The Online Safety Act: what it means for children and professionals

Last updated: 14 Nov 2023 Topics: o
The online world plays a huge role in the lives of children and young people. Social media, online gaming, instant messaging platforms and image-sharing services enable children to interact with their peers, develop and pursue interests, and connect with new communities. However, these platforms and services also come with risks, including online abuse, grooming, and exposure to content that is illegal or harmful.

The Online Safety Act 2023 sets out to minimise these risks, placing new legal duties and responsibilities on online service providers to keep children and young people safe online.

How will the Online Safety Act help keep children safe?

The Act means that tech companies running social networking sites or search engines must promote online safety by tackling illegal material and content that is harmful to children, conducting regular risk assessments, and properly enforcing age limits.

To make sure companies meet these requirements, the government has placed the independent regulator Ofcom in charge of enforcing the regulatory framework and raising awareness around online safety.

Tackling illegal and harmful content

Companies will now need to prevent, detect and remove illegal content. This includes content depicting, promoting or facilitating:

- child sexual abuse
- controlling or coercive behaviour
- terrorism
- suicide.

Companies must prevent children from accessing content that is harmful or age-inappropriate. This includes content depicting, promoting or facilitating:

- pornography
- serious violence
- bullying
- self-harm
- eating disorders.

Regular risk assessments

Companies must assess the risks and dangers that their platforms pose to the safety of children. If risks are identified, companies are required to act by putting mitigations in place.
Larger companies will also need to publish a summary of their risk assessments, promoting increased transparency around the risks that online platforms and services pose to children.

Enforcing age limits

If harmful or age-inappropriate content is present on a platform, companies must use age verification or age estimation tools to prevent children from encountering this type of content.

Companies will have to declare which age assurance tools they are using, if any, and show that they are enforcing their age limits.

How will the Online Safety Act be enforced?

Ofcom will be working with tech companies to make sure they are protecting their users and following the requirements set out in the Act. Their draft guidance and codes of practice are currently under consultation and will come into force once approved by parliament.

If companies fail to comply with the new rules, Ofcom have powers to enforce:

- fines of up to £18 million, or 10% of the company's annual global turnover, whichever is greater
- criminal action against companies and/or senior managers who fail to comply with requirements or fail to follow requests from Ofcom
- business disruption measures, including preventing companies from being accessed or generating income in the UK.

How will the Online Safety Act affect professionals working with children?

The Act places the onus on tech companies to keep children safe on their services and platforms. Although the Act won't affect your duties as a professional, it's important to be aware of changes that may impact your professional practice.

Social media companies will have to provide adults and children with clear, accessible and easy-to-use ways to report problems and make complaints online if harms arise. So if you think a site is falling short of the required standards, it should be easy to raise your concerns with the platform.

If you have ongoing concerns about a platform, you can make a complaint to Ofcom. While Ofcom cannot respond to individual complaints, this information can help them to assess which services are complying with the regulation.[1]

The Act also introduces new criminal offences, including:

- an intimate image abuse offence, which makes it a crime to share an intimate image of someone without their consent
- a 'cyberflashing' offence, which criminalises sending an explicit image for the purpose of sexual gratification or to cause the recipient humiliation, alarm or distress.

It's important that you are aware of these new offences, and that you know what steps to take if you need to support a young person who has had an image shared without their consent, or who has received or sent an explicit image.

> Find out more about responding to instances of nude image sharing

More online safety information for professionals

> Find out more about social media and online safety

> Read about the 4 Cs of online safety in this blog

> Take our CPD-certified Online safety elearning course

> See online safety guidance and resources for schools

About the author

Rani Govender is a Senior Policy and Public Affairs Officer for Child Safety Online at the NSPCC, influencing change in legislation and policy to tackle the preventable abuse and harm children experience online.

Tell me more

E-safety for schools

See our online safety support guidance and resources for schools and colleges.

Learn more

Sharing nudes and semi-nudes training

Take our online training to help respond to incidents of nude image sharing or sexting.

View course

Online safety policy statement and agreement

Templates for an online safety policy statement and an online safety statement you can tailor to the context of your organisation.

Download template