Department for Digital, Culture Media & Sport

Secretary of State for Digital, Culture, Media and Sport
4th Floor
100 Parliament Street
London SW1A 2BQ

020 7211 6000

www.gov.uk/dcms

The Rt Hon. Lord Henley
Chair
Select Committee on Communications
House of Lords
London SW1A 0PW

MC2017/05693/DC
October 2017

Dear Lord Henley

Lords' Select Committee on Communications: Growing up with the Internet Government response

Further to my letter of 20th July, I am pleased to enclose the Government response to the Select Committee's report *Growing up with the Internet*. I am grateful to you and the Committee for considering this important issue.

I wrote to you about our ambition to "make Britain the safest place in the world to be online". I am very pleased to enclose a copy of our Internet Safety Strategy which has been published today in the form of a green paper, which is accompanied by an eight week consultation process. The Strategy sets out how we will address online safety by bringing groups across society together – including the voluntary sector, technology firms, schools, and the people of Britain – and make online communities safer for users.

The Internet Safety Strategy is just the first part of our wider work on the Digital Charter, which will set out a framework for how businesses, individuals and wider society should act in the digital world and ensure that every individual and every business can seize the opportunities of digital technology.

As you will see, we considered the Committee's timely recommendations as we developed the Strategy. The Strategy therefore responds to the majority of the Committee's recommendations. For those recommendations that aren't addressed fully in the Strategy, I attach additional information.

The Committee asked for sustained leadership in relation to online safety at the highest level and you will know that in February, the Prime Minister asked us to develop an Internet Safety Strategy for children and young people. Indeed, we have gone further and the Strategy now covers all users.

Your report also rightly called for a more coordinated approach across government both in terms of policy and action. We have worked with relevant Departments to make this a truly cross-government Strategy that considers not only the wide range of harms that can put internet users at risk, but also how we can work with industry to draw on their technology and engineering expertise. The Minister for Digital is responsible for all digital matters in government and works with Ministerial colleagues across government and with a wide range of stakeholders including the UK Council for Child Internet Safety (UKCCIS) to keep children and young people safe online.

The Committee also called for an ambitious programme on digital literacy. The Internet Safety 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. To help children successfully manage online risks throughout their lives, we will ensure that digital literacy plays a role in new compulsory Relationships Education (primary) and Relationships and Sex Education (secondary) curricula, as well as Personal, Social, Health and Economic (PSHE) education - if this is made compulsory. We will further encourage peer to peer online safety programmes, recognising the positive impact these can have. Work through civil organisations will enable further outreach to children and young people and help will further embed online safety messages. We want parents to confidently engage with their children on online issues and we will work to ensure they have the guidance they need, starting when their children are very young.

One of the main recommendations in the Committee's report, was to set minimum standards for social media companies. The Digital Economy Act provides for a code of practice which will set out guidance for social media providers in relation to conduct on their platforms. This will form a major tool to help keep children safe and confident online. We are consulting on the code of practice as part of the Strategy. The Strategy will also invite views on proposals for other new initiatives: a levy on social media companies; and working with industry to produce an annual internet safety transparency report.

The Committee asked for a commitment to child-centered design in technology. The Strategy considers what it can do to support and develop a world-class online safety industry in the UK, providing better information to startups and app developers on safety and how individual technologies can deliver safer services.

We also acknowledge the pioneering role that the UKCCIS has played in promoting and championing improvements to child online safety in the UK. We propose building on this and remodelling UKCCIS to align with the Strategy so that it can take a leading role in this work.

We agree with the Committee that the voice of children and young people is crucial to the success of the Strategy and to children enjoying the Internet safely, so we plan to hold a children's roundtable to better understand their concerns about online safety. As part of the consultation on the Strategy, we have also plan to hold focus groups with children so they can share their views on online safety.

We agree with the Committee that children's good mental health online is paramount and we have therefore been working closely with the Secretary of State for Health on the forthcoming green paper on Children's and Young People's Mental Health. Indeed, we will shortly jointly chair a roundtable with social media and technology companies to discuss what they are doing to support children's mental health. This will help inform the work of both our Departments.

You raise the important point of how the existing legal measures are applied. You may know the Crown Prosecution Service (CPS) has revised its guidelines regarding online abuse committed on social media. This gives clear advice to prosecutors about the handling of online abuse to ensure consistency. In addition, 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 channelled.

Finally, I am pleased to be publishing a literature review, undertaken by Professor Sonia Livingstone, Professor Julia Davidson and Dr Jo Bryce, on behalf of the UKCCIS Evidence Working 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. The report will be used to inform our work going forward.

I hope you will agree that we have made significant strides to keep children and young people safe online since the Committee submitted its report. I hope the Committee will feel able to respond to the Internet Safety Strategy consultation.

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

House of Lords Communication Select Committee Report on Growing up with the Internet

Government response

The government is grateful to the Committee for its timely inquiry into children and the Internet, for its valuable contribution to the debate on the broad range of communications and public policy, and for highlighting areas of concern to Parliament and the public.

As set out in the accompanying letter, we were able to consider the Committee's recommendations while we were developing our Internet Safety Strategy.

Consequently, we have been able to address the following recommendations within the Strategy - recommendations 1, 2, 6, 8, 10, 12, 14, 15, 16, 17, 18, 24, 25, 26, 29, 30, 31, 32, 33, 34, 36, 37, 38.

This Annex addresses the remaining recommendations that have not been fully acknowledged by the Strategy.

Recommendation 3

The government has a key role in providing an appropriate framework for stakeholders to act in a concerted, joined-up way. It has a particular obligation to comply with the UN Convention on the Rights of the Child to ensure that children's wellbeing is protected, to promote children's right to be heard in matters that affect them, and to act in the best interests of the child in all cases.

Government response

The Internet Safety Strategy will help address the UNCRC Committee's recommendation on keeping children safe on the Internet.

There is an international agreement that protects the rights of children and provides a child-centred framework for the development of services to children. The UK government ratified the United Nations Convention on the Rights of the Child (UNCRC) in 1991 and, by doing so, recognises children's rights to expression and receiving information.

The UNCRC continue to underpin associated government policy and legislation across government. The UK has reaffirmed its commitment to give the UNCRC due consideration.

In October 2016, we responded to the UN's concluding recommendations which included action designed to raise the profile, awareness and embed children's rights across Whitehall and beyond.

The government has committed to:

- put in place a Civil Service Learning package to raise awareness of children's rights and the UNCRC across the civil service;
- work with the Joint Committee of Human Rights and other stakeholders to look at how we can best promote and embed good practice through the use of Child Right's Impact Assessments;
- work with stakeholders to promote and share best practice from those Local Authorities effective in promoting children's rights;
- set up an Action Group;
- update the statutory guidance '*Working Together to Safeguard Children*' to strengthen wording around children's rights;
- engage with those colleagues with expertise, to see how we might change behaviours to ensure children's rights remains at the forefront of policy;
- involve children and young people;
- work with the FCO and Crown Dependencies to ensure extension of the Convention; and
- review progress with government departments and relevant non-government organisations.

Recommendation 4 and 5

We recommend that the government should establish the post of Children's Digital Champion at the centre of the government within the Cabinet Office, with a remit to advocate on behalf of children to industry, regulators and at ministerial level across all government departments.

The remit of the Children's Digital Champion should include:

- establishing and overseeing the implementation of minimum standards of design and practice across the entire internet value chain,
- working with the Department for Education to set the standard of digital literacy and PSHE in all UK schools,

- commissioning research, and ensuring existing rights and legislation are implemented in online settings.

Government response

The Minister for Digital is responsible for all digital matters in government and will work with Ministerial colleagues across government and with a wide range of stakeholders, including the UK Council for Child Internet Safety (UKCCIS) to keep children and young people safe online.

The Minister for Digital plays a central role in government working with Ministerial colleagues in other government departments to address all of these issues. Our proposals for a remodelled UKCCIS will also continue to ensure a coordinated approach to bringing industry together with charities, academics and government.

Recommendations 6 & 7

The committee put forward the proposal of the Prime Minister taking forward the recommendations of the report by convening a summit which would establish minimum standards for child-friendly design, filtering, privacy, data collection, terms and conditions of use, and report and response mechanisms for all businesses in the internet value chain, public bodies and the voluntary sector. The committee recommended that the standards should be set out in a code of conduct, which should also seek to promote digital literacy. If industry fails to implement the recommendations, then the government should take action. The UK must be an exemplar in raising standards.

Government response

We thank the Committee for the suggestion of holding a summit. We will consider this as one of the next steps, following the conclusion of our Internet Safety Strategy consultation.

We will look to industry partners to develop and deliver content that helps children to understand how to build their digital literacy on social media platforms. In the Strategy consultation, we ask questions about the role technology companies should play in supporting children to develop their digital literacy skills and how they can go about doing this. We would expect industry to provide information on how to maximise the benefits of their online activities, how to support other users online and how to report or contact social media companies when things do go wrong.

Recommendation 9

We note the NSPCC's suggestion for creating a user generated age rating system. We recommend that the Children's Digital Champion work with others to investigate the potential of such a scheme.

Government response

It is important that parents and children have the ability to understand the type of content that may be available to them and make choices about what they access. There are currently a number of ways children are protected from accessing and viewing unsuitable content online, accidentally and on purpose, including family friendly filters, the British Board of Film Classification's best practice, voluntary regulation of commercial and internet content delivered via mobile networks and specifically designed platforms and features such as YouTube Kids and YouTube Restricted Mode.

The Internet Safety Strategy and the development of a social media code of practice offer the opportunity to identify the activities that will be most effective in empowering UK citizens to manage the risks posed by age inappropriate content and stay safe online. In addition, the implementation of age verification for online pornography will provide an important demonstration of the regulation of age restricted content. Government will be required to report on impact and effectiveness of the regulatory framework 12-18 months after the powers come into force.

Recommendation 11

The government should also involve further education providers as well as universities and encourage them to incorporate the standards and the code of practice in relevant courses.

Government response

This would primarily be a matter for the providers and awarding organisations who own the qualifications to take forward. Further Education (FE) Initial Teacher Training (ITT) is different to that for schools. Although DfE does not own the content or standards for FE ITT, the Secretary of State for Education has stated her commitment to provide additional support for teachers and leaders working in the sector, and we expect to look carefully at how teachers and leaders are trained to work in the sector, and the qualifications available to them, to ensure that these are fully fit for purpose.

Recommendation 13

We recommend that specific training modules be developed and made compulsory as part of qualifying in frontline public service roles, including but not limited to,

police, social workers, general practitioners, accident and emergency practitioners, mental health care workers and teachers.

Government response

We recognise the benefits of training modules to help workers identify online issues, in a number of public service roles.

Social workers - The independent regulator, the Health and Care Professions Council, sets mandatory standards of initial education and training courses. These standards include a requirement that learning outcomes ensure that, those who successfully complete an approved programme, meet the standards of proficiency for social work (available at: http://www.hcpc-uk.org/assets/documents/10003B08Standardsofproficiency-SocialworkersinEngland.pdf).

The knowledge and skills statement for child and family practitioners includes, in relation to child abuse and neglect, that social workers should 'consider the possibility of child sexual exploitation [and], grooming (on and offline)'.

Teachers - It is for ITT providers to ensure courses support trainee teachers to meet the Teachers' Standards at the appropriate level. These standards include having regard for the need to safeguard pupils' well-being, in accordance with statutory provisions.

The government specifies that ITT providers and trainee teachers must adhere to school-based policies surrounding the safe use of digital technology and digital recordings. In the absence of such a policy, providers are expected to establish and share a code for safe practice.

Health workers - NHS employees can access online safety training via the E-Learning for Healthcare resource. Created as part of the MindEd programme, it is aimed at professionals and volunteers who come into contact with children and young people, so includes teachers, healthcare workers, police, youth workers etc.

The following resources are available online:

- *Online Safety and Wellbeing: Getting the Focus Right* explores the tensions between the expectations of online safety and the realities of young people's behaviours online.
- *Children and Young People's Digital Liv*es outlines some of the risks children may encounter and action they can take. It also highlights the importance of professionals and parents talking to children and young people about their digital usage and online experiences.

- *Online Risk and Resilience* examines risks faced by young people as they negotiate life online. It will explore key concepts underpinning the theory, practice and research of online risk and resilience.

Police - 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 channelled.

Specially trained officers will liaise with the victim and use their knowledge of online hate crime to collect relevant evidence to bring a prosecution. Evidence and any preliminary investigative work to identify the perpetrator will then be allocated to the police force in the victim's local area to take forward the investigation. The hub will provide local forces with guidance or specialist knowledge.

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.

It will begin operating by the end of the year. If successful, the hub could be expanded using match funding from social media companies.

Recommendation 19

We recommend that, as suggested by the Children's Commissioner, her power to request information from public bodies should be expanded to include aggregated data from social media companies and online platforms.

Government response

In our Internet Safety Strategy we are consulting on whether social media companies should pledge greater transparency about the incidences of reporting that takes place on their platforms. We are also consulting on a code of practice which will give companies guidance on how best to keep their platforms safe.

Recommendation 20

We further recommend that there should be a mechanism for independently handling requests from children for social media companies to take down content. This might take the form of an Ombudsman, as suggested by the Children's Commissioner, or a commitment from industry to build and fund an arbitration service for young people.

Government response

Social media companies are already undertaking significant steps to keep their platforms and sites safe for users through education programmes, technological advancements and working with civil society. However, we think there's more which they could do to help us understand the prevalence and seriousness of the harms on their sites and how these are dealt with. Therefore in our Internet Safety Strategy, we are consulting on whether social media companies should pledge greater transparency about the incidences of reporting that takes place on their platforms, as well as consulting on our code of practice which will give companies guidance on how best to keep their platforms safe.

The Minister for Digital and our proposals for a remodelled UKCCIS will ensure that technology companies take their responsibilities to users seriously. Using the evidence gathered as part of our Internet Safety Strategy consultation, we will consider what further options we should take forward, to ensure that we can achieve our goal of creating a safer online environment for children.

Recommendations 21 and 22

We recommend that all ISPs and mobile network operators should be required not only to offer child-friendly content control filters, but also for those filters to be 'on' by default for all customers. Adult customers should be able to switch off such filters.

Those responsible for providing filtering and blocking services need to be transparent about which sites they block and why, and be open to complaints from websites to review their decisions within an agreed timeframe. Filter systems should be designed to an agreed minimum standard.

Government response

The government believes that 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. 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, Talk Talk and BT), covering the vast majority of UK subscribers, are delivered through specialist digital technology companies, and use a combination of web-trawling and human intelligence to ensure acceptable sites are not filtered in error. The ISPs have transparent mechanisms in place for anonymous reporting of any ‘over-blocking’, and to allow customers to ‘white-list’ sites.

Around 95% of the UK fixed broadband market offers free network-level or device-level parental filters. The remaining 5% includes smaller ISPs offering business to business or niche specialist services to limited subscriber bases. Requiring filtering systems to be in place would not necessarily be appropriate or proportionate for these ISPs.

Recommendations 23

We welcome the development of internet services which are specifically designed for very young children but regret that there are no such services for children as they grow older. We have found that there is resistance to providing services which incorporate the support and respect for rights that would enable a better internet experience for all children as they explore the wider internet.

Government response

In our Strategy, we look at how technology can improve safety for all users.

We know that technical solutions, developed by industry, can help keep users safe online. 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 think safety first to raise their level of safety from their launch, and will consider the role that individual technologies, including application (app) stores and operating systems can play in delivering safer services.

Recommendation 27

All platforms and businesses operating online must explain their data collection practices, and other terms and conditions, in a form and language that children are

likely to understand. Their explanations should not try to obfuscate the nature of the agreement.

Government response

From May 2018, the General Data Protection Regulation (GDPR) will reinforce the need for businesses processing personal data for data controllers operating online to explain their collection practices and rights in clear and plain language specifically to a child. This can be found in Article 12 of the GDPR 'Transparent information, communication and modalities for the exercise of the rights of the data subject'.

Recommendation 28

All platforms and businesses operating online must not seek to commercially benefit or exploit value from the sharing or transfer of data gained from a child's activities online, including data transferred between services that are owned by the same parent company. They should uphold a principle of minimum data gathering necessary for the delivery of a service when the end user is a child.

Government response

The data protection principles in the Data Protection Act 1998 set out that processing of personal data must be fair and lawful, that data should only be obtained for one or more specified and lawful purposes, and should not be further processed in any manner incompatible with that purpose or those purposes. The principles also provide that personal data should be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. These principles apply to data controllers, regardless of whether they are operating online or offline.

Recommendation 35

We caution that internet safety systems should not undermine children's rights to privacy, to learn about the world and to express themselves. The government should require schools to obtain the informed consent of parents and students, and they should have the opportunity to opt out.

Government response

Keeping Children Safe in Education sets out that whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding. The guidance can be found here: https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

The government asked UKCCIS to set up an Overblocking Working Group involving charities and industry to look at potential inadvertent blocking of non-harmful sites. In 2014, in addition to their own branded web sites, the UK's four leading ISPs, established a dedicated page to report overblocking or mis-categorisation. Reported numbers were low. Of the 1969 visits, only nine emails were received and all reports were resolved satisfactorily. Overblocking is being kept to a minimum and the ISPs and Mobile Network Operators (MNOs) remain committed to ensuring filtering remains proportional and age appropriate.

The Overblocking Group concluded its work in 2015. However this issue continues to be looked at by the UKCCIS Technical Working Group, while ISPs and MNOs continue to monitor and respond to reports on incidences of overblocking.