Home Office

Karen Bradley MP
Minister for Preventing Abuse, Exploitation and Crime

2 Marsham Street,
London SW1P 4DF
www.gov.uk/home-office

Liz Saville Roberts MP
House of Commons
London
SW1A 0AA

20 APR 2016

Dear Liz

POLICING AND CRIME BILL

During our debate in Committee on your new clause 16 (Digital Crime Review) on 12 April, I undertook to write to you to set out in detail the work that we are doing to protect children online (Official Report, column 314).

This Government works through the multi-stakeholder organisation the UK Council for Child Internet Safety (UKCCIS). UKCCIS brings together government, industry, law enforcement agencies, academia, charities and parenting groups to work in partnership to help to keep children and young people safe online. I co-chair its executive board with the Minister for Children and Families and the Minister for Internet Safety and Security.

Ofcom recently led a social media working group on behalf of UKCCIS, which included Twitter, Facebook, Google, Ask.FM, MindCandy and Microsoft, to develop a practical guide to child safety online to encourage responsible practice by providers of social media and interactive services. This guide, as well as a practical guide for parents and carers whose children are using social media, can be found at www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis.

The four major internet service providers (BT, Sky, TalkTalk and Virgin Media together constitute an estimated 90% of the UK's broadband market) have also delivered on their commitment to provide an unavoidable choice on whether to switch on family friendly network level filters to all their customers. The decision to install filters or change existing settings can only be made by an adult account holder who must be over 18, which is verified when accounts are set up. We have also been working with the Internet Service Providers Association (ISPA), the trade association for ISPs, to see what more smaller providers can do.

On mobile networks, content that would be considered unsuitable for customers under the age of 18 is filtered. The British Board of Film Classification (BBFC) provides an independent framework for mobile networks and defines content that is unsuitable for customers under the age of 18 based on their Classification Guidelines for film and video.

A Friendly WiFi Logo was launched by the RDI (UK) Holdings in July 2014 to help parents identify the safest places to browse the internet. The logo will give parents the assurance that a particular business, retailer, or public space is filtering to an agreed and clearly communicated minimum (currently illegal child abuse content, plus pornography). This is now in place in many stores, including Tesco, Starbucks and IKEA.

The Government committed, in our manifesto, to requiring age verification for access to all sites containing pornographic material. A public consultation exercise was launched on 16 February and ran until 12 April; we will be publishing our response shortly.

In schools, e-safety is now covered at all key stages in the computing curriculum. The introduction of e-safety content in key stages 1 and 2 reflects the fact that younger children are increasingly accessing the internet, and is intended to inform pupils of good practice in staying safe online from an early age. Since September 2014, children in primary schools have started to be taught how to use technology safely and respectfully, how to keep personal information private, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

In secondary schools, pupils are taught about responsible, respectful and secure use of technology, as well as age-appropriate ways of reporting any concerns they may have about what they see or encounter online. There is progression in the content across the key stages to reflect the different and escalating risks that young people face as they get older (initially relating to online content, then to the conduct of and contact with others). The content was developed with input from e-safety experts including Childnet, NSPCC and the UK Safer Internet Centre.

Keeping Children Safe in Education is the statutory guidance to which all schools must have regard to when carrying out their duties to safeguard and promote the welfare of children. All school staff have a responsibility to provide a safe environment in which children can learn. The Department for Education (DfE) are in the process of updating the guidance and changing the requirement from schools "considering" teaching children about safeguarding, including online to "ensuring" they teach children about safeguarding, including online. DfE expect this to be through teaching and learning opportunities, as part of providing a broad and balanced curriculum. This may include covering relevant issues through personal, social, health and economic education (PSHE), and/or, for maintained schools, through sex and relationship education. The guidance will also for the first time include a section covering online safety and providing links to guidance from the UK Safer Internet Centre setting out what appropriate filters and monitoring systems in schools might look like. DfE are also highlighting the importance of schools considering online safety as part of their broader safeguarding policies and processes and ensuring it is reflected in their child protection policy and their safeguarding training plans for their staff. It is anticipated that the new guidance will commence in September.

Our response to child sexual exploitation (CSE) online includes law enforcement agencies taking action against online offenders; developing new capabilities to find and safeguard victims and working with the internet industry to remove illegal images. The National Crime Agency's (NCA) Child Exploitation and Online Protection (CEOP) Command leads, supports and coordinates the law enforcement response to child sexual exploitation and abuse and works closely with social media companies, and law enforcement agencies in the UK and overseas, to identify victims and pursue offenders.

In December 2014, the Prime Minister announced additional funding of £10 million in 2015/16 for further specialist teams in the NCA to tackle online CSE. This has enabled a near doubling of their investigative capability which will lead to more children being safeguarded from sexual exploitation. The Prime Minister also announced a joint NCA and GCHQ team to target the most technologically advanced offenders and this formally commenced operational activity in November 2015.

As I indicated in the debate on new clause 19 (Modern technology: specialist digital unit), all UK police forces and the NCA are now connected to the new Child Abuse Image Database (CAID) that was launched in 2014. A new operational victim identification strategy has been established around CAID by the NCA and is helping to identify even more victims of online child abuse. In the first ten months of 2015/16, UK law enforcement had already identified more than double the number of victims of this abuse than in the whole of any previous year.

The NCA's *Thinkuknow* education programme is aimed at children and young people, their parents/carers and the professionals who work with them. It is at the forefront of the NCA's educational activity to protect children from sexual exploitation and sexual abuse. *Thinkuknow* provides educational resources for use with children and young people helping them to identify the risks they may face both online and off, understand how to protect themselves and know how to seek further support. The resources include films, games, lesson plans and practitioner guidance and are free for all professionals working with children and young people. The *Thinkuknow* website provides children, young people and their parents/carers with access to information and advice about staying safe from sexual exploitation and sexual abuse. In 2014/15, the NCA's *Thinkuknow* educational messages and materials reached 1,556,008 primary aged school children and 1,683,478 secondary aged school children.

The NCA's CEOP Command has built on the success of the *Thinkuknow* programme and recently launched a new website for parents and carers. The site focuses on helping parents protect their children from abuse online, providing up to date advice on preventing their children becoming victims of sexual abuse and exploitation both online and in the 'real world'. Families can visit the Thinkuknow website to access advice and support. Articles provide guidance on topics as diverse as: challenging harmful sexual attitudes and promoting positive behaviours; helping a child with autism negotiate life online; supporting a child who has been sexually abused; and dealing with a range of online issues such as sending nude selfies and viewing pornography. Users can find films, downloadable guides and useful links to support organisations.

Online CSE is a global problem, however, and through the WePROTECT alliance, launched by the Prime Minister in December 2014, the Government is actively working with countries, companies and civil society organisations to develop a coordinated global response. Following on from the successful WePROTECT summits in London and Abu Dhabi, 64 countries, companies and civil society organisations signed up to the commitments in the WePROTECT Statement of Action. In March, Baroness Shields hosted the first meeting of the WePROTECT Advisory Board. The new Board is committed to transforming how the crime of online child sexual exploitation is addressed. Its mission is to empower everyone with a responsibility to protect children online to identify and protect victims, remove child sexual abuse material from the internet and strengthen cooperation to track down the perpetrators of this abuse all over the world.

At the first WePROTECT summit in 2014 the Internet Watch Foundation (IWF) committed to working with technology companies to share hashes – digital 'fingerprints' – of indecent images of children. Since then, almost 19,000 of these hashes – all of which originated from CAID – have been assessed by the IWF and shared with five major global technology companies, to enable the removal, and prevent the sharing, of images from their platforms and services.

I am copying this letter to the members of the Public Bill Committee and placing a copy in the library of the House.

Karen Bradley MP