

Press release: UK to introduce world first online safety laws

- Independent regulator will be appointed to enforce stringent new standards
- Social media firms must abide by mandatory “duty of care” to protect users and could face heavy fines if they fail to deliver
- Measures are the first of their kind in the world in the fight to make the internet a safer place

In the first online safety laws of their kind, social media companies and tech firms will be legally required to protect their users and face tough penalties if they do not comply.

As part of the Online Harms White Paper, a joint proposal from the Department for Digital, Culture, Media and Sport and Home Office, a new independent regulator will be introduced to ensure companies meet their responsibilities.

This will include a mandatory ‘duty of care’, which will require companies to take reasonable steps to keep their users safe and tackle illegal and harmful activity on their services. The regulator will have effective enforcement tools, and we are consulting on powers to issue substantial fines, block access to sites and potentially to impose liability on individual members of senior management.

Prime Minister Theresa May said:

The internet can be brilliant at connecting people across the world – but for too long these companies have not done enough to protect users, especially children and young people, from harmful content.

That is not good enough, and it is time to do things differently. We have listened to campaigners and parents, and are putting a legal duty of care on internet companies to keep people safe.

Online companies must start taking responsibility for their platforms, and help restore public trust in this technology.

A range of harms will be tackled as part of the [Online Harms White Paper](#), including inciting violence and violent content, encouraging suicide, disinformation, cyber bullying and children accessing inappropriate material.

There will be stringent requirements for companies to take even tougher action to ensure they tackle terrorist and child sexual exploitation and abuse content.

The new proposed laws will apply to any company that allows users to share or discover user generated content or interact with each other online. This means a wide range of companies of all sizes are in scope, including social media platforms, file hosting sites, public discussion forums, messaging services, and search engines.

Digital Secretary Jeremy Wright said:

The era of self-regulation for online companies is over. Voluntary actions from industry to tackle online harms have not been applied consistently or gone far enough. Tech can be an incredible force for good and we want the sector to be part of the solution in protecting their users. However those that fail to do this will face tough action.

We want the UK to be the safest place in the world to go online, and the best place to start and grow a digital business and our proposals for new laws will help make sure everyone in our country can enjoy the Internet safely.

Home Secretary Sajid Javid said:

The tech giants and social media companies have a moral duty to protect the young people they profit from.

Despite our repeated calls to action, harmful and illegal content – including child abuse and terrorism – is still too readily available online.

That is why we are forcing these firms to clean up their act once and for all. I made it my mission to protect our young people – and we are now delivering on that promise.

A regulator will be appointed to enforce the new framework. The Government is now consulting on whether the regulator should be a new or existing body. The regulator will be funded by industry in the medium term, and the Government is exploring options such as an industry levy to put it on a sustainable footing.

A [12 week consultation](#) on the proposals has also been launched today. Once this concludes we will then set out the action we will take in developing our final proposals for legislation.

Tough new measures set out in the White Paper include:

- 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.
- Further stringent requirements on tech companies to ensure child abuse and terrorist content is not disseminated online.
- Giving a regulator the power to force social media platforms and others to publish annual transparency reports on the amount of harmful content on their platforms and what they are doing to address this.
- Making companies respond to users' complaints, and act to address them quickly.
- Codes of practice, issued by the regulator, which could include measures such as requirements to minimise the spread of misleading and harmful disinformation with dedicated fact checkers, particularly during election periods.
- A new "Safety by Design" framework to help companies incorporate online safety features in new apps and platforms from the start.
- A media literacy strategy to equip people with the knowledge to recognise and deal with a range of deceptive and malicious behaviours online, including catfishing, grooming and extremism.

The UK remains committed to a free, open and secure Internet. The regulator will have a legal duty to pay due regard to innovation, and to protect users' rights online, being particularly mindful to not infringe privacy and freedom of expression.

NSPCC CEO Peter Wanless said:

This is a hugely significant commitment by the Government that once enacted, can make the UK a world pioneer in protecting children online.

For too long social networks have failed to prioritise children's safety and left them exposed to grooming, abuse, and harmful content. So it's high time they were forced to act through this legally binding duty to protect children, backed up with hefty punishments if they fail to do so.

We are pleased that the Government has listened to the NSPCC's detailed proposals and we are grateful to all those who supported our campaign.

Recognising that the Internet can be a tremendous force for good, and that technology will be an integral part of any solution, the new plans have been designed to promote a culture of continuous improvement among companies. The new regime will ensure that online firms are incentivised to develop and share new technological solutions, like Google's "Family Link" and Apple's Screen Time app, rather than just complying with minimum requirements. Government has balanced the clear need for tough regulation with its ambition for the UK to be the best place in the world to start and grow a digital business, and the new regulatory framework will provide strong protection for our citizens while driving innovation by not placing an impossible burden on smaller companies.

Barnardo's Chief Executive, Javed Khan said:

Children in the UK are facing growing risks online – from cyber-bullying to sexual grooming to gaming addiction.

The internet can be a force for good but we can't ignore the risks. Two thirds of the vulnerable children and young people supported through our sexual exploitation services were groomed online before meeting their abuser in person.

Barnardo's has long called for new laws to protect children online, just as we do offline, so they can learn, play and communicate safely.

The Government's announcement today is a very important step in the right direction. We particularly welcome proposals for a new independent regulator, which should ensure internet bosses make the UK one of the safest places in the world for children to be online.

Alex Holmes, Deputy CEO at The Diana Award said:

The Diana Award welcomes today's Online Harms White Paper. We understand the powerful and influential role that the internet plays in the lives of young people and that's why we are dedicated to training Anti-Bullying Ambassadors in schools across the UK to keep themselves and their peers safe online.

We believe that the time is right for further innovation from the tech sector when it comes to their approach to safety. While their products are constantly evolving and innovating, there is room for innovation on their approach to safeguarding.

We look forward to continuing to work with industry, government and other organisations to help children and young people in particular, manage risks and reduce harms.

Will Gardner, CEO of Childnet said:

We look forward to this opportunity to help shape a better and safer environment for children and to continue and grow our current work to equip them with the information and skills they need to navigate the internet positively and safely. As we speak to thousands of children, parents, teachers and other professionals each year, we want to mobilise and support them to be part of the solution.

We know that young people have strong ideas and opinions on online safety and it is their experiences we hope to reflect when responding to this consultation.”

Carolyn Bunting, CEO, Internet Matters, said:

We support the government’s desire to make the UK the safest place to be online. The internet simply wasn’t built with children in mind, so it is vital that government plays a greater role in determining and setting standards for the services that children commonly use, and that industry responds quickly and effectively.

Proactive regulation and better technical solutions, whilst welcomed, are just one part of the solution. We have to help parents to have greater awareness and understanding of their child’s digital wellbeing. It would be unfair to leave those parents or guardians to figure it out for themselves. Instead we must make available as many accessible, simple resources for parents based on expert advice which makes it as easy as possible for them to understand.□

Read the [White Paper and relevant consultation documents](#).

Today we have published our updated [Digital Charter](#), alongside the White

Paper. Through the Digital Charter, we are protecting citizens, increasing public trust in new technologies, and creating the best possible basis on which the digital economy and society can thrive.

Online harms in scope of the White Paper – The table below shows the initial list of online harmful content or activity in scope of the White Paper, based on an assessment of their impact on individuals and society and their prevalence. This list is, by design, neither exhaustive nor fixed. A static list could prevent swift regulatory action to address new forms of online harm, new technologies and online activities.

Harms with a clear legal definition	Harms with a less clear legal definition	Underage exposure to legal content
Child sexual abuse and exploitation	Cyberbullying and trolling	Children accessing pornography Children accessing inappropriate material (including under 13s using social media and under-18s using dating apps; excessive screen time)
Terrorist content and activity	Extremist content and activity	
Organised immigration crime	Coercive behaviour	
Modern slavery	Intimidation	
Extreme pornography	Disinformation	
Revenge pornography	Violent content	
Harassment and cyberstalking	Advocacy of self-harm	
Hate crime	Promotion of Female Genital Mutilation	
Encouraging or assisting suicide		
Incitement of violence		
Sale of illegal goods / services, such as drugs and weapons (on the open internet)		
Contempt of court and interference with legal proceedings		
Sexting of indecent images by under 18s		

The Cabinet Office has announced the ‘RESIST’ toolkit, which enables organisations to develop a strategic counter-disinformation capability. The toolkit is primarily a resource for public service communications teams and it equips people with the knowledge and skills to identify, assess and respond to disinformation. The ‘RESIST’ model provides straightforward steps to follow and promotes a consistent approach.

The Government is also taking action on disinformation with a [behaviour](#)

[change campaign](#) aimed at the public. The pilot campaign has launched and aims to increase audience resilience to disinformation, by educating and empowering those who see, inadvertently share and are affected by false and misleading information. The campaign will increase the audience's ability to spot disinformation by providing them with straightforward advice to help them check whether content is likely to be false or intentionally misleading.