House of Commons

Science and Technology Committee

Impact of social media and screen-use on young people's health: Government Response to the Committee's Fourteenth Report

Twelfth Special Report of Session 2017–19

Ordered by the House of Commons
to be printed 21 May 2019

HC 2120
Published on 23 May 2019
by authority of the House of Commons

Science and Technology Committee

The Science and Technology Committee is appointed by the House of Commons to examine the expenditure, administration and policy of the Government Office for Science and associated public bodies.

Current membership

Norman Lamb MP (*Liberal Democrat, North Norfolk*) (Chair)

Vicky Ford MP (*Conservative, Chelmsford*)

Bill Grant MP (*Conservative, Ayr, Carrick and Cumnock*)

Mr Sam Gyimah MP (*Conservative, East Surrey)*

Darren Jones MP (*Labour, Bristol North West*)

Liz Kendall MP (*Labour, Leicester West*)

Stephen Metcalfe MP (*Conservative, South Basildon and East Thurrock*)

Carol Monaghan MP (*Scottish National Party, Glasgow North West*)

Damien Moore MP (*Conservative, Southport*)

Graham Stringer MP (*Labour, Blackley and Broughton*)

Martin Whitfield MP (*Labour, East Lothian*)

Powers

The Committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No. 152. These are available on the internet via www.parliament.uk.

Publication

Committee reports are published on the Committee's website at www.parliament.uk/science and in print by Order of the House.

Evidence relating to this report is published on the inquiry publications page of the Committee's website.

Committee staff

The current staff of the Committee are: Danielle Nash (Clerk), Zoë Grünewald (Second Clerk), Dr Harry Beeson (Committee Specialist), Jocelyn Hickey (Committee Specialist), Sonia Draper (Senior Committee Assistant), Julie Storey (Committee Assistant), and Joe Williams (Media Officer).

Contacts

All correspondence should be addressed to the Clerk of the Science and Technology Committee, House of Commons, London SW1A 0AA. The telephone number for general inquiries is: 020 7219 2793; the Committee's e-mail address is: scitechcom@parliament.uk.

You can follow the Committee on Twitter using @CommonsSTC.

Twelfth Special Report

On 31 January 2019 the Committee published its Fourteenth Report of Session 2017–19, *Impact of social media and screen-use on young people's health* [HC 822]. On 10 May 2019 we received the Government's Response to the Report, which is appended below.

Appendix: Government Response

Introduction

The government is grateful for the Committee's very helpful report following its inquiry into the impact of social media and screen-use on young people's health. We recognise that while social media and technology can bring about huge benefits for young people, we need to tackle the harms that arise. The government is already undertaking work to address a wide range of online harms, including those which have particular impact on the mental health of children and young people.

In May last year, the government response to the Internet Safety Strategy Green Paper announced our intention to publish a White Paper in Winter 2018/2019 as a precursor to bringing forward online safety legislation. The joint Department for Digital, Culture, Media and Sport (DCMS) - Home Office Online Harms White Paper, published on 8 April, sets out our plans for world leading legislation to make the UK the safest place in the world to be online. This will make companies more responsible for their users' safety online, especially children and other vulnerable groups.

Although we have had some success working with companies at a voluntary level, government has been clear that more needs to be done to address harms occurring across a growing range of platforms. The White Paper sets out ambitious proposals, including establishing a new duty of care on companies towards their users that will be overseen by an independent regulator - in line with the recommendations of the Committee.

This regulator will set clear safety standards, backed up by mandatory reporting requirements and effective enforcement powers. Companies will be held to account for tackling a comprehensive set of online harms. These range from illegal activity and content, to behaviours that may not be illegal but are nonetheless highly damaging to individuals and society.

The future regulator will have a suite of powers to take effective enforcement action against offending organisations - ranging from issuing fines, improvement notices, information demands and potentially the ability, in the most extreme cases, to block offending websites, hold their senior management to account or disrupt their business activity. As part of the public consultation on the White Paper measures, we are seeking views on these enforcement options.

DCMS and the Home Office continue to work closely with the Department of Health and Social Care (DHSC) to identify possible specific policy options to take forward in relation to young people's mental health and social media. In particular, we continue to build the evidence base to assess what preventative interventions may be necessary and justified. The Committee's report makes a very useful contribution to this issue.

The Government's response to the recommendations in the Committee's report are set out below.

Research on social media and screen-use

Recommendation 1

In order to develop a more valid and reliable understanding of the relationship between the use of social media by young people, and its effects on their health, the information asymmetry between tech companies, the Government, other public bodies and *bona fide* researchers must be addressed swiftly. (Paragraph 29)

Government response

The Department of Health and Social Care (DHSC) will convene a research seminar to identify the avenues for undertaking and funding future research on the relationship between social media and young people's health. DHSC and the Economic and Social Research Council (ESRC) are in discussion about taking this forward.

On 29 April, at the recent social media summit chaired by the Secretary of State for Health and Social Care, key social media companies came together and agreed to establish a world leading strategic partnership with suicide and self-harm prevention experts, led by the Samaritans to take a sector-wide approach to better understand the boundaries around harmful suicide and self-harm related content found online.

Transparency is a crucial element of the regulatory model outlined in the Online Harms White Paper, as it will ensure the regulator has appropriate oversight and can take action where necessary. The regulator will have the power to require annual transparency reports from companies in scope, outlining the prevalence of harmful content on their platforms and what counter measures they are taking to address these. This could include mechanisms companies have in place to protect users around their health and wellbeing. These reports will be published online by the regulator, so that users and parents can make informed decisions about online use.

The regulator will encourage and oversee the fulfilment of companies' commitments to improve the ability of independent researchers to access their data, subject to appropriate safeguards. These measures will help address the current information asymmetry between tech companies, the government and researchers.

Recommendation 2

Regardless of whether Ofcom's remit is eventually expanded to cover social media platforms, its existing obligation to collect data on the 'media literacy' of both adults and children (as set out in the Communications Act 2003) should be strengthened through establishing statutory information-gathering powers. Such powers should require social media companies with registered UK users to provide the regulator with the high-level data it needs to fulfil its duties with respect to media literacy, with legislation introduced in the next Session. (Paragraph 30)

Government response

Ofcom already have a responsibility to promote and carry out research on media literacy under the Communications Act 2003. In January 2019, Ofcom published their latest annual report on media use and understanding among children and young people, which includes research on young people's use of social media and screen time. Their research looked at the negative pressures to look popular on social media, as well as young people's exposure to online bullying on platforms, and safety issues around profile privacy settings. Ofcom is also taking steps to expand and deepen their research base to aid further research work on media literacy. Ofcom will also undertake other areas of bespoke research around how children and adults navigate online news, the use of children's data online, and their understanding of advertising online. Ofcom is also looking to establish new partnerships within the research community, with other stakeholders across the industry and overseas to aid this work.

There is already a lot of excellent work being done in this area by other stakeholders. For example, the National Literacy Trust has set up NewsWise - a free, cross-curricular news literacy project for 9 to 11-year-olds across the UK that provides teachers with a suite of curriculum-based lesson plans, online resources, school workshops and opportunities to speak to real journalists. This initiative is currently funded by Google, and has been developed in partnership with the Guardian Foundation and the PSHE Association. The BBC also launched a new programme in 2018 to support young people identify real news content. As part of this, all schools have been given access to free online materials, including the iReporter game.

However, efforts have so far been uncoordinated. Ofcom has already committed to carrying out a media literacy mapping exercise of current UK initiatives to help establish where the overlaps are and where there are gaps and opportunities for collaboration.

The Cairncross Review, which was published recently (12 February), has recommended that government develops a media literacy strategy, working with Ofcom, online platforms, publishers and broadcasters, as well as voluntary organisations and academics. The government is currently considering this recommendation and will respond on this in due course.

As outlined in the Online Harms White Paper, the government will also go further in developing a specific online media literacy strategy. We will be consulting widely on this, possibly through a new taskforce, in order to ensure the strategy's objectives are well informed by evidence and take account of existing work. This will include convening tech companies, regulators, libraries, academics and civil society organisations and others to support us in coordinating effective work in this area.

In addition to this, the new independent online harms regulator will have oversight of industry activity and spend in relation to education and awareness activities.

Recommendation 3

While respecting data protection principles, social media companies should make anonymised high-level data available, for research purposes, to bona fide researchers

so that a better understanding of social media's effects on users can be established. The government should consider what legislation needs to be in place to improve access by researchers to this type of data. (Paragraph 31)

Government response

As set out in our response to the first recommendation, the government is already considering what legislation and regulation is needed to support better access to UK level data on online harms. Independent research has played a key role in both preventing and tackling harms and will continue to do so.

Several of the largest companies have promised access for independent researchers to anonymised information, in line with data protection requirements. The government welcomes these steps, and believes that this level of transparency to researchers is a necessary part of developing an increased understanding of online harms. The new online harms regulator will help support this approach, and will ensure companies make relevant information available and follow through on their existing commitments. As part of this, we also expect companies to support the developing evidence base around screen time, for example by providing access to anonymised data to researchers as recommended by the CMO.

Transparency will be a critical element of the new regulatory framework. To inform its reports and to guide its regulatory action, the regulator will have the power to require information from companies, including in the form of transparency reports. This information will cover a number of areas including the prevalence of harms and counter measures which companies are taking to address these.

Recommendation 4

We commend the government for its efforts to think more closely about online harms and how best to address them, particularly when those harms have serious, detrimental effects on the lives of young people. While the government has undertaken a wide-ranging consultation process through the publication of its Internet Safety Strategy Green Paper, it is disappointing that it has not sought to address the current limitations of the evidence base by actively commissioning new research. As the government Response to its Green Paper acknowledges, the evidence on the impact of social media on mental health "is not yet conclusive". That the field requires more robust research should not come as a surprise when the Chief Medical Officer described the evidence base, in 2013, as "sparse and contradictory". (Paragraph 38)

Government response

DCMS recognises the need for further research and evidence gathering on online harms: their prevalence, who is being affected and what impact, if any, they are having in the long term. To date DCMS has worked with others including the UK Council for Internet Safety (UKCIS) and Ofcom to build a picture of what is being experienced by internet users through regular reviews of the literature and the media lives surveys[1]&.[2] This is a complex landscape and with the development of online platforms such as social media

[1] https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/childrens-media-lives

[2] https://www.ofcom.org.uk/research-and-data/media-literacy-research/adults/media-lives

being relatively recent, there is little robust longitudinal evidence to show a causal link between their use and long term impacts from harm experienced. We also recognise there is a need to understand what works in reducing the prevalence of harm occurring through improving user behaviours, and measures which reduce the number of users experiencing harm.

DCMS develops plans for commissioning research based on the evidence gaps, the priorities for policy making and the resources available. We have recently commissioned a number of research projects to:

- build an understanding of online platforms and their current capabilities in mitigating the risk of harm to users;
- observe how parents of 10–13 year olds are helping their children stay safe online through ethnographic research; and
- review the literature on adult experiences of harm online.

This research will be published shortly. We are currently developing plans for future research, including what can be commissioned by the department and where we can work with others to expand and enhance the evidence base. The future online harms regulator will work closely with UKRI to ensure support for targeted research into online harms, and to develop the collective understanding of online harms and the evidence base, building on the work of the UKCIS Evidence Group. This will include working with relevant aspects of UKRI's Digital Economy Theme – a partnership between the Engineering and Physical Sciences Research Council (EPSRC), the Arts and Humanities Research Council (AHRC), the Economic and Social Research Council (ESRC) and Innovate UK.

Recommendation 5

To ensure that policy is evidence-based, and that the research needs of Government departments are met, departmental 'Areas of Research Interest' documents must be accompanied by periodic funding calls. Such calls need to take place ahead of an area becoming the subject of a major policy initiative. (Paragraph 39)

Government response

DCMS has strengthened its relationship with the UK Research and Innovation (UKRI) through the appointment of a Chief Scientific Advisor. DCMS has also worked closely with the UKRI to shape strategic research funding initiatives in a manner consistent with the Haldane principle (which dictates that 'decisions on individual research proposals are best taken by researchers themselves through peer review'[3]). DCMS's commissioning of research is also consistent with the recommendations of the Nurse Review, which looked at how the UK can most effectively support research and called for scientists and the government to work closer together and for the creation of a unified body. We are continuing to plan an ongoing research programme on online harms in line with these principles and best practice.

[3] https://publications.parliament.uk/pa/cm201012/cmhansrd/cm101220/wmstext/101220m0001.htm

Recommendation 6

The existing Areas of Research Interest documents produced by the Department of Digital, Culture, Media and Sport and by the Department of Health and Social Care, should be expanded to include how to measure and monitor the harms related to social media use. As a matter of urgency, DCMS should also commission research focused on identifying who is at risk of experiencing harm online, and why, and what the long-term consequences of that exposure are on the young person. (Paragraph 40)

Government response

DCMS is developing plans for future research, for which experiences of harm online and the consequences are a priority. Further information on recently commissioned research is provided in response to recommendation 4. DCMS and DHSC Areas of Research Interest documents are reviewed regularly and recommendations will be considered when the next update is processed.

Risks, harms and benefits of social media and screens

Recommendation 7

The report of the Independent Advisory Group on Non-ionising Radiation on the 'Health effects from Radiofrequency Electromagnetic Fields' is now nearly seven years old. In its Response to our Report, we ask the Government to outline what assessment it has made of the quantity and quality of the research on this topic, published since 2012, and to explain whether another evidence review is now warranted. (Paragraph 64)

Government response

Public Health England (PHE) continues to monitor the emerging evidence on this topic, including newly published studies and comprehensive evidence reviews from independent expert groups around the world. PHE considers the balance of evidence has not changed materially since the Advisory Group on Non-ionising Radiation (AGNIR) reached its conclusions and it is not necessary for the UK to initiate another comprehensive evidence review at this time.

Among the recent comprehensive evidence reviews is a 2015 review prepared for the European Commission by the Scientific Committee on Emerging and Newly Identified Health Risks (SCENIHR), which reached conclusions broadly in line with those of AGNIR. SCENIHR publications can be found through the following webpage and electromagnetic field (EMF) Opinions are under the 'Physical Risks' category: http://ec.europa.eu/health/scientific_committees/emerging/index_en.htm

The World Health Organization (WHO) is presently preparing an Environmental Health Criteria (EHC) monograph covering the evidence in relation to radiofrequency exposures and health. Information from WHO about EMF exposure guidelines can be found at: http://www.who.int/peh-emf/standards/en/

Recommendation 8

We welcome Dame Sally Davies' work in this important area and look forward to reading the results of her review, and subsequent guidance, in due course. We note that many parents find it extremely challenging to moderate social media usage, especially where older children are involved. It would be helpful if this was recognised by those giving guidance to parents. (Paragraph 71)

Government response

The UK Chief Medical Officer (CMO) concluded that the published scientific research is currently insufficient to support evidence-based guidelines on screen time, but there is enough basis to warrant a precautionary approach. The CMO noted that some research has found associations between screen-based activities and negative effects such as increased risk of anxiety or depression. The CMO has now published a report, giving advice on how to have a healthy balance with screen time.[4] This is based on evidence around the importance of key activities important for healthy child development such as sleep, exercise and education. The government supports this advice, which is included in the Online Harms White Paper, and encourages children and parents alike to consider the CMO's messages whilst spending time on screens and online.

Recommendation 9

Great strides have recently been made to address and remove content that incites terrorist activities. The same effort and determination must now be applied to curb the proliferation online of the physical, emotional and sexual abuse and exploitation of children, as a matter of urgency. The Home Secretary stated that he expects a more effective partnership between technology companies, law enforcement agencies, the charity sector and the Government to protect children from sexual abuse and exploitation online. Simply 'expecting' more, however, is an insufficient approach to tackle the grievous nature of the problem. It is worrying that we still do not have a good understanding of the scale of online child sexual exploitation. (Paragraph 108)

Government response

Online child sexual exploitation and abuse (CSEA) is an appalling crime that this government is committed to stamping out.

The National Crime Agency estimates that 80,000 individuals in the UK present a sexual threat to children – and the figure could be significantly higher. As set out in the Serious and Organised Crime Strategy 2018 our aim is to leave no safe space for serious and organised criminals to operate against us within the UK and overseas, online and offline.

The Home Secretary made clear in his speech at the NSPCC on 3 September that he was not asking the technology industry for change, he was demanding it. The Home Secretary outlined five key areas of action for industry:

[4] UK CMO (2019). Commentary on 'Screen-based activities and children and young people's mental health and psychosocial wellbeing'. Available at: https://www.gov.uk/government/publications/uk-cmo-commentary-on-screen-time-and-social-media-map-of-reviews

(1) Block child sexual abuse material as soon as companies detect it being uploaded.

(2) Stop child grooming taking place on their platforms.

(3) Work with us to shut down live-streamed child abuse.

(4) Be more forward-learning in helping law enforcement agencies deal with these types of crimes.

(5) Display a greater deal of openness and transparency, and a willingness to share best practice and technology between companies.

The Home Secretary convened a Hackathon with Microsoft and WeProtect Global Alliance in November 2018. The event was hosted by Microsoft which brought together engineers and legal and operation experts from Microsoft, Google, Facebook, Snap and Twitter to develop a tool to tackle online grooming. The Hackathon successfully created a working prototype to automatically flag suspect conversations for review by experienced human moderators. Work continues to develop the prototype. Once complete, the tool will be rolled out for free to other tech companies that want to deploy it.

Since the Hackathon, the Home Office have been engaging with technology companies, including Facebook and Snap, and discussing how to fulfil the Home Secretary's priority asks of the technology industry, as outlined in his speech on 3 September.

Under the duty of care proposed in the White Paper we will expect companies to take particularly robust action in relation to the most serious online offending, such as CSEA.

Reflecting the threat to the physical safety of children, the government will have the power to direct the new regulator in relation to codes of practice relating to CSEA, in addition to terrorist activity, and these codes must be signed off by the Home Secretary. We continue to encourage companies to take early action to address online CSEA ahead of implementation of the new regulatory framework and interim codes of practice will be published later this year by the Home Office providing guidance about tackling terrorist activity and online CSEA.

Recommendation 10

The Government must proactively lead the way in ensuring that an effective partnership is in place across civil society, technology companies, law enforcement, and non-governmental organisations aimed at ending child sexual exploitation (CSE) and abuse online. The Home Office should use its research budget to commission a large-scale study that establishes the scale and prevalence of CSE which should then be updated annually. Once this has been published, we recommend that the Government set itself an ambitious target to halve reported online CSE in two years and all but eliminate it in four years. That ambition should be matched with the necessary resources, raised by the digital services tax, to make it a reality and should occur in addition to—and not instead of—establishing a legal 'duty of care' by social media companies towards its users who are under 18. Where companies are not voluntarily working with the Government and law enforcement agencies to prevent CSE, the Government should consider whether legal action is necessary. (Paragraph 109)

Government response

ONS data on childhood abuse shows that 28% of those who experienced sexual abuse as a child experienced sexual abuse as an adult (nine times higher than for adults who did not experience sexual abuse in childhood).

The UK government has nearly doubled the number of officers in the National Crime Agency dedicated to tackling online child sexual exploitation and each month coordinated activity by the NCA and policing against online CSEA is resulting in the arrest of over 400 offenders, and the safeguarding of around 500 children.

As outlined in response to the previous recommendation, the duty of care set out in the White Paper will increase the responsibility of online services in relation to CSEA content and activity. Compliance with the duty of care will be overseen and enforced by an independent regulator, which will have a suite of powers to take effective enforcement action against offending organisations - ranging from issuing fines, improvement notices and potentially the ability, in the most extreme cases, to block offending websites, hold their senior management to account or disrupt their business activity. As set out in the response to recommendation 9, companies will be required to take particularly robust action to tackle terrorist content and online CSEA.

Furthermore, the UK recognises that child sexual exploitation and abuse is a global crime that demands a global response. The government plays a leading role in the WePROTECT Global Alliance (WPGA), a global movement bringing together the influence, expertise and resources required to transform how online child sexual exploitation (CSE) is dealt with worldwide. Its multi-stakeholder nature is unique in this field, with 85 countries, 20 global technology companies, 25 leading Non-Governmental Organisations and eight regional organisations signed up to the initiative.

With regard to the Digital Services Tax, the Treasury have recently consulted on their proposed approach. The government recognises the vital importance of ensuring that the new online harms regulator is sufficiently resourced. Our intention is for the new regulator to be cost neutral to the public sector and we are considering fees, charges or a levy on companies whose services are in scope. This could fund the full range of the regulator's activity, including setting and enforcing codes of practice, preparing transparency reports, and any education and awareness activities by the regulator.

Recommendation 11

Our inquiry has illuminated the broad spectrum of benefits, risks and harms that children and young people may encounter via social media and screen-use. While social media and screen-use is not necessarily creating these risks, it has, in numerous cases, amplified them. Initiatives are in place to address some of these harms—notably around cyberbullying—yet others are falling through the cracks. A comprehensive, joined-up approach to address the plethora of negative effects is needed. (Paragraph 131)

Government response

The Online Harms White Paper establishes a coherent and Government-wide approach to a range of online harms which affect all users online, through both legislative and non-legislative initiatives.

The White Paper sets out proposals, consistent with the Committee's recommendations, for a new regulatory framework. This will feature an overarching statutory duty of care to make clear the responsibility that companies have towards their users in taking proportionate steps to protect them, and additional robust requirements to tackle the most serious and clearly defined illegal harms online, such as terrorism and child sexual abuse and exploitation.

We also recognise that the government needs to lead the way in ensuring that an effective partnership is in place, across civil society, technology companies, law enforcement agencies, and government and non-governmental organisations. The government response to the Internet Safety Strategy Green Paper in May 2018 made clear that industry's voluntary approaches to addressing online harms had not gone far or fast enough. We are, therefore, proposing stronger intervention to ensure that all companies take proper steps to keep their users safe.

Our White Paper sets out a wide range of harms which will fall within the scope of the new regulatory framework, including those which are illegal as well as those which are harmful but not necessarily illegal. It explores the use of technology to improve user safety; makes proposals to support users in increasing their digital resilience; and outlines what direct action government can take to address online harms.

Such a comprehensive approach to tackling a range of harms online is a world first, and it will ensure a joined-up approach keeping UK citizens, and particularly young and vulnerable users, safe online.

Recommendation 12

Underpinning the Government's forthcoming White Paper, and subsequent legislation, should be the principle that children must, as far as practicably possible, be protected from harm when accessing and using social media sites. All the physical and mental health harms we have outlined in this chapter—including cyberbullying, grooming, child abuse and child sexual exploitation (CSE), 'self-generated' images and 'sexting', the live streaming of CSE, violence, hate speech and pornography—should be covered. (Paragraph 132)

Government response

The White Paper sets out a programme of action to tackle harmful material online across an extensive range of harms – including focusing on harms that specifically impact children. These include: illegal activity such as CSEA, harassment and cyberstalking, sexting of indecent images of under 18s; alongside legal but harmful activity which includes cyber-bullying and trolling; coercive behaviour; advocacy of self harm and promotion of female genital mutilation (FGM). The White Paper also examines underage exposure to harmful online content like legal pornography and age-restricted social media activity and engagement.

The proposed regulatory framework, and in particular the duty of care, will require companies to take necessary and proportionate steps in protecting all users, but particularly children, from these types of harm.

As well as setting out our new regulatory approach, the White Paper sets out proposals for ways in which the regulator and government can encourage innovation and adoption of new safety technologies and support safety education and awareness for all users. These actions will also contribute to systematically tackling potential harms to children online.

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

Organisations that offer online services need to obtain parental consent to the processing of personal data for children who are under the age of 13. By law they must also make reasonable efforts to verify that the person providing consent holds parental responsibility for the child. Organisations which fail to comply with this obligation may be subject to enforcement action by the ICO. There are a number of tools available for the ICO to ensure compliance with data protection legislation. These include powers for non-criminal enforcement, audit, and criminal prosecution. The ICO also has the power to serve a monetary penalty notice on a data controller.

The Information Commissioner is working to produce a code of practice on age-appropriate design, as required by the Data Protection Act 2018. The Age-Appropriate Design Code will provide guidance on the privacy standards that organisations should adopt where they are offering online services and apps that children are likely to access and which will process their data. Work on developing the code is well advanced with calls for evidence and commissioned research already concluded. A formal public consultation was launched on 15 April 2019 which will run until 31 May 2019.

Resources for schools and parents

Recommendation 13

As children spend an increasing proportion of their life online, there is a pressing need for the education system to catch up and ensure that young people are equipped with the skills that they need to navigate, and critically assess, what they are seeing on social media and beyond. The Children and Social Work Act 2017 presents the government with a vital opportunity to establish digital literacy and resilience as integral parts of the curriculum for primary and secondary school students, through making 'Personal, Social, Health and Economic' (PSHE) education mandatory. This chance must not be wasted. (Paragraph 148)

Recommendation 14

We recommend that 'Personal, Social, Health and Economic' (PSHE) education be made mandatory for primary and secondary school children in the next parliamentary session and that the PSHE curriculum delivers an age-appropriate understanding of, and resilience towards, the harms and benefits of the digital world. (Paragraph 149)

Recommendation 15

The Department for Education should commission research early in 2019 to evaluate existing resources on online safety and digital resilience. This should be undertaken with a view to creating guidance on, and signposting teachers towards, high-quality information and teaching resources that can be used with primary and secondary school-age children. (Paragraph 150)

Government response

We want to support all young people to be happy, healthy and safe in all contexts, including online. We want to equip them for adult life and to make a positive contribution to society. To do this, we are making Relationships Education compulsory for all primary pupils, Relationships and Sex Education (RSE) compulsory for all secondary pupils and Health Education compulsory for all pupils in primary and secondary state-funded schools.

The Children and Social Work Act 2017 placed a duty on the Secretary of State for Education to make Relationships Education mandatory for all pupils receiving primary education and RSE mandatory for all pupils receiving secondary education. It also gave the Secretary of State the power to make PSHE mandatory, although doing so would be subject to careful consideration.

The Department for Education conducted a public call for evidence,[5] which ran from 19 December 2017 to 12 February 2018 and received over 23,000 responses, and worked with around 90 stakeholder organisations. Following this engagement, the Secretary of State made the decision to make only the health element of PSHE mandatory. This decision was made as there is a clear case for ensuring all pupils learn about health concepts, the personal and social aspects of PSHE will be covered by the introduction of Relationships Education and RSE and the economic aspects are already covered by the maths and citizenship curricula. Through our extensive consultation activity ahead of the introduction of the new subjects, we have heard a clear message that the role of the internet in young people's lives, whilst often positive, can also be harmful. It is clear that we need to help pupils to understand how to keep themselves safe online.

The outcome of the public call for evidence informed the draft regulations, the subject content in the statutory guidance, and the regulatory impact assessment, on which the department consulted between 19 July 2018 and 7 November 2018. The Department was contacted by over 40,000 individuals and organisations. These included parents, young people, headteachers, teachers, governors, subject specialists, teaching unions, charities

[5] Department for Education (2017). Call for evidence on the changes to Sex and Relationship Education and PSHE. Available at: https://www.gov.uk/government/consultations/changes-to-teaching-of-sex-and-relationship-education-and-pshe

and faith groups. The Department analysed the responses to the consultation and have since published the government response, laid the regulations in Parliament and updated the draft statutory guidance.

The draft statutory guidance for the new subjects specifies the subject content pupils must be taught in an age appropriate way. Pupils will be taught about online relationships, the implications of sharing private or personal data (including images) online, harmful content and contact, cyberbullying and where to get help and support for issues that occur online. The Health Education content includes extensive internet safety and harms content, including managing time spent online, how to be a savvy consumer of online information, age restrictions, trolling, bullying and how online information is targeted. Pupils will also be taught, at age appropriate points, about specific issues online, such as who and what to trust, sharing information, and about sexually explicit content and the impact it can have. In Health Education, pupils will also be taught about how to be safe and healthy, and how to manage their academic, personal and social lives in a positive way.

Pupils are also taught online safety through the computing curriculum, which covers the principles of e-safety at all key stages, with progression in the content to reflect the different and escalating risks that young people face. This includes how to use technology safely, responsibly, respectfully and securely, protecting their online identity, and where to go for help and support when they have concerns about content, contact, or conduct online.

Our recently-launched National Centre for Computing Education will develop an easily navigable repository of free, quality-assured resources. This will be aligned to the content of the national computing curriculum at key stages 1–4, and include the elements of online safety outlined above.

The department is committed to supporting schools to deliver high quality teaching of Relationships Education, RSE and Health Education. That is why we have announced that we have a budget of £6m in the 2019–20 financial year to develop a programme of support for schools. Further funding beyond the next financial year is a matter of the forthcoming Spending Review. We will provide a supplementary guide, targeted support on materials, and training; and are encouraging as many schools to start teaching the subjects from September 2019. We will share best practice from these early adopter schools with schools teaching the subjects from September 2020. We also intend to produce supporting information for schools on how to teach about all aspects of internet safety, not just those relating to relationships, sex and health, to help schools deliver this in a coordinated and coherent way across their curriculum.

Recommendation 16

Parental engagement can play a vital role in helping children develop 'digital resilience', so that they can confidently identify and judge online risks themselves. Parents, however, need high-quality support to ensure these conversations are as effective as possible. (Paragraph 155)

Government response

The government agrees that parental engagement plays a vital role in ensuring that children and young people develop digital skills and resilience ensuring that they are able to confidently navigate their lives online. The Internet Safety Strategy Green Paper consultation response survey highlighted that of the 222 parents that participated in the online survey 32% were keen to receive more information on data protection, 31% mental health impacts, 28% cyberbullying, 27% deception/fraud, 27% critical thinking, 23% physical impacts of being online and 23% digital resilience.

We will continue to ensure that online safety education is available to all children, as well as considering how we can continue to support parents in tackling internet harms. We are working with the UK Council for Internet Safety, who have previously developed a framework that helps to equip children and young people for digital life and a practical guide for parents to help their children understand what the risks of social media are.

As stated in the Online Harms White Paper, we are committed to continuing to support parents in preventing and dealing with online harms. We recognise that there is currently insufficient resource for adults which covers online media literacy and that there is a need for further work to address issues such as disinformation.

As outlined in our response to recommendation 2, the government has committed in the White Paper to develop an online media literacy strategy. Alongside this, whilst we recognise that companies fund a range of valuable education and awareness activity, we believe there needs to be greater transparency about the level of investment, that all activity needs to be evaluated to ensure resources are directed at the most impactful initiatives, and that there should be greater coordination across industry to avoid duplication. The new regulator will have the power to require companies to report on their education and awareness raising activity.

The government also recognises the need for improved coordination of activity. Ofcom are working with a number of partners to assess existing research and evidence about people’s attitudes and understanding of being online. This will assist policy-makers to identify gaps and opportunities.

Recommendation 17

I***n addition to identifying the gaps in the ‘online safety information available to parents’, the Government should commission the UK Council for Child Internet Safety to produce a toolkit in 2019 for parents and caregivers. The toolkit should enable them to have an effective, open and ongoing dialogue with their children about how to recognise, manage and mitigate online risks in relation to social media. This work should complement the proposed review of existing teaching resources recommended in paragraph 150***. (Paragraph 156)

Government response

It is critically important to ensure that parents and carers are media literate, and have the right support in place to have a meaningful dialogue with their children on online risks. Organisations such as BBC, Internet Matters, Childnet and Parent Zone, already produce high-quality materials to support parents and carers. In addition the UK Council for Internet Safety has published a practical guide to online safety for parents and carers.[6] Much of this material is signposted to schools in England via the statutory guidance, Keeping Children Safe in Education, so they in turn can highlight and signpost to parents and carers.

A priority delivery area for the reformed UKCIS over the next year is producing a digital resilience framework and toolkit to help families, educators, policymakers, frontline service workers and the industry better support users online, across a wide range of harms.

Recommendation 18

We have heard how children bringing smartphones into schools can be both a help and a hindrance to learning. While it is right that each school should have the freedom to decide its own policy on the use of mobile phones on its premises, it is essential that schools are supported to make that choice with evidence-based guidance. (Paragraph 164)

Recommendation 19

We recommend that the Government's 'What Works Centre for Education' evaluates the different approaches to handling smartphone use in schools so as to provide a basis for making evidence-based guidance available to both primary and secondary schools. This evaluation should be produced by the end of 2019. (Paragraph 165)

Government response

We recognise that the use of smartphones in schools can be regarded as both a help and hindrance to a child's education. Whilst the Department for Education (DfE) has recommended that it should be for schools to decide on their policy on the use of mobile phones, as per a report carried out for the Department by Tom Bennett 'Creating a Culture: How school leaders can optimise behaviour' (2017), we agree that further advice may be helpful for schools when making this decision.

The recommended timescale would not allow the Education Endowment Foundation (EEF) to carry out an in depth evaluation of different approaches to handling smartphone use, as it rules out any potential for evaluating attainment. However, the Department has asked the EEF to include further advice for schools on whole-school behaviour policies (including policies related to technology and smartphone use) in forthcoming guidance for schools on behaviour policies and management, which will be published in 2019.

DfE recognises the need to explore this subject further. To that end we aim to carry out an initial review of the evidence in this space. Regulation and guidance.

Recommendation 20

In February 2018, the Prime Minister described social media as one of the "defining technologies of our age". Like many age-defining technologies, it has brought a raft of benefits to its users, together with a host of unintended consequences; a number of

[6] https://www.gov.uk/government/publications/child-safety-online-a-practical-guide-for-parents-and-carers

which have been particularly detrimental—and in some instances, dangerous—to the wellbeing of children. Currently, there is a patchwork of regulation and legislation in place, resulting in a "standards lottery" that does little to ensure that children are as safe as possible when they go online, as they are offline. A plethora of public and private initiatives, from digital literacy training to technology 'solutions', have attempted to plug the gaps. While the majority of these are to be welcomed, they can only go so far. A comprehensive regulatory framework is urgently needed: one that clearly sets out the responsibilities of social media companies towards their users, alongside a regime for upholding those responsibilities. The Government's forthcoming Online Harms White Paper, and subsequent legislation, presents a crucial opportunity to put a world-leading regulatory framework in place. Given the international nature of social media platforms the Government should ideally work with those in other jurisdictions to develop an international approach. We are concerned, however, based on the Government Response to its Internet Safety Strategy Green Paper, that it may not be as coherent, and joined-up, as it needs to be. We recommend a package of measures in this Report to form the basis of a comprehensive regulatory framework. (Paragraph 226)

Government response

The government recognises that there has been, up until now, a fragmented regulatory landscape for online safety. We produced the original Internet Safety Strategy Green Paper as a first step towards developing a coordinated, strategic approach to online safety. We agree with the need to establish a responsibility for tech companies to keep UK citizens safe online. The White Paper proposes establishing a new statutory duty of care under which companies will be expected to deal with both illegal and harmful but 'legal' content and activity on their platforms. This will increase the responsibility of social media platforms to take action to prevent, and/or remove, harmful or illegal content from their sites.

The White Paper also proposes that a new independent regulator with statutory powers to oversee this new regulatory framework is established. We are currently consulting on whether it should be an existing or a new body. The White Paper also seeks to establish what enforcement powers that regulator will need. It will be necessary for any regulator to have sufficient enforcement powers, against both domestic and international organisations, for when there are systematic breaches of the duty of care. We have, therefore, proposed a range of core enforcement measures, including the ability to issue fines, and are consulting on a range of other powers to use in the most serious of circumstances - such as the ability to block sites, disrupt companies' business activities or hold senior management liable. We are also consulting on the information-gathering powers that will be needed to support better access to data including on complaints handling and redress.

The White Paper looks to tackle a comprehensive range of harms. An indicative list of harms in scope is included in the White Paper, based on an assessment of their impact on individuals and society and their prevalence. However, the list is neither exhaustive nor a fixed static list as we expect this will evolve to ensure swift regulatory action in addressing new forms of online harm, new technologies and online activities.

The new regulatory framework will apply to all companies that allow users to share or discover content or interact with each other online. This will also ensure legislation remains fit for purpose and future proofed, as the nature and form of tech companies changes over time.

Given the international nature of social media platforms it is vital that the regulator takes an international approach. Where similar regulators and legal systems are in place in other countries, the regulator will lead engagement with its international counterparts. Having these relationships will support the UK's ability to put pressure on companies whose primary base is overseas.

The government is working closely with international partners as we develop our own approach that reflects our shared values and commitment to a free, open and secure Internet. The approach proposed in this White Paper is the first attempt globally to tackle this range of online harms in a coherent, single regulatory framework. We will continue to share experiences and seek to build an international coalition.

The government believes this action delivers the comprehensive regulatory framework called for by the Committee.

Recommendation 21

To ensure that the boundaries of the law are clear, and that illegal content can be identified and removed, the Government must act on the Law Commission's findings on Abusive and Offensive Online Communication. The Government should now ask the Law Commission to produce clear recommendations on how to reform existing laws dealing with communication offences so that there is precision and clarity regarding what constitutes illegal online content and behaviour. The scope for enforcing existing laws against those who are posting illegal content must be strengthened to enable appropriate punishment, while also protecting freedom of speech. (Paragraph 227)

Government response

In February 2018 the Prime Minister announced that the Law Commission would undertake a review of current legislation on offensive online communications to ensure that laws are up to date with technology, and that the criminal law is fit for purpose when tackling abusive behaviour on social media platforms.

The Law Commission published their review and recommendations, the Scoping Report on Abusive and Offensive Online Communications (the Scoping Report) in November 2018. The Scoping Report looked at the applicable criminal law, focusing on whether the recipient of online and offensive communication has as much protection from the criminal law, in theory and in practice, as they would be afforded if the offending behaviour occurred offline. They also considered whether specific groups in society are more vulnerable to abuse than others.

The Scoping Report concludes that for the most part "abusive online communications are, at least theoretically, criminalised to the same or even greater degree than equivalent offline behaviour." But the Law Commission found that practical and cultural barriers mean that not all harmful online conduct is pursued in terms of criminal law enforcement to the same extent that it might be in an offline context.

The Scoping Report makes a number of initial recommendations for reform, proposing that the two main communications offences could be combined and updated to better account for modern communications technologies and provide better clarity for victims, police and prosecutors. The Scoping Report also recommends further investigation into the issues relating to "pile on" harassment and legal reform in relation to the misuse of private images and information. DCMS is currently considering how the recommendations should be taken forward, including the scope for a possible second phase of the Law Commission report to consider these issues in more detail.

The government has also recently asked the Law Commission to consider a broad review of the law of hate crime in England and Wales. Government's intention is that recommendations made in the Scoping Report in relation to the effectiveness of the law in addressing hate speech will be addressed further in the context of the Hate Crime Review.

Recommendation 22

A principles-based regulatory regime for social media companies should be introduced in the forthcoming parliamentary session. The regime should apply to any site with registered UK users. One of the key principles of the regulatory regime must be to protect children from harm when accessing and using social media sites, while safeguarding freedom of speech (within the bounds of existing law). This principle should be enshrined in legislation as social media companies having a 'duty of care' towards its users who are under 18 to act with reasonable care to avoid identified harms. This duty should extend beyond the age of 18 for those groups who are particularly vulnerable, as determined by the Government. (Paragraph 228)

Government response

The regulatory framework set out in the White Paper makes clear companies' responsibilities to keep UK users safer online through establishing a duty of care towards all UK users. Protecting children, and other vulnerable users, will be a central component of our approach, with the regulator required to take a risk based approach to enforcement - which would mean prioritising, among other things, sites with a large number of young users, or the risk of such users coming to harm is considered greatest. The new regulator will have a legal duty to pay due regard to protect users' rights online, particularly their privacy and freedom of expression.

As already outlined, in the White Paper we propose that the regulatory framework should apply to companies that allow users to share or discover user-generated content or interact with each other online. These services are offered by a very wide range of companies of all sizes, including social media platforms, file hosting sites, public discussion forums, messaging services and search engines.

Recommendation 23

***While the Government should have the power to set the principles underpinning the new regulatory regime, and identify the harms to be minimised, flexibility should be built into the legislation so that it can straightforwardly adapt and evolve as trends change and new technologies emerge*.** (Paragraph 229)

Government response

Establishing a duty of care in law which applies to certain activities (specifically the hosting of user generated content and interaction of users) enables a large degree of flexibility which ensures the regulatory framework outlined in the White Paper is 'future proofed'.

Harmful content and behaviour originates and migrates across a wide range of online services, and these cannot readily be categorised by reference to a single business model or sector. To ensure that the regulatory framework remains effective within the fast changing tech sector, we are consulting on our broad approach to defining the companies in scope. Otherwise we risk harms simply moving or proliferating outside of the scope of our regulation.

As stated previously, we expect the list of harms in scope of the White Paper to evolve over time to respond to new harms and threats.

And while the duty of care will be established in law, the specific steps expected of companies to uphold this will be set out by the regulator in codes of practice which can be updated to reflect evolving trends and technologies.

Recommendation 24

***A statutory code of practice for social media companies, to provide consistency on content reporting practices and moderation mechanisms, must be introduced through new primary legislation, based on the template in the Government Response to its Internet Safety Strategy. The template must, however, be extended to include reports of, and responses to, child sexual abuse and exploitation*.** (Paragraph 230)

Government response

Currently the Digital Economy Act 2017 (DEA 2017), S103, requires the government to publish a code of practice for providers of online social media platforms. The statutory social media code of practice was published in draft in the government response to the Internet Safety Strategy in May 2018.

In accordance with the DEA 2017 S103, the draft code provides guidance to social media providers on appropriate reporting mechanisms and moderation processes to tackle bullying, insulting, intimidating or humiliating conduct online. Following draft publication, we have engaged extensively with a variety of stakeholders to further shape the code of practice. This revised version of the Code was published on 8 April alongside the Online Harms White Paper. By setting out clear standards for industry, we will make sure there is improved support for users online, and that more companies are taking consistent action to tackle abuse. By virtue of statute, the code does not deal with illegal conduct or content.

In future the codes of practice set out by the online harms regulator, however, will set out in detail the steps that companies should take to fulfill their duty of care across a broader range of harms. This might include, for example, measures to ensure that processes for reporting and moderating content and activity are transparent and effective, and steps to ensure that users who have experienced harm are directed to, and receive, adequate support.

As noted earlier, we will expect companies to take particularly robust action against CSEA - with the government having the power to direct the regulator in drawing up the code of practice and the Home Secretary signing off the final version. The Home Office will bring forward an interim code of practice on this issue later this year.

Recommendation 25

A regulator should be appointed by the end of October 2019 to uphold the new regime. It must be incumbent upon the regulator to provide explanatory guidance on the meaning and nature of the harms to be minimised; to monitor compliance with the code of practice; to publish compliance data regularly; and to take enforcement action, when warranted. Enforcement actions must be backed up by a strong and effective sanctions regime, including consideration being given to the case for the personal liability of directors. The regulator must be given the necessary statutory information-gathering powers to enable it to monitor compliance effectively. (Paragraph 231)

Government response

As previously outlined, the government will establish a new statutory duty of care to make companies take more responsibility for the safety of their users and tackle harm caused by content or activity on their services. Compliance with this duty of care will be overseen and enforced by an independent regulator - with effective powers to monitor compliance, gather information and take enforcement action where necessary.

The publication of the Online Harms White Paper will be followed by a 12 week consultation period. Following this the government's response will be published, setting out next steps for legislation. Ahead of the implementation of the new regulatory framework, we will encourage companies to take early action to address online harms. The Government expects companies to take action now to tackle harmful content or activity on their services, and the Home Office will publish interim codes of practice in relation to CSEA and terrorist use of the internet later this year. The White Paper also outlines at a high level the steps companies are expected to take in relation to a range of harms.

We will bring forward legislation as soon as time allows. In the meantime, we are considering the role existing regulators could play both in the interim and longer term.

Recommendation 26

Those subject to the regulatory regime should be required to publish detailed Transparency Reports every six months. As a minimum, the reports must contain information on the number of registered UK users, the number of human moderators reviewing reports flagged in the UK, the volume of reports received from UK users broken down by age, what harms the reports relate to, the processes by which reports are handled—including information on how they are prioritised, the split between human and machine moderation and any reliance on third parties, such as Trusted Flaggers—the speed at which reports are resolved, data on how it was resolved, and information on how the resolution or response was fed back to the user. (Paragraph 232)

Government response

As outlined in our response to recommendation 1, as part of the Internet Safety Strategy Green Paper, the government proposed a system of voluntary transparency reporting. This would provide data on the amount of harmful content being reported to platforms in the UK and information on how these reports are dealt with.

Developing a culture of transparency, trust and accountability will be a critical element of the new regulatory framework and the regulator will have the power to require annual transparency reports from companies in scope, outlining the prevalence of harmful content on their platforms and what countermeasures they are taking to address these. The regulator will also have powers to require additional information, including about the impact of algorithms in selecting content for users and to ensure that companies proactively report on both emerging and known harms.

Recommendation 27

The Government should consider implementing new legislation, similar to that introduced in Germany, such that when content that is potentially illegal under UK law is reported to a social media company, it should have to review the content, take a decision on whether to remove, block or flag that item (if appropriate) or take other actions, and relay that decision to the individual/organisation reporting it within 24 hours. Where the illegality of the content is unclear, the social media company should raise the case with the regulator, who has the authority to grant the social media company additional time to investigate further. The Government should consider whether the approach adopted in Germany of allowing an extra seven days, in the first instance, to review and investigate further should be introduced in the UK. (Paragraph 233)

Government Response

As outlined above, the Online Harms White Paper sets out our plans for new legislation to tackle a wide range of both illegal and unacceptable content and activity online. The new regulatory framework for online safety will make clear companies' responsibilities to keep UK users, particularly children, safer online with the most robust action to counter illegal content and activity.

In shaping our proposals in the White Paper we have investigated many alternative approaches, including looking to learn from a variety of different international examples, including strongly interventionist models - like Germany's NetzDG law that fines social media companies that don't remove untrue or criminal content within 24 hours.

The government agrees that accessible reporting options and features on social media platforms are important for empowering the public to flag the potentially harmful content they encounter online. Having effective reporting processes will be an integral part of fulfilling the new duty of care and will be covered in the codes of practice issued by the independent regulator. We envisage that these codes of practice will also require companies to take prompt, transparent and effective action following user reporting, and to provide clarification as to what constitutes an expedient timeframe for removal of illegal content.

Furthermore, the Safety by Design framework proposed in the White Paper will include principles around user reporting, so that this crucial feature is built into new products and platforms as standard.

Recommendation 28

Given the innovation of new technologies such as "deep fake videos" which cannot be easily identified by human moderators, Social media companies should put in place artificial intelligence techniques to identify content that may be fake, and introduce ways in which to "flag" such content to users, or remove (as appropriate). (Paragraph 234)

Government Response

The government is concerned about the use of the online information environment to manipulate individuals. That is why online manipulation and disinformation has been included as one of the harms in our Online Harms White Paper. Online manipulation can take many forms including the misuse of personal data, the use of AI based algorithms, and the dissemination of false or misleading information. We define 'disinformation' as the deliberate creation and sharing of false and/or manipulated information intended to deceive and mislead audiences, either for the purpose of causing harm or for political, personal or financial gain and define 'misinformation' as the inadvertent sharing of false information.

Deepfake technology is a concern for the government. Used as part of a broader set of tools to disseminate disinformation and other false narratives, deepfakes have the ability to deceive users by accurately replicating a known person's voice (e.g. a public figure) and manipulating video footage to make the content believable. The government is also aware of promising research projects and initiatives that use AI to detect deepfakes.

Social media companies must take the threat of disinformation and wider online manipulation seriously. Government is proactively working with stakeholders, including social media companies and civil society organisations to explore technical solutions, including the use of artificial intelligence, to help tackle these critical problems.

Recommendation 29

Social media companies must put robust systems in place—that go beyond a simple 'tick box' or entering a date of birth—to verify the age of the user. Guidance should be provided, and monitoring undertaken, by the regulator. The Online Pornography (Commercial Basis) Regulations must be immediately revised so that making pornography available on, or via, social media platforms falls within the scope of the regulations. (Paragraph 235)

Government Response

We have been clear that online platforms must do more to enforce their own terms and conditions and protect children and young people from harmful content. Government will continue to work with the technology sector to identify innovative tools and approaches that could be used to safely and reliably verify the age of users.

In terms of Age Verification of Online Pornography, the inclusion of social media platforms was specifically considered during the passage of the Digital Economy Act. It was agreed that the scope should be focused on commercial pornography sites, not popular social media platforms where the overwhelming majority of content is not pornographic.

We will keep this distinction under review; indeed the Secretary of State must report on the regulatory framework within 12–18 months of commencement.

Recommendation 30

Safety-by-design principles should be integrated into the accounts of those who are under 18 years of age. This includes ensuring strong security and privacy settings are switched on by default, while geo-location settings are turned off. Strategies to prolong user engagement should be prohibited and the government should consider improvements to ways in which children are given recourse to data erasure where appropriate. (Paragraph 236)

Government Response

The Government's Internet Safety Strategy sets out the need for the tech industry to establish a culture of 'safety by design' for all users, in which principles of online safety are considered by manufacturers from the very start. The strategy also brings out the role of government in working with industry and consumer groups to agree standards and promote best practice.

As stated in the Online Harms White Paper, the government and the new regulator will work with industry and civil society to develop a safety by design framework, linking up with existing legal obligations around data protection by design and secure by design principles.

The government shares concerns around designed addiction and is determined to ensure that we have sufficient evidence on this risk, and the right expectations of companies to design their products in safe ways. As outlined in the Online Harms White Paper, we expect the future regulator will continue to support research in this area to inform future action and, if necessary, set clear expectations for companies to prevent harm to their users. We also expect companies to be transparent about design practices which encourage extended engagement, and to engage with researchers to understand the impact of these practices on their users.

Separately, the Information Commissioner is working to produce a code of practice on age-appropriate design, as required by the Data Protection Act 2018. The Age-Appropriate Design Code will provide guidance on the privacy standards that organisations should adopt where they are offering online services and apps that children are likely to access and which will process their data. Work on developing the code is well advanced with calls for evidence and commissioned research already concluded. Key interests have already been engaged ahead of a formal public consultation.

Recommendation 31

We believe that Ofcom, working closely alongside the Information Commissioner's Office (ICO), is well-placed to perform the regulatory duties and recommend to the government that it resource Ofcom, and where relevant, the ICO, accordingly to perform the additional functions outlined above. (Paragraph 237)

Government response

As outlined above, the Online Harms White Paper sets out a regulatory framework which will be overseen by an independent regulator.

The government, through the White Paper, is currently consulting on whether that regulator should be a new or existing body, such as Ofcom which would be a strong candidate.

Whichever outcome, we strongly agree that the independent regulator must be adequately funded. We are committed to ensuring the regulator has sufficient resources and the right expertise and capability to perform its role effectively from the outset.

The government intends the new regulator to quickly become cost neutral to the public sector. To recoup the set-up costs and ongoing running costs, the government is considering fees, charges or a levy on companies whose services are in scope. This could fund the full range of the regulator's activity, including setting and enforcing codes of practice, preparing transparency reports, and any education and awareness activities by the regulator.