children - can have a safe and enjoyable online gaming experience;
- exploring how the principles behind our social media code of practice should apply to the interactive elements of the games industry, with particular respect to reporting and take down of offensive user generated content.

[10] http://www.askaboutgames.com/

6. How can technology improve online safety for all users

Increasingly, the best solutions for keeping users safe online are technological ones. The growing effectiveness and accuracy of tools based on artificial intelligence, for example, are making a real difference. This Strategy aims to put in place the right support for this technological innovation to flourish in Britain. This will not be about heavy-handed government intervention; instead, we will look at overcoming barriers to safety-conscious and responsible companies bringing their products to market, and seeking to create the demand to support long-term UK growth for safety products.

Microsoft PhotoDNA is a technological response to tackling child exploitation images that have been identified by trusted sources. PhotoDNA Cloud Service hashes and converts images into numerical values which are matched against databases of hashes from known illegal images. This hashing and matching process makes it possible to distinguish and flag harmful images from the billions that are uploaded daily. While child sexual abuse imagery will not be addressed through this Strategy, we will work closely with technology companies to promote the development of analogous technological solutions.

Instagram recently announced a new artificial intelligence system to reduce the number of comments that violate Instagram's Community Guidelines. The new filter, DeepText, connects how words are used together to differentiate between an innocent use of a word and where, when put with other particular words, it can have a negative or harmful meaning.

As part of our consultation, we are keen to gather views on how we can encourage manufacturers, developers, retailers and consumers to give consistent consideration to safety. We want to embed the principle of 'think safety first' into the development of new technology. To achieve this, we intend to explore the following areas:

1. Supporting the internet safety technology market

As set out in our Digital Strategy, this Government wants to foster an innovation-friendly regulatory environment, to ensure that regulation across sectors is open to the benefits of new and disruptive digital innovations which help to improve online safety. We will work with business and partners across government to understand whether there are existing barriers to entry for companies looking to bring online safety products to market and look to address these problems.

The UKCCIS Technical Working Group first met in October 2016. The overall aim of the group is to provide a focal point and centre of excellence within UKCCIS for technical issues as related to online child safety. The group has identified issues that need further consideration including smart TVs, privacy and collection of data and virtual, mixed and augmented reality issues.

We will build on the work of the fledgling UKCCIS Technical Working Group to enhance the reach of their work and help turn their recommendations for better safety design features into reality by creating a Technical Network. This will bring together a specialised group of engineers and innovative tech businesses who will work together to develop and share new ideas and where businesses can communicate and challenge each other. This will look at areas such as artificial intelligence and the Internet of Things (IoT) and how they can be made safer for all users.

2. Encouraging technology firms to 'think safety first'

This Government made clear in our Digital Strategy, our ambition to make Britain the best place in the world to start a digital business. But start-ups developing new products have told us they lack the capacity and expertise needed to build safety into their products from the start. To address this, DCMS will work with industry bodies like TechCity UK to support start-ups at the very earliest stages of their development so that they know what good online safety looks like. Along with sharing of industry best practice, this will help them to build online safety features into their products from the very start.

This work will sit alongside discussions already underway as part of DCMS's 'Secure by Default' review. As part of the review, a report will be published which will include high level recommendations that will seek to improve the cyber security of consumer internet-connected devices and the connected services.

DCMS will also work with established companies who are developing new products or updates, to ensure that internet safety, cyber security and data protection are all part of the design process.

We will work with the industry to develop guidance explaining the safety principles that apps should aim to achieve, without prescribing specific technical measures.

This will emphasize the business benefits of getting online safety right, including simple reporting mechanisms and quick response times to complaints. For example, there has been a pattern that a lack of reporting on new apps can lead to them being used to send inappropriate or harassing content. Including reporting from the start would greatly improve customer experience and save the business from future complaints and need for app redevelopment. This work will be informed by lessons learned about online safety by larger, more established apps.

As part of this offer to start-ups and smaller companies, DCMS will also produce easy to follow guidelines about where companies can seek support if something does go wrong.

3. Additional measures for the safety of all users

We would like to encourage social media companies to tailor their products so that they provide consistent protections to children and young people. For example, by offering walled garden versions of their platforms, companies can give children the freedom to explore with less chance of harm. Many of the key companies have already developed excellent online products and tools.

In 2017, the LEGO Group launched their social themed app, LEGO® Life. The app is designed for younger children, particularly those from ages 8 -12, and it aims to inspire children to build and share their creations in a high-safety, high-trust environment. LEGO® Life applies the principle of safety-by-design, as well as introducing children to some of the more positive features found in other social platforms, demonstrating how social media sites can enrich their lives through sharing with family and friends.

The app is now available in 18 countries around the world and has over 3.2 million downloads. In addition to this, in 2018 the LEGO Group will launch a Parental App, Hub and Dashboard, taking a further step in securing the peace of mind of parents as well as providing them with more opportunities to share in the creative experience with their children.

One major concern is that a high proportion of children using the Internet, and their parents and carers, are not aware of the tools on offer that can keep them safe. We would like companies who already offer these features to promote these more effectively, both to their younger users, and to

their parents and carers, so that there is much greater awareness of what tools are available for staying safe online, how easy they are to use, and the benefits of using them.

The Youtube Kids app was launched in the UK in 2015 to offer a safer Youtube experience. Adults are able to tailor the viewing experience, for example a timer can be set to limit how much time a child spends on the app.

iPlayer Kids provides a similar platform for BBC children's content. The app has a variety of safety features including a lock that stops children leaving the app and filtered, age-appropriate content.

Online safety is an issue for everyone, not just children. As part of this consultation, we are keen to understand what specific safety features you would like to see manufacturers or online companies introduce.

4. The role that applications and app stores play

With over two million apps available through the major app stores, we want to ensure that online safety is built into these platforms. This will involve app platforms developing safety standards for the apps sold on their platforms, including more information about safety features and how users can enable them.

Both the Google Play Store and Apple's App Store already promote safety features, particularly for apps designed for children.

All apps in the Google Play Designed for Families programme must be relevant for children under 13 and must meet certain criteria, including in relation to ads, interactive elements, age-appropriate content and privacy. Apps that are primarily aimed at children must participate in the Designed for Families programme and are then featured in the Family section of the Google Play store.

The App Store Kids Category highlights apps that are suitable for children. Apps must be designed for younger users and must not include links out of the app, in-app purchasing or other distractions to children. Apps must not include behaviour advertising or advertising that is age-inappropriate.

Despite the schemes already on offer, details on safety features within apps are inconsistent. To encourage 'think safety first' (ie building in safety features from the start of the design process) and improve consumer understanding, we are keen for app store providers to make safety considerations and features in apps clearer and more uniform in app descriptions. We will work with the app stores on the most effective way to implement the government's commitment to introduce new protections for minors from age-inappropriate content in app stores.

While we welcome age ratings on all apps, games and other online platforms, where there are age requirements within the app's terms and condition, we would also like these to be made clear to consumers.

We are interested in how a voluntary cross-industry approach, including app stores and social media platforms, could improve online safety.

5. Safety values

We are considering whether our 'think safety first' work should be underpinned by the development of a voluntary 'baseline', setting out a series of basic principles which we would want to see applied

across all app stores. This would help set clear expectations for the industry, and by helping consumers make informed choices, the business value of developing strong online safety would be clearer to start-ups.

The baseline could cover key areas such as:

- What safety functions details should be included in upfront descriptions of an app on stores;
- Clear information to users on what metrics need to be considered when app producers / app stores assign a rating to a product;
- Information on how to report safety concerns relating to a specific app, and the feedback process users can expect after reporting concerns;
- Buyers being given material information about products they are being offered. Apps, connected toys, and other products including a basic explanation of how they operate, what they connect with and what happens to data that is collected as a result;
- Key information which should be included in terms and conditions.

App stores may also be able to play a part in the promotion of safety conscious apps through the 'featured' section of their store. This would give the apps with proper safety features better publicity and encourage both consumers and developers to consider the business value of safety features.

In 2015, the UK Council for Child Internet Safety (UKCCIS) published a practical guide for providers of social media and interactive services. The guide has examples of good practice from leading technology companies, and advice from charities and other online child safety experts. Its purpose is to encourage businesses to think about "safety by design" to help make their platforms safer for children and young people under 18.

As part of our work on the Strategy, DCMS will consider how to tailor and promote this UKCCIS guidance for app stores.

6. Connected toys

The UK is already an international leader in research and development and adoption of the Internet of Things (IoT). Government action includes the three year IoT UK Programme. The benefits of IoT to citizens, including children and young people, could be huge. However, connected devices such as toys and home electronics also bring new challenges, for example, in relation to children's privacy.

Earlier this year, the connected My Friend Cayla doll was banned in Germany over fears that it has a concealed transmitting device. The move was taken by the Federal Network Agency (Bundesnetzagentur) which enforces bans on surveillance devices and German parents have been urged to disable the interactive toy.

DCMS are leading a review which is looking at the security of consumer internet-connected devices and the connected services linked to the devices. Following the publication of the review's report, we will consider where the lessons from this review might help inform further work on connected toys and scope other aspects that should be considered, including privacy requirements.

7. Innovative delivery

We know that any Strategy from government that sounds like it is instructing people how to behave runs the risk of missing the mark. This is why, we will look at more innovative delivery models to reach users.

Where DCMS's arm's length bodies and partner organisations interact with internet users, we will explore how they can deliver messages about safety online.

7. Supporting children, parents and carers

We believe society needs to equip everyone to be safe online. As part of this, we want children and young people to be confident in using the Internet and accessing the benefits it can bring. As children are now using the Internet earlier than ever before, we need to start building digital literacy skills from a young age. These skills should continue to be built throughout a child's life, so all children can understand and successfully manage online harms when these occur. Ultimately we hope that fostering good online safety skills from a young age will help individuals develop into responsible adult users of the Internet.

Although schools clearly play a key role in educating children about online safety, we also want to ensure online safety information is disseminated through other means so that children receive consistent, regular reminders about how to stay safe online, and understand how to think critically about the content they consume and engage with. This consultation asks questions about how we can best ensure this happens. The measures put forward in this section cover children in England, as education is a devolved issue. They form our response to the manifesto commitment, to ensure that all children learn about the risks of the Internet, including cyberbullying. We hope a similar emphasis will be placed on teaching children online safety across Britain.

Parents and carers have a critical role in protecting their children online. We want them to teach their children about online safety, just as they help them tackle other challenges in the offline world like road safety. But this does not happen when parents are uncomfortable with the technology their children are using, and intimidated by the fact that their children know more about it than they do. This Strategy looks at how we can support parents and carers to give them the knowledge and confidence they need.

Part 1 - Supporting children

1. RSE and PSHE education

Today's is the first generation of children who are learning about relationships and sex in an online world. Many of the experiences that are fundamental to growing up, like building friendships, testing parental boundaries and exploring sexuality, are complicated by growing up online.

The risks are not new. Problems like pornography and bullying have challenged previous generations. But the Internet has amplified the risks. It is right that we take a fundamentally new approach to preparing our children to tackle these risks.

Public Health England's 'Rise Above' campaign which launched in 2015 aims to delay and prevent risky behaviours and by tackling multiple issues builds emotional resilience in young people aged 11 to 16. It aims to equip them with the skills and knowledge they need to make better health decisions, and deal with the pressures of growing up. The campaign covers a range of topics from core risk behaviours such as drinking and smoking to sexual health and mental health issues including online stress, cyberbullying and the impact of social media on relationships and body image.

The changes introduced in the Children and Social Work Act 2017 represent a step change to education on these issues. For the first time it will be compulsory for primary-aged children at school in England to be taught Relationships Education, and for all secondary-school children to be taught Relationships and Sex Education (RSE).

In addition, the Department for Education (DfE) will carefully consider whether to also make Personal, Social, Health and Economic (PSHE) education compulsory in all schools.

DCMS and DfE will ensure new compulsory subjects in England address the challenges experienced by young people online and are seeking views to work out how best to do so. DfE will support schools to ensure that content is pitched at the right level for each school year and builds knowledge as children grow up. Engagement and consultation will help us to get the detail right, but we expect it will start with the basics, including building friendships online in the early years of primary school, through to cyberbullying and contact advice; and then online pornography and sexting education at age-appropriate points as children get older.

DCMS and DfE will generate the 'online safety' aspects of these subjects; and conduct thorough and wide-ranging engagement and consultation, including with parents and carers as well as children and young people. This will include: subject content, school practice and quality of delivery in order to determine the content of regulations and statutory guidance. We will work with partners, including: social media and technology companies, subject experts, law enforcement, English schools and teaching bodies to ensure these subjects are up-to-date with how children and young people access content online and the risks they face. Recognising that these can be challenging topics for schools and teachers to deliver successfully, DfE will also consider how best to support schools in the delivery of these new subject(s).

DfE set out in their policy statement in March this year, that mandatory Relationships Education, RSE and - subject to the outcome of a thorough consideration as set out above - PSHE - will come into force in September 2019. Schools in England will be required to publish their policies on Relationships Education and RSE to ensure parents understand what their children will be taught at school in these subjects. DfE will consider how best to ensure relevant guidance remains up to date with technology and trends, and will update the guidance regularly.

Teachers will play a vital role in delivering the online aspects of the Relationships Education, RSE and, potentially, PSHE and we need to make sure they feel equipped with the right knowledge and skills. DfE will ensure schools in England can deliver the new compulsory subjects to a high quality.

2. Digital literacy

Digital literacy is already part of the new computing curriculum and will be part of the new compulsory subjects of Relationships Education, RSE and - potentially - PSHE. Maintained schools already teach children basic e-safety information such as recognising inappropriate content and contact; and how to report concerns. Digital literacy helps give children the tools they need to make smart choices online.

We want to tackle the growing trend that online behaviours fail to meet the standards that we expect from our children in the 'real world'.

Digital literacy is also about being able to critically interpret content encountered online, for example being able to recognise commercial content and advertising. It needs to include an understanding of how search engine results are generated, and being able to question sources of information and news. We want to ensure that schools develop children's critical thinking skills so that young people are better able to recognise intentionally misleading information. In the long-term, giving our young people the tools they need to assess material online will be the single most effective antidote to fake news.

In developing digital literacy, children should learn digital citizenship: understanding what behaviours are acceptable online and how to contribute to a positive online environment where everyone feels able to participate. As well as digital resilience: building the personal emotional resources needed to understand online risks, knowing what to do to seek help, learning from experience and recovering when things go wrong.

DCMS and DfE expect that digital literacy, including online citizenship, will form a part of compulsory Relationships Education, RSE and/ or a possible compulsory PSHE subject. The engagement process and consultation on introducing these subjects will help us to determine how this topic will be covered, working closely with established stakeholders such as the PSHE Association.

The PSHE Association has integrated digital literacy (including skills and attributes that contribute to digital literacy and online safety) into their curriculum framework for PSHE education and the teaching resources they develop. The Association is also developing a comprehensive training offer from early 2018 to help teachers cover the range of online issues through their PSHE programmes.

We will ensure that any new digital literacy teaching builds upon existing lessons. The new computing curriculum (covering ages 5-16) is compulsory in maintained schools in England and can be used as a benchmark in Free Schools and Academies. It was developed by industry experts and includes digital literacy. Children in maintained primary and secondary schools are taught how to use technology safely, respectfully and responsibly; how to keep personal information private; how to recognise unacceptable behaviour; and how to report concerns about content and contact. The e-safety content of the computing curriculum was developed with input from organisations such as the NSPCC and the UK Safer Internet Centre.

Pupils are also taught offline citizenship at key stages 3 and 4 as part of the national curriculum (covering all maintained schools, and those academies and free schools that opt to use this). While the online world is not explicitly approached, citizenship aims to teach pupils the knowledge they need to think critically and to develop the skills to research and to interrogate evidence, including teaching on 'the diverse national, religious and ethnic identities and the UK and the need for mutual respect and understanding'. The current citizenship curriculum therefore complements the aims of this Strategy to develop young people's digital resilience and sense of digital citizenship.

DfE continually monitor the impact of all curriculum reforms through uptake of qualifications, attainment of pupils, progression rates and stakeholder feedback.

'Internet Legends' is Google's programme to educate primary school children in the UK on online safety. The aim is to empower children with skills they need to stay safe and act responsibly online. The programme was designed in partnership with Parent Zone and with support from Childnet, Oxford Internet Institute and Internet Matters. The programme has reached over 20,000 children to date.[11]

As part of this consultation, we are asking for your views on how the technology industry can best support children's digital literacy.

3. The wider role of the education system

Early years

As children are using the Internet from a very young age, we need to ensure that they do so safely. We will ensure online safety guidance is received by parents and carers with children at the Early Years stage. We will consider how this can be shared with settings via key early years stakeholders. Any changes in this area will have a wide reach and ensure that children from families who aren't confident technology users, still receive the support they need.

[11] https://www.google.co.uk/intl/en/safetycenter/families/legends/

Schools

The role of schools in assisting children with online safety is not restricted to formal education. Schools play a critical role supporting children when they have suffered online harms. This can include responding to incidents of cyberbullying (both in and outside of school hours) and intervening following the unwanted sharing of sexually explicit images around classmates. This presents additional challenges for schools and teachers, particularly in relation to their legal responsibilities. Together, DCMS and DfE will continue to ensure support for schools, including signposting the range of materials that are available.

Keeping Children Safe in Education (KCSIE) is the statutory guidance to which all schools and colleges (in England) must have regard when carrying out their duties to safeguard and promote the welfare of children; it was last updated in September 2016. For the first time, it included a section covering online safety in schools. According to KCSIE guidance, schools and colleges should have appropriate filtering and monitoring systems in place to safeguard children from harmful and inappropriate online material.

The UK Safer Internet Centre has published guidance as to what "appropriate" might look like and sets out the need for a whole school approach to online safety, including a clear policy on the use of mobile technology in the school or college. DfE will continue to use statutory safeguarding guidance to reinforce the responsibilities of schools and colleges with regards to online safety. DfE will be consulting on revising this guidance in Autumn 2017.

By law, every school must have measures in place to prevent all forms of bullying. Pupils should feel that they can report bullying which may have occurred outside school including cyberbullying. DfE will work on how to support schools to be clear about their responsibilities on cyberbullying.

Many schools are already successfully keeping their children safe online and responding to incidents of online harm. Organisations like UKCCIS, Childnet and Internet Matters have helpful resources for schools to use in doing so. Some schools have full handling plans in place to deal online harms, and we want to see these best practices become standard. Schools also present a platform to provide messages to parents and other responsible adults on online safety. More information about how government will support adults to help children is outlined in the following section.

South West Grid for Learning (SWGfL) is a charity that works in the field of online safety, with a specialism in supporting those working with children, particularly schools. SWGfL provide tools such as 360 Degree Safe, an online safety self-review tool which is currently supporting over 11,500 schools to evaluate their online safety provision and strategy. Similarly, their tool Online Compass is designed to show any group that works with young people (for example, sports clubs and libraries) what needs to be done to make their use of technology safer.

The UKCCIS Education Working Group will be shortly launching a detailed framework for teachers to identify the key learning that pupils should have received at various ages in order to be a good digital citizen. The planned second phase of this work includes developing accompanying resources such as teacher's activities, and an assessment criteria which will underpin the framework. The framework will outline 'what' needs to be done by teachers in the area of online safety and the accompanying materials will outline the 'how'. This will also support development of Relationships Education, RSE and, if relevant, PSHE. DfE will continue to use the UKCCIS Education Working Group to provide support to schools on online safeguarding.

UK Safer Internet Centre (UKSIC)
The UK Safer Internet Centre is a partnership of three leading charities – Childnet, the Internet Watch Foundation (IWF), and South West Grid for Learning (SWGfL) - with a shared mission to make the Internet a better and safer place for children and young people.

The partnership was appointed by the European Commission as the Safer Internet Centre for the

UK in January 2011 and is one of the 31 Safer Internet Centres of the Insafe network.

The UKSIC delivers five main activities:

1. Education, training and awareness: increasing the UK's resilience through innovative tools, services, resources, campaigns and training
2. Helpline: supporting the children's workforce
3. Hotline: disrupting the distribution of child sexual abuse content
4. Youth participation: giving youth a voice and inspiring active digital citizenship and peer education
5. Leadership and collaboration: creating a UK and global eco-system that embeds online safety

For more information visit www.saferinternet.org.uk and the websites of the partners: Childnet, Internet Watch Foundation and SWGfL.

Safer Internet Day

Safer Internet Day celebrates the safe and positive use of digital technology for children and young people. It is celebrated globally in February each year and over one hundred countries took part in 2017. The UKSIC co-ordinate the event in the UK. Over 1,600 organisations supported Safer Internet Day 2017 and the day collectively reached 42% of UK children and 23% of UK parents.

4. Other ways to support children

As part of this consultation, we want to hear how you think we could further support children in understanding and handling online risks.

DCMS's recent Digital Strategy highlighted the innovative initiatives that are taking place outside of formal education including the 5,000 Code Clubs that use volunteers and top quality online material to give young people the opportunity to learn how to code. The majority of Code Clubs are run from local libraries. The government will ensure that online safety resources are available to these Code Clubs.

As a resource for children, the BBC's online services provide a safe, trusted space where they can learn, create and have fun in one place. It makes a substantial impact in children's digital literacy and resilience, with the brand[12] and creative track record to do so.

CBBC's Dixi, for example, has won the BAFTA for Best Interactive[13] for the way it has engaged children on online safety issues within an innovative online drama format. Now on its fourth series, it has made a significant impact on its audience: 85% of its audience consider it a fun way to learn about being safe online; and two thirds have updated their privacy settings on Twitter and Facebook as a result.[14]

The BBC will be building on its brand, reach and creativity to engage children online further. It has launched Stay Safe, an online portal for digital safety and citizenship, and has announced additional investment of £34 million across three years to 2019/20 into BBC Children's that will fund an enhanced online offer.

[12] CBeebies is the most well-loved brand among 0-6 year olds (Ipsos Mori Brand Tracker). It's the 3rd most popular website for children after Google and Microsoft (Ofcom, Children's Media Use and Attitudes 2016, top web properties accessed by children aged 6-14 from desktop and laptop computers)

[13] BAFTA 2014 for first series

[14] Safer Internet Day 2015 Evaluation, Populus/UKCCIS

We will engage with the BBC as they support and promote child online safety and digital literacy through BBC Children's Stay Safe initiative, helping UK children become among the most digitally literate and resilient in the world.

Peer to peer support

Children and young people are increasingly using the Internet to provide each other with peer support and social media can be an excellent resource in assisting children in accessing communities and support.

Peer to peer support can play a vital role in helping children to help themselves with online safety. Messages about online safety delivered from government, parents and carers or teachers run the risk of being ignored by children and teenagers as unconvincing, or failing to appreciate why and how young people use the Internet the way that they do. In contrast, support from peer groups is likely to be more persuasive.

In developing this Strategy we have considered existing initiatives, like Childnet's Digital Leaders scheme which aims to empower children and young people to champion digital resilience within their schools and to educate their peers, parents and teachers about staying safe online.

The Childnet Digital Leaders Programme is a pupil-powered online safety programme that helps schools put young people at the heart of their whole-school approach and ensures internet safety learning is fun and effective. With interactive training and an exciting online community, the programme empowers young people to be Digital Leaders so they can educate their peers, parents and teachers about staying safe online. The programme is delivered by Childnet as part of its work in the UK Safer Internet Centre.

Feedback includes:

"I think the programme is so useful for being able to get young people involved in spreading the word about internet safety. It has taught me new ideas that I have never thought of as well as allowing me to teach my friends and peers about this too so we become a safer community overall." Pupil

"The programme has enabled and inspired the children to create their own resources and posters etc, which have been displayed around the school site raising the profile of online safety." Teacher

Other initiatives include the Diana Award Anti-Bullying Campaign, funded by DfE and supported by Facebook and Vodafone, which has trained over 22,000 young people to be Anti-Bullying Ambassadors; young people who are responsible for leading on Anti-Bullying campaigns and promoting online and offline safety to their peers. The Diana Award has also established a National Youth Board, a group of young people from across the country who meet to share ideas on how to tackle bullying and provide support on online issues. In addition, they will be developing a dedicated anti-cyberbullying toolkit with support from top social media providers including Facebook and Snapchat.

The Childnet Film Competition is an annual national competition established in 2010 that invites young people aged 7-16 years to create short films to inspire their peers to use technology safely, responsibly and positively. Harnessing the positive power of digital creativity, the project gives young people an opportunity to take the lead in educating and empowering young people in their school and across the UK. The competition is delivered by Childnet as part of its work in the UK Safer Internet Centre.
Over 120 entries were received from children and young people right across the UK, and the six winning entries were showcased at a private screening at the BFI in London attended by industry guests and all of the young filmmakers. The films are all BBFC-rated and shown on the big screen.

DfE are launching a pilot of how to safely put in place peer support schemes for children and young people's mental health and wellbeing as part of pastoral support in 100 schools and colleges as well as in ten youth and community groups. DfE will work with a contractor to deliver the pilot, which will be accompanied by an independent evaluation. The pilot will run into 2018/19.

We believe there will be significant value in DCMS encouraging and supporting peer to peer support programmes like these that are focused specifically on online safety. This consultation asks which children you think would most benefit from such a programme.

Ditch the Label were the first digital anti-bullying charity, providing digital interventions and support for thousands of young people every week. It has revolutionised the way teens access support which feels natural and authentic to them.

In addition to hundreds of support guides which tackle bullying and the surrounding issues, they have *Community* which brings young people together in a safe space to discuss any concerns they may have. They are also able to support teens 1:1 through their website.

Civil society

We are keen to explore how we can work with civil society to get young people the guidance they need to stay safe online. We are exploring how to engage with the National Citizen Service graduate network, which is expected to comprise of 400,000 young people by the end of 2017. We will work with Scouts and Girl Guiding UK, particularly through their mixed programmes and open access youth services to reach young people.

The Scout Association have partnered with Vodafone to make sure that young people are not only using technology to enhance their lives, but are doing so safely. Last year they released an e-safety game called 'Stay Safe' which helps young people to understand how to stay safe online through a number of interactive activities. They additionally partnered with Vodafone to create two new badges, the Digital Citizen and Digital Maker badge. These badges aim to empower Scouts to develop their digital skills and teach them how to balance their digital and "real-world" time, ensuring they have time away from screens.

Girl Guiding has agreed to work with government to help girls and young women stay safe online. This includes: sharing research, for example the annual Girls' Attitudes Survey conducted by Girl Guiding; peer to peer education programmes; and joining resources to spread safety messages and useful tools for both parents and children.

The 2017 Girls' Attitudes Survey which surveyed over 1900 girls and young women aged 7–21, found over a third of girls as young as eleven say that comparing their lives to others is one of the greatest worries they have about spending time online. While less than half (47%) of those questioned feel that their parents realise the pressures they face on social media.[15]

Such civil society groups have a good track record on reaching children from lower socio-economic backgrounds and 'hard to reach' families who can be particularly vulnerable to online harms. To support the delivery of key internet safety messages, the government will ensure that appropriate materials are available for these groups to use.

Libraries

[15] https://www.girlguiding.org.uk/social-action-advocacy-and-campaigns/research/girls-attitudes-survey/

The 3,000 libraries in England offer many ways of engaging both children and parents and carers, locally and nationally. There are several ways in which libraries could deliver messages about online safety. We will encourage them to:

- Embed online safety aspects into existing library projects and events;
- Run family learning sessions to help adults to support their children online;
- Display online safety material and signpost resources for library staff, parents and children.

Public libraries support Safer Internet Day, often delivering workshops and drop in sessions to help their communities feel more confident about being online. The UK Internet Safer Centre creates Education Packs and complementary Safer Internet Day TV films tailored for 5-7s, 7-11s, 11-14s, 14-18s and parents and carers.

Sports clubs

We know that sports programmes have the potential to strengthen social networks and community identity. We also know that there is a link between active lifestyles and healthier, happier people. Being active matters and sports clubs are one way children and young people can lead active lives.

The Child Protection in Sport Unit (CPSU) is a partnership between the NSPCC, Sport England, Sport Northern Ireland and Sport Wales. CPSU works with UK Sports Councils, National Governing Bodies (NGBs), County Sports Partnerships (CSPs) and other organisations, as well as in partnership with over 200 sports bodies in England, Wales and Northern Ireland through multi-agency safeguarding in sport partnerships in each home country.

CPSU provides guidance and training on how to set and manage policies and procedures for electronic communications, club websites and use of social media. The government will work with CPSU and others on how we can enable children and young people to have positive and safe interactions in online communities around sport.

Part 2 - Empowering parents and carers to help children

This Strategy is also concerned with how parents, carers and teachers can be empowered to talk to children about online safety.

The majority (84%) of parents of 5-15 year olds have approached the subject of online safety with their children. Parents are now more worried about their children sexting than they are about them drinking or smoking.[16]

Help and advice already exists for parents and carers, but this offer is piecemeal and varies between organisations. The government wants to see consistent advice for parents which is easily accessible and well-publicised. We will task UKCCIS with reviewing the online safety materials which are currently available, identifying any gaps in resources. We will seek their advice on how we can ensure parents and carers know what is available and can easily access the support they need.

Government supported material for parents includes the work of Thinkuknow, an education programme from the National Crime Agency's CEOP Command established in 2006. The NCA's Thinkuknow education programme provides educational resources for use with children and young people helping them to identify the risks they may face both online and off. Thinkuknow produces up-to-date social media guides for parents and carers. These include –"Should I be worried", "How to set parental controls" and "How to make a report to the site/app".

[16] https://www.pshe-association.org.uk/news/parents-call-education-address-sexting-children

The Children's Commissioner for England will be exploring whether the access of children in care to digital networks is restricted by their care status or safeguarding concerns of the adults caring for them, and what can be done to broaden access safely and fairly. The Commissioner is also working with partners and care leavers to explore creating a safe digital platform to connect children in care councils across the country. Both the Commissioner and DCMS will be feeding into DfE's fostering stocktake which is reviewing the fostering system to improve outcomes for looked after children.

Following the publication of the Children's Commissioner's report on Growing Up Digital in January 2017,[17] the Commissioner for England has continued to play an active role in looking at how we prepare children for life online and continues to challenge policy makers to put children's digital rights and resilience at the heart of the new citizenship curriculum.

Most recently, the Children's Commissioner has launched a 'Digital 5 a day' campaign which is designed to help parents and children manage their time online.[18] The campaign aims to encourage parents to talk to their children about: who they connect with online; the importance of balancing physical activity with time online; using creative internet tools; giving to others to make the Internet a positive environment and being mindful about the amount of time spent online and how it can affect mental wellbeing.

The Commissioner has challenged social media companies to be clearer with children about their rights and privacy. As part of this, the Commissioner is working with TES to produce simplified versions of the terms and conditions for Instagram, Facebook, WhatsApp, YouTube and Snapchat so that teachers can help their pupils understand how the web works and what they agree to when they join social media sites and install apps.

We recognise the importance of external challenge and will work with the Children's Commissioner and other leading bodies to deliver this Strategy.

1. Support for parents

We know that new parents and carers are particularly receptive to parenting advice. Equipping new parents to deal with online safety issues should help prevent future online harms. DCMS will ensure that targeted information about young children and technology is available to new parents. This information will be sent to parents through a number of different routes, for example National Childbirth Trust courses, Bounty packs, Sure Start children's centres and other early years settings, Bookstart, Mumsnet, Netmums, Facebook groups for local communities of parents, pharmacies, nurseries and parenting apps.

This information will focus on the technology and parenting issues that are relevant to this young age group, including the impact of screen time on a child's cognitive development and information that parents may want to think about before sharing photos of their child, like whether the app has location-sharing enabled, and privacy considerations. We are keen to seek parents' views on the topics which they would most like support on.

By starting with the technology issues that we know parents are already concerned about, we hope to start an informed conversation with them about child safety from the cradle, meaning they feel better equipped to handle future challenges like their child's use of social media, cyberbullying, harassment and online pornography.

Parent Zone provide information to parents and schools on issues related to the Internet. They

[17] https://www.childrenscommissioner.gov.uk/publication/growing-up-digital/
[18] https://www.childrenscommissioner.gov.uk/2017/08/06/digital-5-a-day/

produce a Digital Parenting Magazine, in partnership with Vodafone, and distributed 1.5 million copies of the last edition. Parent Zone also provide online advice which schools can share with parents via their own website, as well as offering other resources and training through their Digital Schools programme. Their parent guides cover a diverse range of issues including live streaming, virtual reality and connected toys.

2. Technology solutions for parents

A burgeoning market for online safety technology tools for parents already exists and this Strategy aims to provide more information about the available options to parents. UK technology companies, including Internet Service Providers and mobile network operators, have traditionally been at the vanguard of technical development to deliver tools to help parents manage their children's online activities.

Smaller firms and start-ups have also now entered the safety market and there are technological solutions available that allow parents to play a more active role in protecting their children online. These range from apps which monitor children's social media accounts and switch off their devices remotely, to software content filters that alert parents if a child is at risk of cyberbullying or other risks.

Amazon's **Fire Kids Edition** tablet offers easy-to-use parental controls that encourage learning before play. Parents can limit access to games, cartoons and videos while leaving unlimited time for reading—or can block access to content until after educational goals have been met. It has a child-safe camera which allows parents to view photos and videos taken by their child, and there are no ads or in-app purchases. Parents can control when the tablet shuts down, and set up multiple profiles so that each child's experience can be personalised.

In addition to this, Amazon offers **Fire for Kids Unlimited**. It's a subscription service which provides age-appropriate content for 3 - 5, 6 - 8 and 9 - 12 year olds, including books, videos, educational apps and games. Amazon's free Parent Dashboard lets parents discover the content their children are enjoying and Discussion Cards help start conversations and connections with their children about those titles.

It is not the intention of this Strategy to direct or instruct parents to use certain tools, instead DCMS will work with and through trusted partners to raise the level of awareness around the most innovative products that are available. We will also seek to encourage wider consideration of different age-groups across digital products. This will fit alongside the work to raise parents' awareness of the safety features that exist already on social media platforms and work to help Britain develop a world class online safety industry.

On the Net Aware website, the NSPCC and O2 have produced a guide for parents about the social media that kids use. The site provides an explanation of how each social media company works and the safety features that they offer. We will consult with the NSPCC, O2 and other industry partners to develop our approach to promoting technology firms.

3. Digital skills

For parents to properly tackle online safety issues, it is crucial that they have the right digital skills to start the conversation with their children.

Technology companies' role

Not all parents may feel equipped to understand, support and deal with the challenges of their children's use of the Internet and connected devices. Ofcom research indicates that even parents who consider themselves digitally savvy can struggle with managing their children's screen time as they grow older.

The current industry-led self-regulatory approach on parental control filters works well, as it encourages parents to think about online safety, but applies filters where they are not engaged. Internet Service Providers (ISPs) are best placed to know what their customers want, and to deliver flexible parental control tools that keep up-to-date with rapid changes in technology. A mandatory approach to filters risks replacing current, user-friendly tools (filtering across a variety of categories of content, but built on a common set of core categories) with a more inflexible 'top down' regulatory system.

The control filters offered by the 'big four' ISPs (Sky, Virgin Media, TalkTalk and BT), cover the vast majority of UK subscribers. ISPs have transparent mechanisms in place for anonymous reporting of any 'over-blocking', and allow customers to 'white-list' sites.

Staying up to date on new apps and technology trends can prove challenging, and the more social media companies engage in educating and offering tools for parents, the better opportunities for parents to take responsibility for mediating their children's internet use.

The government will work with social media companies and organisations such as Internet Matters to ensure safety messages are built into online platforms, so that parents can stay up-to-date more easily. This work will form part of the UK Council for Internet Safety's initiative to streamline and signpost information that is available to parents and schools. Government will ensure that safety initiatives from elsewhere in the Strategy, including the code of practice and the outputs of work with app stores is publicised through these information channels.

The major technology companies have started to come together to tackle issues of online safety at an industry level. The creation of Internet Matters is a good example of this cooperation. Founded by BT, Sky, TalkTalk and Virgin Media in 2014, and joined by Google and the BBC in 2016, it is an online initiative to help parents keep their children safe online, addressing risks that include cyberbullying, sexting and online pornography. It is also supported by a number of organisations including Facebook, EE, and Dixons Carphone.

Over 2.0 million people visited www.internetmatters.org between April 2016 and March 2017 and the organisation reaches an average of 7 million people per month through social media channels.

4. Troubled families

The Department for Communities and Local Government's (DCLG) Troubled Families programme supports families who are facing multiple problems. For example, families may be in poor health, the children may not attend school regularly and the adults may be out of work. The programme is currently working with more than 185,000 families.

As part of the Troubled Families programme, key workers visit families to support them towards making sustained and significant progress to address their problems. DCMS will work with the government's Troubled Families programme's existing channels to ensure frontline professionals have access to best practice advice on online safety risks so they can support families in understanding online safety.

5. Looked after children, children in need and care leavers

Those children who are more vulnerable to harms in the real world are also more vulnerable online. We will ensure that particular action is taken to support these individuals.

We will also consider what more can be done to support foster carers, children's residential care workers and local authorities with responsibility for looked after children to support positive online interactions. This could include producing guidance/ materials on online safety for those responsible for children and young people in these groups.

8. Responding to online harms

While the work set out in this green paper will go some way in reducing the harm experienced online, and prevent harm escalating into more serious illegal activity online, we must also be prepared to respond when this does happen. Significant work is already happening across government to tackle harms online, including through implementing and enforcing existing legislation and working with industry and partners as part of crime-specific Strategies.

Legislation

Any behaviour or action that is illegal when committed offline is also illegal if committed online. Where behaviour does break the law, current legislation, some of which was passed before the digital age, has shown itself to be flexible and capable of catching and punishing offenders whether their crimes are committed by digital means or otherwise. For example, the Protection from Harassment Act 1997 includes the offences of stalking, harassment and of putting people in fear of violence, and applies to offences committed online, as well as offline.

In addition, the legislation that captures online abuse and harassment includes:

- Malicious Communications Act 1988
- Computer Misuse Act 1990
- Protection from Harassment Act 1997
- The Criminal Justice and Public Order Act 1994
- Section 15 Sexual Offences Act 2003 (for grooming)
- Breach of the Peace (common law offence)
- Communications Act 2003.

Police response to online hate crime

As part of this Strategy, the Home Office are creating a new national police online hate crime hub. The hub will act as a single point through which all reports of online hate crime are channeled. Specially trained officers will liaise with the victim and use their knowledge of online hate crime to collect relevant evidence that will be needed by the CPS to bring a prosecution. Evidence and any preliminary investigative work to identify the perpetrator will then be allocated to the relevant police force where the alleged offence took place to take forward the investigation. The hub will provide local forces with guidance or specialist knowledge. This will provide victims with a better service and will make it more likely that prosecutions can be brought.

The hub will improve the police response to online hate crime and improve the response to victims. It will:

- Assess whether the circumstances relate to a crime or non-crime incident;
- Combine duplicate reports;
- Seek to identify the perpetrator;
- Refer appropriate cases to internet hosts for action;
- Feed any intelligence into the National Intelligence Model;
- Produce an evidence package for local recording and response where there is a positive line of enquiry;
- Update the complainant with progress and explain where there is no enforcement action possible;
- Advise local police colleagues on effective responses.

The national hub will be established under the National Police Chiefs Council. It will begin operating by the end of the year. Initial funding for the hub is £200,000 a year. This will be found from the current Home Office hate crime budget.

Online dating and networking sites

The rise in popularity of applications and social media services that enable users to meet online has created new opportunities to make social connections, including those romantic or sexual in nature. Companies such as Tinder and Grindr offer services to UK users that enable location-based meet-ups. While some services are strictly oriented towards adults through their terms and conditions, these are not always enforced even where users identify themselves as young people in their profiles, or their communications with other users. We know that children can and do seek out information about sexuality online and use the Internet as a means to experiment and to initiate contact with others. However, sexual communication with a child under the age of sixteen is illegal, and there are serious risks to young people presented when they engage in this kind of behaviour and are then prompted to meet new contacts in person.

While it is right that we continue to work with police to prevent child sexual exploitation and to bring offenders to justice, there is a role for companies providing adult-oriented services, in particular those that monetise their users, to ensure that their user-base is over the age of consent and to prevent solicitation and contact between adults and children. There is also a role for users in identifying and flagging users to review teams and being encouraged to do so, in order to prevent children putting themselves at risk.

We would like to work with companies offering adult-oriented dating services to review processes and procedures, and to develop new protective messaging to help their user community prevent young people being put at unnecessary risk, and to ensure they remain in line with the law. We will consider whether there is a role for companies to provide appropriate messaging, and to take a stronger role in terminating accounts belonging to young people.

Prosecuting crimes committed online

The Crown Prosecution Service (CPS) plays an important role in providing legal guidance that sets out how prosecutors should make charging decisions and handle specific types of cases in court. In August 2017, following consultation with community groups and criminal justice partners, they produced revised statements and legal guidance, covering the different strands of hate crime: racist and religious; disability; and homophobic, biphobic and transphobic.[19] The CPS is continuing to work with communities to make reporting hate crimes as easy as possible.

Get Safe Online (www.getsafeonline.org) is an independent organisation, funded by industry and government, to ensure that high-quality advice is available to users. Often, even basic research, such as checking social media sites or using search facilities, can help check whether a person is actually who they say they are.

Government strategies

There are a number of existing strategies which seek to protect internet users from online harm and the Internet Safety Strategy will support these efforts.

[19] http://www.cps.gov.uk/victims_witnesses/hate_crime/index.html#a04/

These strategies include:

- The **Ending Violence Against Women and Girls (VAWG) Strategy**, published in March 2017, emphasises the importance of protecting people from these crimes online and offline, as well as addressing offending specifically facilitated by the Internet. The Strategy commits to working with law enforcement and online safety forums to ensure the risk posed by online VAWG is understood, and that all victims have the confidence to report these crimes. We are clear that civil orders, as well as legislation, apply equally online as offline, and we have committed to introduce new Stalking Protection Civil Orders, which will have the power to place restrictions on stalkers' online, as well as offline behaviours.

- The **Serious and Organised Crime Strategy** was published in 2013, to coincide with the launch of the National Crime Agency (NCA), a powerful new agency with the funding and clout to lead the fight against serious and organised crime, including cyber crime. The Strategy is built on the successful framework we use to counter terrorism, to Pursue, Prevent, Protect and Prepare. Strong partnerships are at the heart of the Strategy - we are working closely with our partners in government and law enforcement to turn the full force of the state against those behind the most serious crime, including cyber crime and online child sexual exploitation. Through the Serious and Organised Crime Strategy Review we will set out a strategic approach to reduce the risk to the UK from serious and organised crime, suited to the scale and nature of the evolving threat and building on progress made under the 2013 strategy. The new strategy will test the definition of serious and organised crime (SOC) and provide a framework to guide activity and investment by HMG and the wider public sector. It will support the development of an integrated and cohesive SOC community, setting out clear roles and responsibilities and governance arrangements to drive accountability and evaluation.

- We have boosted the capabilities of the **NCA's National Cyber Crime Unit** by increasing their ability to investigate the most serious cyber crime, and improved the response to online child sexual exploitation through the launch in 2015 of the Joint Operations Team, a collaborative venture between the NCA and GCHQ, to target the most sophisticated online offenders. The NCA has led and will continue to lead operations against dark net criminals. This includes joint operations with industry and international law enforcement partners across the globe to disrupt cyber criminals, attack their infrastructure and protect UK businesses and citizens. The WePROTECT Global Alliance, in which HMG has played a leading role, published their strategy in 2015 on eradicating online child sexual exploitation.

- The **National Cyber Security Strategy 2016:** The 2015 National Security Strategy reaffirmed cyber as a top tier one risk to UK interest – highlighting cyber threats as one of the key challenges to drive the UK security priorities for the coming decade. The National Cyber Security Strategy published in November 2016 defines our vision and ambition for the future: a UK that is secure and resilient to cyber threats: prosperous and confident in the digital world. It is supported by £1.9 billion of transformational funding to provide the UK with the next generation of cyber security. Our overall cyber crime strategic objective is to reduce the impact of cyber crime on the UK and its interests by deterring cyber criminals from targeting the UK and relentlessly pursuing those who persist in attacking us.

- **The Hate Crime Action Plan**, launched in July 2016, focuses on five key areas:
  1. Preventing hate crime by challenging beliefs and attitudes;
  2. Responding to hate crime within our communities;
  3. Increasing the reporting of hate crime;
  4. Improving support for victims of hate crime; and
  5. Building our understanding of hate crime.

We already have a strong legislative framework to tackle hate crime. The action plan includes new actions to ensure the legislation is used effectively to support victims and deal with perpetrators.

Under the hate crime action plan the government committed to funding community demonstration projects to tackle hate crime. We are pleased that so far nine community projects have benefitted from £300,000 for innovative schemes to help tackle hate crime across all five strands of hate crime (race, religion, sexual orientation, disability and transgender identity). The second year of the scheme was launched on the 31 July 2017.

The hate crime action plan also commits to providing funding for physical protective security measures to places of worship that have been or are vulnerable to hate crime attacks. The scheme is currently in its second year.

The Home Secretary has announced a further £1 million will be available this financial year to fund security measures in vulnerable places of worship. This is running separately to the current places of worship scheme, and was launched on the 30 June 2017.

Case Study – using technology to capture evidence of cyber harassment
A cyber harassment project known as Operation Capture, led by Bedfordshire Police and the National Centre for Cyberstalking Research, with funding through the Police Innovation Fund, has developed a new Cyberharassment Mobile Application (CybHAPP) and a technology-driven online risk assessment tool (DRASH) for officers investigating online harassment and stalking. The app will enable automated and instantaneous transfer of cyber evidence, ensuring the integrity of evidence to increase the likelihood of a successful prosecution, while reducing the burden on digital forensics, as well as the reliance on victims to secure their own evidence. The app also generates metrics that show the times or days when activity peaks – which can help victims gain a degree of control and could also help shed light on offender behaviour. The app will be trialled with victims of cyber stalking and harassment from early 2018.

Fraud and older people

While fewer older people use the Internet (37% of those 65+ have never used the Internet, compared to 0.4% of those 25–34), the proportion of older people in the population is rising, which will increase the exposure of those aged 65+ to online crime and harms. While older people are currently less likely to be victims of crime, they can face barriers in seeking support as victims, and can take longer to recover.

The Home Office is leading an Action Plan for Older People to strengthen our approach to protecting vulnerable older people from abuse, exploitation and crime.

The Action Plan has four main aims:

1. Improving awareness of abuse and exploitation so that early signs are challenged and identification and reporting of abuse increases;
2. Address root causes of social isolation and ‘informal’ (i.e. family member) carer burnout;
3. ‘Design out’ opportunities for people to financially abuse older people; and
4. Improve the criminal justice and victim care response to older people so that offenders are brought to justice and older people are better able to recover from abuse.

Work to address financial abuse of older people, including online, is primarily being delivered and driven through the Joint Fraud Taskforce, and voluntary participation by the banking sector, working closely with government, Trading Standards and victim support. This includes roll-out of new banking protocols to protect vulnerable victims from fraud in-branch, development of new minimum standards for banks dealing with victims of fraud, and piloting new initiatives, in conjunction with the Behavioural Insights Team, which will protect vulnerable people from financial abuse and fraud.

The second phase of the ‘Take Five’ communications campaign will re-launch in October 2017 as a new joint Home Office and UK Finance led campaign, jointly funded by the Office for Security and Counter-Terrorism and private sector partners in the UK financial sector. The campaign equips the public to more confidently challenge fraudulent approaches, including via email or online. Take Five’s partnerships activity will focus on the over 65s, leveraging the combined brand powers of HMG and UK Finance alongside influential public, private and third sector partners to deliver protective messages.

Annex A – Research and the current landscape

The majority of unpleasant behaviours online, like bullying, are not new and it is not digital technology itself that creates the problem. Rather, the Internet is the medium by which these behaviours are perpetrated and accelerated, providing significantly wider access to victims as well as new and innovative ways of attack. Children and adults can both be victims and the harms can be significant.

More than four in ten adults users say they have seen something that has upset or offended them on social media in the past 12 months.[20]

The nature of online posting means that bullying and trolling content has the potential to have a lasting impact on victims: it can be seen by a larger number of people and 24 hour access to the Internet means that it's an ever present threat. Online perpetrators are also getting savvier about their interactions with one another, leaving little evidence, or using anonymous apps or group chats to target individuals meaning that it is becoming increasingly difficult to take action against the perpetrators.

There is a growing body of evidence that suggests online harms can have detrimental effects on users and, in some cases, can have a long-term impact. This Strategy is grounded in the assumption that the risks that users encounter online do not inevitably translate into harm.

Studies that clearly demonstrate a causal relationship between online exposure and harm are scarce. For areas such as mental health impacts and cyberbullying which have "offline counterparts" more research has been conducted whereas the insights into relatively new phenomena such as hate content online and sexting are limited. In fact, evidence has suggested that 1-2 hours a day of digital screen time could have a positive effect on children and young people's wellbeing.[21]

Increasing time and presence online

Today, adults and children are spending more time than ever on the Internet.

Ofcom estimates that the average weekly time spent online for all adults in 2016 was 22.9 hours,[22] 1.3 hours more than 2013. 5-15 year olds spend 15 hours a week online; increasing their exposure to risks. Even 3-4 year olds who go online are spending 8 hours per week doing so.[23]

The ways in which individuals access the Internet is also changing. Adults are now less likely to go online via a computer (62% in 2016 vs. 71% in 2015) and they are proportionally more likely to use a smartphone than a computer to go online (66% in 2016 vs. 62% in 2015).[20] Also more children are increasingly using mobile devices such as tablets or smartphones to access the Internet which could lead to a lack of supervision and increased privacy. In addition, we know that there is a growing trend for even very young children to spend time online.

---

[20] Adults' media use and attitudes, Ofcom report (2017) https://www.ofcom.org.uk/__data/assets/pdf_file/0020/102755/adults-media-use-attitudes-2017.pdf
[21] A Large-Scale Test of the Goldilocks Hypothesis: Quantifying the Relations Between Digital-Screen Use and the Mental Well-Being of Adolescents, Andrew K. Przybylski and Netta Weinstein, Psychological Science, 2017, Vol. 28 (2) 204–215
[22] Adults' media use and attitudes, Ofcom (2017) https://www.ofcom.org.uk/__data/assets/pdf_file/0020/102755/adults-media-use-attitudes-2017.pdf
[23] Children and parents: media use and attitudes, Ofcom (2016) https://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf

Ofcom[24] has found that record numbers of older people are also embracing social media, with half of internet users aged 65-74 having a social media profile. However, older adults still spend less time online compared to younger users - those aged 16-24 spend 35.2 hours online per week, but those aged over 75 only spend 7.4 hours.

The Internet offers a space for creativity, innovation and support

It is important that we recognise the benefits that the Internet can bring to users of all ages in allowing them to be creative, share ideas and build relationships. Adults underline that they see social media as an important way of sharing information among friends, family or their local community and that social media also exposes them to different opinions and viewpoints.[25] In the recent years, there has been an increase in the number of people who say they are confident in being creative online.[25] A UK-study also found that training older people to use social media improves cognitive capacity, increases a sense of self-competence and could have a beneficial overall impact on mental health and physical wellbeing.[26]

In particular for today's children, technology has brought opportunities that previous generations never had and continuing innovation means that the benefits of being online continue to grow. The majority of evidence points to this positive impact, particularly the role that the Internet plays in teenagers' lives: in 2015, 99% of 13-18 year old respondents have seen people posting things online that are supportive, kind or positive, with 46% saying they see this all or most of the time.[27] The Internet also fosters self-expression, connects children to their peers and provides opportunities to respect and celebrate differences. The majority of teens report that they can be themselves online. However, this figure is lower for girls rather than boys (74% of girls and 82% of boys).[27]

> *"These [internet] companies give the chance to people around the world to socialize with each other and find out new things about multicultural things. Also this helps people discover new abilities or talents like making and editing videos for YouTube."*[28]

Increased Exposure to Risk

As the Internet becomes increasingly integral to all of our lives, it is important to understand how online activities may have negative consequences on wellbeing and safety.

Users say that the Internet allows them to be more critical rather than being more supportive of one another.[29] The research also shows that four-in-ten internet users are victims of online harassment with varying degrees of severity. Young adults and women were found to be more likely than any other groups to experience online harassment.

In the past year, almost one fifth of 12-15 year olds encountered something online that they 'found worrying or nasty in some way.'[30] Also half of UK adult internet users say they have concerns about what is on the Internet. These concerns relate mainly to offensive/ illegal content (38%), risks to

---

[24] Rise of the Social Seniors revealed, Ofcom (2017) https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/rise-social-seniors
[25] Adults' media use and attitudes, Ofcom (2017) https://www.ofcom.org.uk/__data/assets/pdf_file/0020/102755/adults-media-use-attitudes-2017.pdf
[26] Training elderly in social media improves well-being and combats isolation, University of Exeter (2014) http://www.exeter.ac.uk/news/featurednews/title_426286_en.html
[27] Creating a better internet for all: Young people's experiences of online empowerment + online hate, UK Safer Internet Centre (2016), http://childnetsic.s3.amazonaws.com/ufiles/SID2016/Creating%20a%20Better%20Internet%20for%20All.pdf
[28] Internet Safety Strategy, Perspectives from Young People, Childnet and UK Safer Internet Centre
[29] Online Harassment, Pew Research Center (2014) http://www.pewinternet.org/2014/10/22/online-harassment/
[30] Children and parents: media use and attitudes, Ofcom (2016) https://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf

others/ society (22%) and concerns about security/ fraud (20%). Other concerns include personal privacy (9%) and advertising (7%).[31]

Children are likely to be particularly vulnerable and thus have a higher risk of experiencing harm. When they are online, children can face bullying, abuse and content that promotes self-harm, suicide and eating disorders. These are not new problems, but as it has transformed our lives, the Internet has increased the ease and frequency with which people can be exposed to these harms.

Although most social media platforms have reporting features, it can take time to get content removed and unfamiliarity with the available safety features may prevent some from using the technology at all.

Upsetting content can vary but children mostly find this type of content on video-sharing sites or on social networking sites.[32] This is concerning as children are often left to navigate these platforms on their own.

In the case of children and young people, the online risks can be summarized in three different categories:[33] **Conduct** (vulnerable to interactive situations e.g. cyberbullying), **Contact** (participation in interactive situations e.g. sexting) and **Content** (exposure to mass-distributed or targeted content e.g. hate speech or pornography).

Table 1 - An overview of the classification for online risks

	Content Child as receiver (of mass production)	**Contact** Child as participant (adult-initiated activity)	**Conduct** Child as actor (perpetrator/ victim)
Aggressive	Violent/ gory content	Harassment, stalking	Bullying, hostile peer activity
Sexual	Pornographic content	'Grooming', sexual abuse on meeting strangers	Sexual harassment, 'sexting'
Values	Racist/ hateful content	Ideological persuasion	Potentially harmful user-generated content
Commercial	Advertising, embedded marketing	Personal data exploitation and misuse	Gambling, copyright infringement

Source: EU Kids Online (Livingstone, Haddon, Görzig, & Olafsson), 2010

Adults can be affected by these online risks too. Particular groups of adults may be more at risk than others. For example, Ofcom's recent report into adults' media use and attitudes found that internet users aged 16-24 are more likely to say they have been trolled online (5% vs. 1%).[34]

When risks result in harm

[31] Adults' media use and attitudes, Ofcom (2017)
https://www.ofcom.org.uk/__data/assets/pdf_file/0020/102755/adults-media-use-attitudes-2017.pdf
[32] Net Children Go Mobile - The UK Report. A comparative report with findings from the UK 2010 survey by EU Kids Online, Livingstone et al. (2014).
https://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/NCGMUKReportfinal.pdf
[33] Risks and safety on the internet: The UK report. Full findings from the EU Kids Online survey of UK 9-16 year olds and their parents, Livingstone et al. (2010 http://eprints.lse.ac.uk/33730/1/EU_Kids_Online_Report_April2014.pdf
[34] Adults' media use and attitudes, Ofcom (2017)
https://www.ofcom.org.uk/__data/assets/pdf_file/0020/102755/adults-media-use-attitudes-2017.pdf

It is not inevitable that risks result in harm, and there is no particular set of characteristics that make a user more vulnerable online; but, it is important to understand which risks can lead to the highest probability of harm for particular groups.

The emerging research in this field highlights both opportunities and risks that come with online activity. Conclusive evidence covering prevalence and the impact of online risk for both adults and children are scarce. This is mainly due to the difficulties in defining the exact nature of the risks in changing online environments. The evidence we have suggests there is potential for both positive and negative outcomes from interacting online. The below text highlights some areas of risk which have been frequently discussed. The themes covered are not an extensive list of all risks that users face online but should give an illustrative overview of the evidence and policy challenges.

Internet usage and young people's mental health

Internet use may exert both positive and negative effects on young people at risk of self-harm or suicide. We know from the experiences of people who have used the Internet to seek help and advice, and who have experienced suicidal ideation, that it can be a useful source of information, guidance and peer support.

It can also be a stressful environment where people may be exploited, experience bullying and harmful content and often their distress can go unnoticed.[35] Common themes of suicidal ideation emerge as cyberbullying, online abuse and emotional and behavioural difficulties.[36] Research funded through the Cross-Government Suicide Prevention Strategy showed that three quarters of 21 year olds surveyed who had attempted suicide reported some sort of suicide-related internet use.[37] However, many of these people had used the Internet to seek help.

Many studies have tried to explore the connection between excessive time spent online by children and a negative impact on their social and emotional development, as a predictor of higher risk of poor mental health. However, whether increased internet use has a causal effect is not clear.[38]

Internet forums may provide a support network for socially isolated young people but they could also be potentially harmful for vulnerable adolescents.

17% of 11-16s reported seeing self-harm material online in 2013 (only 6% in 2010)[39] and 4% said they had seen websites where people discuss ways of committing suicide in 2013.

The upcoming Children and Young People's Mental Health green paper, which will be published before the end of the year, will reference improving the evidence base relating to the impact of the Internet on mental health and considering the role that technology has in affecting children and young people's mental health.

Pornography affecting children online

---

[35] Digital Futures, Samaritans (2015) http://www.samaritans.org/digitalfutures
[36] Children's online activities, risks and safety - A literature review by the UKCCIS Evidence Group, Livingstone et al. (2017). https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis
[37] Priorities for suicide prevention: balancing the risks and opportunities of internet use, University of Bristol (2016). http://www.bristol.ac.uk/news/2016/november/suicide-internet.html
[38] Children's mental ill-health by time spent on social networking sites, UK, 2013 to 2014, ONS (2017). https://www.ons.gov.uk/peoplepopulationandcommunity/wellbeing/adhocs/006721childrensmentalillhealthbytimespentonsocialnetworkingsitesuk2013to2014
[39] Net Children Go Mobile - The UK Report. A comparative report with findings from the UK 2010 survey by EU Kids Online, Livingstone et al. (2014). https://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/NCGMUKReportfinal.pdf

Children and adolescents can access pornographic content (material designed primarily to cause sexual arousal and stimulation) intentionally and unintentionally and are doing so, particularly as they become older. A 2016 UK study conducted by Martellozzo et al. on behalf of the NSPCC and the Office of the Children's Commissioner for England found that at the age of 11, the majority of children had not seen online pornography, whereas sixty five per cent of 15-16 year olds reported having seen pornography.[40]

Evidence suggests that pornography is a great concern to children online[41] and appears to influence them in negative ways. Pornography use by children could be, for example, associated with more permissive and unrealistic sexual attitudes, stronger gender-stereotypical sexual beliefs and maladaptive attitudes about relationships.

A study in the UK and four other European countries found that of 4,564 young people aged 14-17, boys who regularly watched online pornography were significantly more likely to hold negative gender attitudes.[42]

In other areas research is less conclusive. Pornography use among adolescents may relate to more sexual aggression,[43] in terms of perpetration and victimisation.[44] However, the evidence in this area is conflicting with some studies finding no link at all between pornography and sexual aggression, and others finding that people with already above average levels of sexual aggression had levels of aggression approximately four times higher after watching porn regularly compared to counterparts who do not watch porn regularly. Therefore while there is evidence of harm, the exact nature and long-term effects are uncertain.

A survey showed that of those children that view pornographic material online just over half of boys (53%) believed that the pornography they had seen was realistic compared to 39% of girls. A number of girls said they were worried about how porn would make boys see girls and the possible impact on attitudes to sex and relationships.[45]

The Digital Economy Act 2017 has introduced requirements for online pornography provided on a commercial basis to be inaccessible to under-18s. Pornographic content will need to be placed behind robust age verification barriers to stop children from viewing sexualised content. We believe that every child has a right to develop at a time that suits them, and this legislation will help protect children from potentially harmful content on online porn sites. DCMS will be taking this work forward alongside the implementation of this Strategy, with the ambition that age verification is in place during 2018.

The age verification measures will create a regulatory framework that disrupts the business of sites that refuse to comply, backed by civil sanctions. The regulator will be able to: notify payment providers and other service providers that the websites they are doing business with are in breach of UK law; and, direct internet service providers to block non-compliant websites.

---

[40] 'I wasn't sure if it was normal to watch it' - A quantitative and qualitative examination of the impact of online pornography on the values, attitudes, beliefs and behaviours of children and young people,
Martellozzo, E., Monaghan, A., Adler, J.R., Davidson, J., Leyva, R. and Horvath. (2016).
https://www.nspcc.org.uk/globalassets/documents/research-reports/mdx-nspcc-occ-pornography-report.pdf

[41] In their own words: What bothers children online?. Sonia Livingstone, Lucyna Kirwil, Cristina Ponte and Elisabeth Staksrud, with the EU Kids Online network (2013).
http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/Intheirownwords020213.pdf

[42] Pornography, sexual coercion and abuse and sexting in young people's intimate relationships: A European study, Stanley, N et al. (2016). http://journals.sagepub.com/doi/10.1177/0886260516633204

[43] 'Sexual aggression' is defined here as a collective term that can refer to any sexual contact against a person's will.

[44] Basically ... porn is everywhere: a rapid evidence assessment on the effects that access and exposure to pornography has on children and young people., Horvath et al. (2013). http://eprints.mdx.ac.uk/10692/1/BasicallyporniseverywhereReport.pdf

[45] 'I wasn't sure if it was normal to watch it' - A quantitative and qualitative examination of the impact of online pornography on the values, attitudes, beliefs and behaviours of children and young people, Martellozzo et al. (2016). Report for: Childrens Commissioner and NSPCC https://www.nspcc.org.uk/globalassets/documents/research-reports/mdx-nspcc-occ-pornography-report.pdf

This is a major step forward for protecting children from harmful online material that should reduce the chance of young children stumbling across pornography online.[46] We know that a determined child will still seek ways to access pornographic content and that this requires more than a singular approach. Therefore this work sits alongside other initiatives such as parental filters and this Government will consider the issue of pornography in developing the regulations and guidance on Relationships and Sex Education, which the Children and Social Work Act (2017) requires us to make compulsory in all secondary schools in England.

Commercial content and advertising targeted at children and adults

Children are exposed to targeted advertising online through various products such as banners, sponsored Google search results or YouTube videos. Online gaming is very popular among children and also offers a big platform for online advertisers that target children, with most older children being aware of advertising that encourages them to 'pay-to-win'.

However, evidence suggests that children, in particular younger ones, lack a critical awareness when it comes to advertising online, but their understanding is increasing in the last few years.[47] A minority of 8-15s can identify sponsored links in search engine results.

55% of 12-15s who go online are aware of personalised advertising, in that they are aware that other people might see adverts online that are different to those they see, up from 45% in 2015.[47] More than half of internet users aged 12-15 (57%) are aware that the vloggers might be being paid by the company to say favourable things, this is a ten percentage point increase from 2015.[47]

Researchers such as Agnes Nairn and Juliet B. Schor[48] [49] have written about the risk that young children do not process profile targeting on a critical level. Young children are therefore often susceptible to advertisements as they are unable to discern the messages in them or, in the case of advergames, that they are a form of advertising at all.[50]

Ofcom's report on Adults' media use and attitudes report demonstrates that adult users may also not be aware of commercial content. While the majority of internet users stated that they were confident that they could recognise advertising online, only half of search engine users recognised adverts on Google. Internet users aged 55-64 (12%), 65-74 (15%) and 75+ (18%) are more likely than other age groups to say they are 'not confident' identifying advertising online. 28% of adults who use video-sharing sites don't realise that vloggers might be paid to endorse products and only 44% of adults are aware that the main source of funding for YouTube is advertising.[51]

Fake news and educating young people to distinguish between fact and fiction on the Internet

---

[46] 'I wasn't sure if it was normal to watch it' - A quantitative and qualitative examination of the impact of online pornography on the values, attitudes, beliefs and behaviours of children and young people, Martellozzo et al. (2016). Report for: Childrens Commissioner and NSPCC https://www.nspcc.org.uk/globalassets/documents/research-reports/mdx-nspcc-occ-pornography-report.pdf

[47] Children and parents: media use and attitudes, Ofcom (2016) - report 2016 https://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf

[48] "Consumer Kids". The influence of the commercial world on our children, Nairn, A (2009). *Education Review – journal of NUT*. Autumn, http://www.longwood.edu/staff/miskecjm/400marketingarticle.pdf

[49] Born to Buy: The Commercialized Child and the New Consumer Culture, Juliet Schor (2004).

[50] Children, Advertising and the Internet, LSE Media Policy Project Blog (2015). http://blogs.lse.ac.uk/mediapolicyproject/topic-guides/children-advertising-and-the-internet/

[51] Adults' media use and attitudes, Ofcom (2017) https://www.ofcom.org.uk/__data/assets/pdf_file/0020/102755/adults-media-use-attitudes-2017.pdf

It is important for children and young people to be aware that not everything they see and read online is real. Being able to distinguish between factual and fabricated content is a critical skill. In an age where children and young people predominantly get their news from social media outlets it is important that they are given the skills to critically evaluate the content they are consuming.

In a 2016 Ofcom survey,[52] more than one in four of the children surveyed (across the full age range surveyed, 8 - 15) agreed that "if Google lists information then the results can be trusted". Further qualitative research revealed that some children had a limited understanding of the source of search results, assuming an authoritative human fact checker was involved in their selection. UK adults' critical awareness was also shown to be lacking in a Channel 4 "fake news" survey in 2017.[53] The survey found that only 4% of respondents were able to identify all three true new stories in a selection of six they were presented with, and 49% of respondents thought at least one of the three fake news stories was true.

That is why we will be working with DfE to ensure that children's critical thinking skills are enhanced as part of increased digital literacy training so that young people are better able to recognise "fake news" and intentionally misleading information on the Internet.

Hate crime and the exposure to hate content for all internet users

In 2015/16, 15,442 hate crimes were prosecuted - the highest number ever.[54] This type of crime is increasingly conducted online and there are indications that individuals' exposure to hate content online has risen in recent years.

Hate crime occurs where an offence has been committed by reason of the victim's race, religion, disability, sexual orientation or transgender identity. Hate crime committed via social media can also involve harassment and stalking behaviour or the distribution of written or visual material. There are a number of legislative means to prosecute hate crime; racially or religiously aggravated offences (sections 28-32 of the Crime and Disorder Act 1998), offences stirring up hatred on the grounds of race, religion or sexual orientation (Parts 3 and 3A of the Public Order Act 1986) and enhanced sentencing (sections 145 and 146 Criminal Justice Act 2003). The appropriate legislative means to be used to prosecute cases would depend on the specifics of each case. Further details of existing legislation and regulations can be found in Annex B.

The Internet has enabled people to offend, insult or abuse individuals more generally, outside of a specific hate crime context (commonly referred to as 'trolling').

The Crown Prosecution Service has revised its guidelines on social media to incorporate new and emerging crimes being committed online. Advice was added to the guidelines about the use of false online profiles and websites with false and damaging information. The revised guidelines include sections on:

- Hate Crime;
- Violence against Women and Girls, including potential cyber enabled VAWG offences, such as "baiting", humiliating peers online by labelling them sexually promiscuous;
- False or offensive social media profiles;
- Vulnerable and intimidated witnesses;
- Reporting and preventing abuse on social media.

There is no conclusive evidence on the rate of exposure for adults to hate content online and the harm caused. Further research into the prevalence of hate content and its impact on individuals would address these evidence gaps.

---

[52] Children and parents: media use and attitudes, Ofcom (2016) https://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf
[53] Channel 4, http://www.channel4.com/info/press/news/c4-study-reveals-only-4-surveyed-can-identify-true-or-fake-news (2017)
[54] Hate Crime Report, CPS (2016) http://www.cps.gov.uk/publications/docs/cps_hate_crime_report_2016.pdf

More is known about children's exposure to hate content online and research shows that the number of children affected seems to be rising. A survey in 2013 showed that 23% of 11-16s had seen hate messages online[55] whereas in 2010 only 12% of 11-16 years olds reported that they have been exposed to hate content. A more recent survey showed that 64% of children and young people aged 13-17 have seen people posting images or videos that are offensive to a particular targeted group.[56]

In 2016 one in three 12-15s who go online (34%) say they have seen hate speech online in the last 12 months.[57]

Further research must be conducted to better understand the impacts of online abuse, the motivations behind such behaviour and how we can best challenge it.

Cyberbullying amongst children and the adults' experiences of trolling

Evidence indicates that cyberbullying is becoming an increasingly common phenomenon for young people and it is different to 'offline' bullying in that it happens mostly outside of schools.[58] Cyberbullying can be a 24/7 issue that can lead to the victim feeling under surveillance.

Reporting to social media companies is low amongst those who recognise they have been cyberbullied. Children, particularly those who had no direct experience of reporting issues, had little confidence in social media companies to resolve cyberbullying. But, satisfaction amongst those who have reported is much higher. This disparity between perceptions and actual experience of reporting indicates there is more social media companies could do to raise awareness and improve clarity of reporting mechanisms. This might help improve perceptions and the likelihood of young people reporting issues in the future.[59]

The Childline bullying report 2015-16 highlights that bullying is one of the most common reasons why children contact Childline, accounting for 9% of all counselling sessions (25,740 sessions in 2015/16). A total of 4,541 counselling sessions were delivered about cyberbullying in 2015/16, an increase of 13% from the previous year.

Research shows that young people do not always recognise cyberbullying. Around two-thirds of those who had experienced something negative online did not define their experiences as cyberbullying meaning it might be an even bigger problem than current evidence suggests.[59]

Cyberbullying can also pose a threat to adolescents' health and wellbeing.[60] As with more traditional forms of bullying, it can cause psychological, emotional and physical distress. Research into the impacts of cyberbullying suggests the prevalence of depression, loss of confidence, isolation, relationship problems, self-harming and suicide amongst victims.[61] [62]

---

[55] Net Children Go Mobile - The UK Report. A comparative report with findings from the UK 2010 survey by EU Kids Online, Livingstone et al. (2014).
[56] Power of image: A report into the influence of images and videos in young people's digital lives, UK Safer Internet Centre (2017). www.saferinternet.org.uk/safer-internet-day/2017/power-of-image-report
[57] Children and parents: media use and attitudes, Ofcom (2016) https://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf
[58] Bullying: Evidence from the Longitudinal Study of Young People in England 2, wave 2, DfE (2015). https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/570241/Bullying_evidence_from_the_longitudinal_study_of_young_people_in_England_2__wave_2_brief.pdf
[59] Cyberbullying: Research into the industry guidelines and attitudes of 12-15 year olds. Family Kids & Youth. (2017). Report for The Royal Foundation of the Duke and Duchess of Cambridge and Prince Harry.
[60] Children's online activities, risks and safety - A literature review by the UKCCIS Evidence Group, Livingstone et al. (2017). https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis
[61] Current perspectives: the impact of cyberbullying on adolescent health, Nixon, C. L. (2014). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4126576/

In September 2016, DfE announced £1.6 million of funding over two years, for four anti-bullying organisations to support schools tackle bullying, including cyberbullying. Internet Matters led a project to support reporting of cyberbullying to schools. There are a range of online platforms which can support schools. One example is Tootoot, an online tool which can be used by young people, parents and carers to report bullying incidents to schools, and include evidence such as pictures or screenshots from social media.

Adults also often experience cyberbullying which can take different forms such as harassment or trolling. The word 'trolling' alludes to the method of catching fish by casting a baited line in the water and waiting for a fish to bite. Similarly, a troll online tries to catch an unsuspecting victim to demean and humiliate. Not much large-scale research has been done on the prevalence of trolling and its impact on victims but anecdotal evidence paints the picture of the many people that face abuse online in the UK each year. The new research being undertaken by a remodeled UKCCIS will consider this and build our understanding of this issue, informing our future approach to the problem.

There is much anecdotal evidence that online abuse and hate crime can silence the voices of women, BAME, faith, disabled and LGB&T communities, who feel that they have to remove themselves from certain platforms and discussions in order to stay safe.

Media coverage shows that this is a particular issue for female public figures, activists and campaigners who are targeted specifically for giving their opinions. Those who do not conform to stereotypical norms or what is deemed as acceptable in their appearance are also frequently targeted. Changing Faces[63] is a charity that campaigns on behalf of people with a disfigurement who can disproportionately suffer abuse online.

The Microsoft Digital Civility Challenge
Microsoft is challenging people around the world to embrace "digital civility" and to treat each other with respect and dignity online.

In an attempt to put empathy more front and centre in digital dialogues, Microsoft have created a Digital Civility Index and Digital Civility Challenge. The challenge calls on people to commit daily to four ideals and to share their pledge on social media, using the hashtags #Challenge4Civility and #Im4DigitalCivility. Specifically, they are encouraging people to:

- 'Live the Golden Rule' by acting with empathy, compassion and kindness in every interaction, and treating everyone they connect with online with dignity and respect.
- Respect differences and honour diverse perspectives, and when disagreements surface to engage thoughtfully, and avoid name-calling and personal attacks.
- Pause before replying to things people disagree with, and not posting or sending anything that could hurt someone else, damage reputations or threaten people's safety.
- Stand up for themselves and others by supporting those who are targets of online abuse or cruelty, reporting activity that threatens anyone's safety, and preserving evidence of inappropriate or unsafe behaviour.

Online misogyny

Online misogyny can range from distasteful comments or jokes, to grossly offensive or targeted bullying, to death and rape threats. This abusive behaviour can also form part of a wider pattern of stalking or abuse, with victims being pursued both on and offline.

---

[62] Hate Crime and Bullying in the Age of Social Media, Williams & Pearson (2016). https://orca-mwe.cf.ac.uk/88865/1/Cyber-Hate-and-Bullying-Post-Conference-Report_English_pdf.pdf
[63] https://www.changingfaces.org.uk/about-us

While online abuse is aimed at both men and women, the nature of abuse can be acutely gendered. Online abuse of women and girls more often targets their specific gender identity, and commonly includes threats of rape and violence. Abuse and threats in these cases are often couched in stereotypes and misogynistic terms, whereby abusers consider their actions justified if women and girls act outside of prescribed gender roles. This can leave women and girls feeling vulnerable and isolated, and undermines their contributions in the online world.

Being the victim of online abuse can be a frightening and humiliating experience for its targets. But for every direct victim, there are a greater number of people who are indirectly affected – those who see the abuse, and fear that if they speak up, they may be next. Online misogyny normalises the silencing of women and the use of rape threats to close down dissent: it is particularly visible in trolling campaigns against women of achievement. There have been a number of cases of MPs and journalists removing themselves from social media having received threats and abuse when they speak openly about equality and women's rights. The cumulative impact of online misogyny undermines women's and girls' digital contributions, silencing their voices and reducing their visibility: half of the girls and young women surveyed by Girl Guides think that sexism is worse online than offline with many saying fear of abuse makes them feel less free to share their views.[64]

The nature of the online world allows perpetrators to remain anonymous, at a distance, and often act with impunity. Abusive partners and ex-partners can now use a range of online behaviours and tools in addition to the more "traditional" forms of domestic and intimate partner abuse. This includes monitoring or checking their partner's phone and internet use, financial abuse by blocking access to accounts, as well as stalking and using location trackers on mobile and tablet devices to monitor someone's movements. Domestic abuse, sexual violence and stalking and harassment are all addressed through the Violence Against Women and Girls Strategy, and while outside the scope of this green paper, government departments are working closely together and with partners to understand and address the interactions between violence against women and girls and harmful activity online that falls short of a criminal offence.

In 2016, the Government Equalities Office established a cross-government officials group on online misogyny, in partnership with the Home Office, to map out current action and to understand opportunities for action across government.

Women's Aid and Facebook's guide to help women stay safe online
Women's Aid, a leading national domestic abuse charity, and Facebook have worked together to launch a new guide to empower women to stay safe online.

The guide by Women's Aid and Facebook provides advice to help women and girls understand the risks and tools needed to protect themselves and stay safe on social media. The guide has a lot of helpful tips – from how to report something that is abusive, to stopping an intimate, private or sexual image from being shared online. It aims to help women take greater control of their own safety on Facebook, whilst staying connected to the people and causes they care about.

The guide is specifically designed to provide information and advice to survivors of domestic abuse. Whilst the online world should be open and safe for everyone to use, many women experience domestic abuse online. Though many survivors are already experts at managing their own risk and safety, Women's Aid and Facebook have brought together some specific steps they can take to protect themselves online.[65]

Sexting amongst young people

[64] Girls Attitudes Survey, Girl Guides (2016) https://www.girlguiding.org.uk/globalassets/docs-and-resources/research-and-campaigns/girls-attitudes-survey-2016.pdf
[65] https://www.womensaid.org.uk/keeping-women-safe-online/

Definitions of sexting vary greatly and there is little detailed research on its prevalence and effect either on adults or on teenagers. Sexting can include the sending of sexually suggestive images via mobile phones or over the Internet, though younger people also perceive sexting as sharing explicit text messages.

Research suggests that many children and young people who engage in the behaviour do so in the context of consensual romantic relationships.

A study examining the behaviour in the context of the romantic relationships of 724 children and young people aged 14-17[66] found that 38% of the sample had sent sexual images to a partner during or after their relationship, and 49% had received them. The proportion of the sample sending and receiving sexts increased with age (26% aged 14 compared with 48% aged 16). Girls were more likely to send sexts than boys (44% compared with 32% respectively), but they were equally likely to receive them.[73]

The sample commonly reported motivations are to flirt and in response to partner requests in relationships and many children and young people report that this is a positive experience.[67]

There is evidence that some girls and boys experience pressure and coercion to engage in this behaviour within their relationships.[73] Key concerns about sexting relate to non-consensual forwarding to peers or images being posted online, and the associated social and emotional consequences[68] [69], including distress, humiliation and reputational damage, as well as online and offline peer harassment and unwanted sexual advances.[70] Where children send sexual images of an under-18, even where this is self-generated, this is a criminal offence, for children and adults.

The government wants all young people to develop healthy, respectful relationships. GEO and the Home Office jointly funded £3.85 million to launch the second phase of the *This is Abuse* campaign, called 'Disrespect NoBody,' in February 2016. The campaign encourages young people to rethink their understanding of abuse within relationships, which includes issues like sexting.

Advice on sexting
The UKCCIS Education Group have produced advice for schools and colleges on responding to incidents of 'sexting.' The advice aims to support them in tackling the range of issues which these incidents present including responding to disclosures, handling devices and imagery, risk assessing situations and involving other agencies.

The advice also contains information about preventative education, working with parents and reporting imagery to providers. This advice is non-statutory and should be read alongside the Department for Education's Keeping Children Safe in Education statutory guidance and non-statutory Searching, Screening and Confiscation advice for schools.

In tandem with this, the National Police Chiefs Council produced guidance dealing with sexting that seeks to enable law enforcement professionals to respond in a proportionate way to reports of under 18's possessing, sharing or generating indecent imagery of themselves or other children.

---

[66] Images across Europe: The sending and receiving of sexual images and associations with interpersonal violence in young people's relationships. Wood, M et al. (2015). *Children & Youth Services Review*, 59, 149-60. doi:10.1016/j.childyouth.2015.11.005
[67] Children's online activities, risks and safety - A literature review by the UKCCIS Evidence Group, Livingstone et al. (2017). https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis
[68] A qualitative study of children, young people and 'sexting', Ringrose, J et al. (2012). *London: NSPCC*. http://eprints.lse.ac.uk/44216/
[69] The association between adolescent sexting, psychosocial difficulties, and risk behavior: Integrative review, Van Ouytsel, J et al.(2015). *The Journal of School Nursing*, 31(1), 54-69. doi:10.1177/1059840514541964.
[70] Children's online activities, risks and safety - A literature review by the UKCCIS Evidence Group, Livingstone et al. (2017). https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Revenge pornography

Adults can also experience issues with sexting and the sharing of explicit images, and in 2015 'revenge porn' was made a specific criminal offence. A helpline dedicated to supporting victims of revenge porn was given additional government funding in April 2017. Since its launch the helpline has taken over 6,000 calls. 75% of those seeking advice and support are female.[71]

So-called revenge porn is the sharing of private sexual photographs or film without consent and with the intent of causing distress to the person depicted. Explicit or compromising images are posted online, sometimes on fake social media accounts, or shared with family and friends via mobile devices to embarrass and shame the victim; or otherwise the threat to do so is used with as much power.

Analysis conducted by the BBC found that there were 1,160 reported incidents of revenge pornography from April 2015 to December 2015 in England and Wales. 30% of those offences involving young people under 19 and Facebook was used by perpetrators in 68% of cases where social media was mentioned in reports, followed by Instagram (12%) and Snapchat (5%).[72]

Evidence suggests that the majority of cases involve a female victim, with the original image(s) posted by someone known to them but then shared by multiple other internet users either intentionally to add to a stranger's distress or unknowingly, thinking that the images are pornography. Some images are shared without the victim knowing they existed to begin with.

The *End Revenge Porn* campaign found that out of the victims they interviewed:

- 90% of victims were women
- 93% of victims said they suffered "significant emotional distress"
- 82% claimed "significant impairment in social, occupational, or other important areas of functioning" due to being a victim
- 51% had suicidal thoughts due to being a victim
- 42% sought psychological services.[73]

There is anecdotal evidence that while legitimate pornographic websites quickly remove content considered to be abusive, and those hosted within the UK are bound by UK law to remove them, there are a number of websites that have grown a reputation for, or even exist with the sole purpose of, posting images of revenge pornography knowing it is distressing to the victims. These same sites sometimes publicly posting refusals to remove material when requested.

Adults and children providing personal information online

There is much evidence to suggest that many individuals do not feel in control of personal data they disclose online and that they are concerned about privacy and data protection when participating in the digital economy.[74] 'Privacy' is often cited as important, and sometimes as the most important factor, for individuals engaging in online activities.[75]

---

[71] https://www.gov.uk/government/news/revenge-porn-helpline-given-further-funding
[72] Revenge pornography victims as young as 11, investigation finds, BBC's own analysis (2016), http://www.bbc.co.uk/news/uk-england-36054273
[73] Research from Cyber Civil Rights Initiative. https://cyberbullying.org/revenge-porn-research-laws-help-victims
[74] Research and analysis to quantify the benefits arising from personal data rights under the GDPR - Report for DCMS, London Economics (2017). https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/635701/PersonalDataRights_LE_-_for_Data_Protection_Bill__1_.pdf
[75] Digital Footprints: A question of trust, Communications Consumer Panel (2016). http://www.communicationsconsumerpanel.org.uk/downloads/communications_consumer_panel_digital_footprints-cover_report.pdf

The Communications Consumer Panel's 2016 research found that most people understand that personal information is collected, stored, and used by public and private sector organisations. However, fewer are aware of how such technologies work or how their personal data is used.

Consideration of data or privacy concerns vary amongst adults. Ofcom's report suggests that almost nine in ten (89%) internet users describe themselves as confident online, but one in four internet users (24%) don't use reliable checks before entering their personal details online and one-third (33%) of internet users who buy things online don't check that the site looks secure.[76] This can leave users open to fraud and cyber crime.

Children's digital literacy increases fairly steadily from age eight to young adulthood. While children come to understand the digital environment better with age and experience, it is by no means clear that a critical understanding of the digital environment results in cautious behaviour regarding personal data protection. Indeed, the data show how uneven children's digital literacy is.[77] For instance, while more than three quarters of 12 to 15-year-olds are cautious about their privacy and data sharing when visiting new websites, the majority (58%) believe information online can be easily removed if they no longer wish to share it with other people.[78]

Government is committed to updating and strengthening data protection laws through a new Data Protection Bill, introduced into Parliament in autumn 2017. It aims to provide everyone with the confidence that their data will be managed securely and safely. Under the plans, individuals will have more control over their data by having the right to be forgotten and to ask for their personal data to be erased.

Catfishing

Catfishing is when an individual (or individuals) use the Internet to create a false identity or identities to form a romantic relationship, but without committing a criminal offence. While individuals have always been able to enter romantic relationships using deception, the Internet has provided a new mechanism for doing so, through creating entirely false identities and conducting relationships entirely online. Catfish may form close relationships with individuals, some lasting many years, without revealing their true identity.

Where a deceptive online relationship is used for financial gain, this is a criminal offence, and is outside the scope of this Strategy. Tackling fraud is the responsibility of the Home Office and law enforcement agencies, and is being addressed separately through the Joint Fraud Taskforce as well as the Serious Organised Crime and National Cyber Security Strategies.

More than half of online dating users say they have come across a fake profile and the number of people defrauded in the UK by online dating reached a record high in 2016 (Which 2016).

[76] Adults' media use and attitudes, Ofcom (2017).
https://www.ofcom.org.uk/__data/assets/pdf_file/0020/102755/adults-media-use-attitudes-2017.pdf
[77] Digital literacy can be understood as the ability of individuals to use skills, knowledge and understanding in order to make full use of the opportunities offered by the new media environment as well as safeguard themselves from associated risks (see Digital Media Literacies: rethinking media education in the age of the Internet, Buckingham (2007)).
http://te831us.wiki.educ.msu.edu/file/view/Buckingham.DigitalLiteracy.pdf)
[78] Children's online activities, risks and safety - A literature review by the UKCCIS Evidence Group, Livingstone et al. (2017).
https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Annex B – Existing legislation and regulation

As set out in our principles, we believe that behaviours online should mirror those in the offline world. We are clear that there is already legislation and regulation in place which means that we can take action when inappropriate behaviours occur.

The current law in England and Wales includes a number of criminal offences and rights to civil actions which may be relevant in cases of misuse of the Internet or social media. Material published on the Internet, or by mobile phone, etc, is subject to the same restrictions as material published elsewhere: in other words, what is illegal offline is illegal online.

Self-regulation also allows a broad range of interested parties to participate and can be an effective way of coming up with innovative and effective solutions to issues which, due to the nature of the Internet, are often global. However, government is prepared, where necessary and effective, to take legislative action in order to deliver our objectives as is the case on age verification legislation for access to sites containing pornographic content.

Criminal offences online

The government is absolutely clear that abusive and threatening behaviour online is totally unacceptable. An action which is illegal offline is also illegal online. The law does not differentiate between criminal offences committed on social media or anywhere else – it is the action that is illegal.

A number of criminal offences may be committed by those abusing others on social media, including offences under the Protection from Harassment Act 1997; the Malicious Communications Act 1988; and the Communications Act 2003.

Section 1 of the Malicious Communications Act 1988 makes it an offence to send material to another person which conveys an indecent or grossly offensive message, a threat or information which is false and known or believed to be false by the sender. The offence can also be committed by sending an article or electronic communication which is, in whole or part, of an indecent or grossly offensive nature. In order to be guilty of the offence the sender's purpose (or one of them) in sending the item must be to cause distress or anxiety to the recipient or to any other person to whom the sender intends that the item or its contents or nature should be communicated.

Changes to the law in the Criminal Justice and Courts Act 2015 increased the maximum penalty for the offence in section 1 of the Malicious Communications Act 1988 to two years imprisonment, and removed the requirement that prosecutions should be brought within six months of the offence being committed.

The Protection from Harassment Act 1997 creates an offence of harassment (section 2) e.g. it is an offence for a person to pursue a course of conduct which amounts to harassment of another and which he knows or ought to know amounts to harassment of the other. Online harassment is not separately criminalised but may be considered as part of the general criminal offence of harassment. The Act also creates an offence of stalking (section 2A). Harassment is generally understood to involve improper, oppressive and unreasonable conduct that is targeted at an individual and calculated to alarm them or cause them distress. The conduct might be verbal or non-verbal and it does not have to be the same type of action on each occasion. Critically the individual elements of a course of conduct need not in themselves be criminal. However when a series of events are seen in combination, they may form a course of conduct which could amount to a criminal offence. A 'course of conduct' in relation to a single person must involve conduct on at least two occasions.

Section 127(1) of the Communications Act 2003 creates a specific offence of sending (or causing to be sent) grossly offensive, indecent, obscene or menacing messages over a public electronic communications network. Section 127(2) creates a separate offence of causing annoyance, inconvenience or needless anxiety to another either by sending or causing to be sent, by means of a public electronic communications network, a false message or by persistently using the network. Amendments were made to the Act by the Criminal Justice and Courts Act 2015 which extended the time within which prosecutions under section 127 of the Communications Act 2003 may be brought, to up to three years from commission of the offence, as long as this was also within six months of the prosecutor having knowledge of sufficient evidence to justify proceedings.

Public protection and investigating whether an offence has taken place are matters for the police. Where an individual is concerned they are at risk of an offence being committed against them or they believe an offence may have been committed, they should always contact the police. It is then for the police to investigate any reports that an offence has taken place and for the police or the Crown Prosecution Service to decide whether to prosecute, depending on the circumstances of the case.

The Crown Prosecution Service has published guidelines on prosecuting cases involving communications sent via social media: http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/.

The government is committed to preventing these crimes and to giving all online users the protection and support they need. Our laws in this area are rightly robust, strict and respected across the world and it is vital that victims of crime see strong and certain justice delivered to their offender.

Equalities

The Equality Act 2010 legally protects people from discrimination in the workplace and in wider society.

Discrimination law is based on protection for people against discrimination because of particular characteristics (described as “protected characteristics”). These are, in the Equality Act: age, disability, gender reassignment, pregnancy and maternity, marriage and civil partnership, race, religion or belief, sex and sexual orientation.

A strong evidence base has built up over time that people with these protected characteristics have faced serious discrimination affecting their employment prospects and access to goods and services, like housing, health services and education, leading to disadvantage for themselves and their dependents.

Common framework for media standards

The government set out its concerns relating to consumer confidence and safety in accessing audiovisual content in the 2013 paper ‘Connectivity, Content and Consumers’. The paper is available online at: https://www.gov.uk/government/publications/connectivity-content-and-consumers-britains-digital-platform-for-growth

Industry and regulators worked together on a voluntary basis to ensure a common framework for media standards. This framework aims to support a more consistent approach across different media and ensure consumers understand what content has been regulated.

Ofcom has been leading the work to develop the framework, focusing on linear broadcast and on demand television as well as ‘TV-like’ content in the Internet television space where that is currently regulated by Ofcom.

Statutory guidance for schools

Keeping Children Safe in Education (KCSIE) is the statutory guidance to which all schools and colleges must have regard, when carrying out their duties to safeguard and promote the welfare of children. Working Together to Safeguard Children is statutory guidance for all schools that sets out inter-agency working to safeguard and promote the welfare of children. The guidance is available online: https://www.gov.uk/government/publications/working-together-to-safeguard-children--2

Age verification for access to sites containing pornographic content

Part 3 of the Digital Economy Act 2017 requires a person making available pornographic material on the Internet to persons in the UK on a commercial basis to do so in a way that ensures that the material is not normally accessible by persons under the age of 18. It also allows the regulator to act against those providing extreme pornographic material, regardless of whether age verification is in place. It provides powers for the age-verification regulator to notify payment providers and ancillary service providers of non-compliant persons, and to direct internet service providers to block access to non-compliant sites. Government intends to commence the requirement in 2018.

The Digital Economy Act 2017 also amended the definition of 'specially restricted material' in section 368E (5) of the 2003 Communications Act, which provides that On Demand Programme Service must not contain any 'specially restricted material' unless the material is made available in a manner which secures that persons under the age of 18 will not normally see or hear it. The definition now includes pornographic video works which have received an 18 certificate ("18 sex works") or other pornographic material which would receive an 18 certificate had it been submitted for classification.

Keeping pace with technology changes

As and when new technology has outstripped legislative capacity, we have taken steps to address the gaps identified and we will continue to do so.

For example, S65 of the Coroners and Justice Act 2009 was introduced to provide a definition of images to include data capable of conversion into moving or still images. Further, S69 of the Criminal Justice and Immigration Act 2008 amended the Protection of Children Act 1978 to extend the definition of 'photograph' to include derivatives of photographs, such as other forms of data. These derivatives include computer traced images, for example, computer traced images of photographs taken on a mobile phone or images manipulated from photographs using computer software.

HM Government