PANORAMIC

ONLINE SAFETY REGULATION

United Kingdom - England & Wales

LEXOLOGY

Online Safety Regulation

Contributing Editors

Jenna Rennie, Rory Hishon and Alexander Beaton

White & Case LLP

Generated on: March 31, 2026

Contents

Online Safety Regulation

Contributors

United Kingdom - England & Wales

White & Case LLP

WHITE & CASE

Rory Hishon	rhishon@whitecase.com
Jenna Rennie	jenna.rennie@whitecase.com
Joseph Carroll	joseph.carroll@whitecase.com
Ben Harris	ben.harris@whitecase.com

LEGAL FRAMEWORK

Legal regime

Does your jurisdiction have a legal regime governing or addressing online safety? If so, how does it operate?

In the UK, the Online Safety Act 2023 (OSA) is the dedicated legal regime regulating online safety. It imposes statutory duties on providers of user-to-user services and search services, requiring them to take steps to identify, assess and mitigate risks arising from illegal content and (if the service is child-accessible) from content that is harmful to children. Providers of certain pornographic content are also required to prevent children from accessing such content. The OSA empowers the Office of Communications (Ofcom) as the UK's online safety regulator.

The OSA is supplemented by regulations (to be made by Ofcom and the Secretary of State) on various topics, as well as by detailed 'codes of practice' and guidance from Ofcom about how in-scope providers can comply with their duties. The OSA not the only source of UK law that may impact the online safety landscape. Other legal instruments contribute to a safer online environment by targeting particular risks and strengthening protective measures across digital services. For example, the UK's General Data Protection Regulation (the UK GDPR) is primarily designed to safeguard personal data and privacy, and the Terrorism Act 2006 imposes obligations on intermediary services to act if notified by police of unlawful terrorism content. However, given the number and variety of such laws, and the fact that they narrowly relate to particular issues or aspects of online safety, we have focused below on the OSA, as the UK's principal legislation designed to address online safety more broadly.

Law stated - 18 December 2025

Online harms covered

Which online harms are covered under the relevant legislation and how are these harms defined?

The OSA covers three main categories of online harms: (1) illegal content; (2) content that is harmful to children; and (3) 'provider pornographic content':

- 'Illegal content' is defined in section 59 and schedules 5 to 7 of the OSA. It refers to user-generated content that 'amounts to a relevant offence'. 'Relevant offences' are: (1) 'priority' offences specified in schedules 5 to 7, such as terrorism offences and offences related to child sexual exploitation and abuse (CSEA); and (2) 'non-priority' offences, covering any other offence targeting individuals (subject to certain exclusions relating to intellectual property and consumer protection offences). In total, the OSA lists over 130 priority offences, which Ofcom's guidance sub-divides into 17 broad content categories (such as: sexual exploitation of adults, human trafficking, unlawful immigration, fraud and financial offences, and drugs and psychoactive substances). Ofcom's guidance also identifies a small number of non-priority offences that providers are likely to encounter (including 'cyberflashing' and false communications).
-

In addition to illegal content, sections 60 to 62 of the OSA define various categories of user-generated 'content that is harmful to children'. This comprises: (1) specified types of 'primary priority' content, including pornographic content, suicide and self-harm content and eating disorder content; (2) specified types of 'priority' content, such as bullying content, violent content, and dangerous stunts and challenges content; and (3) 'non-designated' content, which is any other type of content that presents a 'material risk of significant harm' to an 'appreciable' number of children, and can include content related to depression or content that shames or otherwise stigmatises body types or physical features. Such content may or may not be illegal.

- Finally, section 79 of the OSA defines 'provider pornographic content' as pornographic content that is published or displayed on a service by the provider of the service, or which the provider provides the means for users to generate on the service (eg, via AI).

The OSA also includes duties relating to 'fraudulent advertisements', which are paid-for advertisements that amount to a fraud offence and that are not regulated user-generated content. However, these duties only apply to certain 'categorised' services. As no services have yet been categorised, these duties are not currently applicable.

Law stated - 18 December 2025

Online services covered

Which online services are covered under the law and how are these services defined?

The OSA covers three main categories of online services:

- 'user-to-user services', which are services that allow users to create, upload and/or share content that other users can see or otherwise 'encounter' on the service (eg, social media services);
- 'search services', which are (or include) public search engines that enable users to search content across multiple websites or databases; and
- services that publish or display pornographic content.

A service can (in effect) fall into more than one of these three categories. For example, a user-to-user service that includes a public search engine is referred to in the OSA as a 'combined' service, and must comply with the duties for both user-to-user services and search services.

Whether a service is in scope of the OSA is determined principally by whether it is a regulated type of service (ie, user-to-user, search or pornographic content provider) and whether it has 'links with the UK', for example, due to the number of UK users of the service, or due to the service targeting the UK market.

In-scope user-to-user and search services must assess whether they have (or are likely to attract) a 'significant number' of child users. If so, they will be considered 'likely to be accessed by children' and be in scope of the OSA's child safety duties.

Services that do not allow user-generated content, do not include a search engine or do not have 'links with the UK' (eg, due to a lack of UK users) are generally not 'regulated' services under the OSA. In addition, the OSA excludes certain narrowly scoped types of user-to-user and search services, such as those that function solely as internal business services.

Larger user-to-user and search services may also be 'categorised' by Ofcom, meaning that they are subject to additional duties. The possible categories are:

- Category 1: the largest and highest-risk user-to-user services, which have a content recommender system and either: (1) an average of more than 34 million monthly active UK users; or (2) an average of more than seven million monthly active UK users and the ability for users to forward or share content with other users;
- Category 2A: large search services that have an average of more than seven million monthly active UK users. Subject-specific 'vertical' search services are excluded; and
- Category 2B: user-to-user services that have an average of more than three million monthly active UK users, and which have a (private) direct messaging feature.

Ofcom is expected to implement the categorisation regime and publish the register of categorised services in summer 2026.

Law stated - 18 December 2025

Territorial scope
What is the territorial scope of the relevant law?

The OSA has a broad territorial scope with extraterritorial effect. It applies to services that have 'links with the United Kingdom', regardless of whether they are provided from within the UK or whether the provider has a UK presence. Under sections 4 and 80 of the OSA, an online service may be considered to have links with the UK if it has a 'significant number' of UK users, if the UK is a target market for the service, or if it can be used by UK users and there are 'reasonable grounds' to believe that content on the service presents a 'material risk of significant harm' to individuals in the UK.

This broad scope is designed to ensure that UK users are protected when using online services regardless of where the service provider is based.

Law stated - 18 December 2025

Codes of practice
Are there any codes of practice or other non-binding guidelines or recommendations relating to online safety in your jurisdiction?

The OSA requires Ofcom to produce various non-binding guidelines and codes of practice (COPs). These provide detailed regulatory guidance on how Ofcom considers that providers should comply with their duties under the OSA.

The guidelines cover areas such as: how providers should conduct risk assessments for illegal content and content that is harmful to children; how providers should determine

whether a particular piece of content is illegal or harmful to children; and standards that should be met by providers that implement age assurance (eg, in order to protect children from regulated provider pornographic content or other content harmful to children).

The COPs set out 'recommended' measures for providers to comply with their illegal content and child safety duties. The scope of each measure differs; some apply to all services of a particular type (eg, all user-to-user services), while others may only apply to services that meet additional criteria (eg, where the service's risk assessment has identified a medium or high risk of a particular type of content).

Providers are not required to implement the measures that are recommended for their service, and can choose to adopt appropriate alternative measures to comply with their duties. However, the COPs provide a 'safe harbour' – if providers do implement all the recommended measures that apply to their service, they are automatically deemed to comply with the duties to which those measures relate, such as the duty to have 'proportionate' measures in place to mitigate the risks of illegal and harmful content.

Law stated - 18 December 2025

Harmful versus illegal content

How does the law in your jurisdiction distinguish between harmful and illegal content?

The OSA's duties regarding illegal content apply to content that amounts to a specified 'priority' offence or (for some duties) that amounts to a 'non-priority' offence. The OSA's duties regarding harmful content only apply to content that is harmful to children, including specified types of 'primary priority' and 'priority' harmful content, other 'non-designated' harmful content and regulated provider pornographic content.

Some content that is harmful to children may also be illegal. For example, content that encourages suicide is a type of 'primary priority' harmful content, and may also be a 'priority' offence. However, there is no requirement for content to be illegal in order to be considered harmful to children – legal content will also be captured.

The OSA does not define, or impose any duties relating to, types of legal content that are harmful to adults.

Law stated - 18 December 2025

Extremist and terrorism-related content

How does your jurisdiction regulate the dissemination of extremist and terrorism-related content online?

The OSA defines 'terrorism content' by reference to specific terrorism-related offences that are set out in Schedule 5 of the OSA, including the dissemination of terrorist content (which is an offence under section 2 of the Terrorism Act 2006).

The OSA designates terrorism content as a type of 'priority' illegal content. As with other types of priority illegal content under the OSA, this means that providers must comply with

various duties to deal with such content, including duties to: (1) assess the risk of harm that terrorism content presents to users on their service; and (2) implement measures, systems and processes to mitigate this risk (eg, by preventing individuals from encountering terrorism content and swiftly taking it down when identified).

Ofcom's illegal content COPs recommend measures to comply with these duties, including certain measures specific to terrorism content – for example, to remove accounts from a service if there are reasonable grounds to infer that the account is operated by or on behalf of a group or organisation proscribed under the Terrorism Act 2000. Ofcom's guidance on 'illegal content judgements' assists providers with making such inferences and contains guidance to help providers determine whether a given piece of content constitutes terrorism content and should be removed from their service.

Reflecting the seriousness with which the OSA treats terrorism content, Chapter 5 of Part 7 of the OSA gives Ofcom an additional power specific to terrorism content. This enables Ofcom to require a provider to use accredited technology to proactively identify and deal with terrorist content that is publicly communicated on the service (eg, by preventing users from encountering such content and taking it down where identified).

Finally, entities that are proscribed as terrorist organisations under the Terrorism Act 2000, or that have the purpose of supporting such an organisation, are excluded from the OSA's definition of 'recognised news publisher'. This means that they do not benefit from the additional freedom of speech protections accorded to content from such publishers.

In addition, a provider may receive a notice from law enforcement under section 3 of the Terrorism Act 2006, requiring an item of terrorist content on its service to be taken down. If the provider fails to do so within two working days of receiving the notice or subsequently fails to prevent repeat publication of the content, the provider can itself be liable for disseminating terrorist content under section 2 of the Terrorism Act 2006.

Law stated - 18 December 2025

Disinformation versus misinformation

How, if at all, does the law in your jurisdiction distinguish between misinformation and disinformation online? Does it include malinformation?

The OSA does not expressly define or address misinformation, disinformation or malinformation. However, such content may fall within categories of illegal or harmful content that are regulated under the OSA.

For example, the 'foreign interference' category of priority illegal content relates to content amounting to a foreign interference offence under section 13 of the National Security Act 2023. This offence can apply to certain activities intended by the perpetrator to have a harmful 'interference effect', such as activities carried out by or on behalf of a foreign power and that could undermine the safety or interests of the UK. This can include misrepresentation of a person's identity or purpose, or state-backed disinformation campaigns.

The OSA also introduces a criminal offence of knowingly sending false information with intent to cause non-trivial psychological or physical harm. This could apply to

certain deliberate harmful disinformation, but would not include, for example, inadvertent misinformation.

Law stated - 18 December 2025

OBLIGATIONS FOR ONLINE SERVICE PROVIDERS

General obligations

What general legal obligations relating to safety are imposed on providers of online services, including providers of online intermediary services?

Providers of in-scope user-to-user services and search services are subject to duties relating to illegal content, and may be subject to similar duties relating to content harmful to children. These duties require the provider to conduct annual risk assessments relating to illegal content and content that is harmful to children, and to implement various measures, systems and processes to deal with such content and the risks posed to users. These duties relate to all aspects of the service, including its design, operation and use, as well as content present on the service.

Providers of services that contain regulated provider pornographic content, and providers of user-to-user services that permit any type of 'primary priority' content harmful to children, are also required to use 'highly effective' age assurance measures to ensure that children cannot access such content.

Additional obligations also apply to categorised services, depending on the category. For example, all categorised services must provide the Office of Communications (Ofcom) with annual 'transparency reports' setting out information about their service that is specified by Ofcom, such as the incidence of illegal content and the measures that are in place to comply with applicable duties. Category 1 services are subject to more onerous requirements. For example, they are required to give users the option to verify their identity, and provide tools to limit exposure to certain content, features and unverified users. They are also required to take additional steps to protect the free expression of 'content of democratic importance' and 'journalistic content' on their service.

Law stated - 18 December 2025

Risk assessments and mitigation

Are there any specific legal obligations for online service providers to conduct risk assessments and mitigate risks to safety?

Providers must conduct a 'suitable and sufficient' illegal content risk assessment regularly (at least annually), and prior to making a 'significant change' to their service, such as significant updates to the design of user-facing algorithms, systems and processes. They must also keep their risk assessments up to date, including to reflect any significant changes made by Ofcom to the 'risk profile' guidance that is relevant to the service.

Illegal content risk assessments involve assessing the risk level of each of the 17 categories of priority illegal content, and of any types of non-priority illegal content that are likely to occur on the service. Assessing the risk level requires the provider to assess the likelihood of each

kind of illegal harm taking place, and the impact of that harm on users. The assessment should be based on relevant information and evidence, including Ofcom's 'risk profiles' for different types of services, the characteristics, design and operation of the service, and how it is used. Ofcom has produced detailed guidance addressing how and when such risk assessments should be carried out, and how they should be recorded, to help providers comply with these obligations.

Services in scope of the child safety duties must carry out a 'suitable and sufficient' children's risk assessment. This is similar to an illegal content risk assessment, but relates to content that is harmful to children, and requires providers to consider the risk level that such content poses to children specifically (including how this risk may differ for children in different age groups). Ofcom has produced separate guidance relating to children's risk assessments.

A risk assessment will result in each type of content being assigned a risk level (high, medium, low or negligible/no risk). Providers must then identify and implement 'proportionate' mitigation measures, which may include content moderation. What is 'proportionate' for a particular service and particular type of content will depend on the risk level assigned to that content, as well as the provider's size and capacity. Ofcom's codes of practice (COPs) relating to illegal content and content harmful to children set out Ofcom's recommended mitigation measures. A provider that adopts all of the recommended measures applicable to its service will automatically be deemed to have 'proportionate' mitigation measures in place.

Law stated - 18 December 2025

Protection of minors and age verification

Are there any specific legal obligations to protect minors online? If so, what measures are required or advised, such as age verification?

Providers of user-to-user and search services that are likely to be accessed by children must: (1) conduct regular (at least annual) children's risk assessments; and (2) based on the outcome of these assessments, implement 'proportionate' child safety measures to address the risks of children encountering harmful content on their service. Ofcom's recommended measures are set out in the child protection COPs.

For providers of user-to-user services that permit any type of 'primary priority' content harmful to children (and providers of any service that contains regulated provider pornographic content), these measures are required to include 'highly effective' age assurance to ensure that children cannot access such content.

Ofcom recommends other measures in its child protection COPs. These include recommendations for certain other providers to implement highly effective age assurance, including providers that permit any kind of medium or high risk 'priority' content harmful to children, and providers that prohibit – but are unable to take down – 'primary priority' and 'priority' content harmful to children. Other recommended measures relate to governance and accountability, content moderation, reporting and complaints, recommender systems, settings and user controls, and terms of service.

In addition, Chapter 5 of Part 7 of the Online Safety Act 2023 (OSA) gives Ofcom a specific power to deal with CSEA content. As with the equivalent power relating to terrorism content,

this enables Ofcom to require a provider to use accredited technology to proactively identify and deal with CSEA content (eg, by preventing users from encountering such content, and taking it down where identified). Unlike the terrorism-related power, which is limited to publicly communicated content, this power extends to CSEA content that is privately communicated.

Law stated - 18 December 2025

Civil and human rights

Are there any obligations for online service providers to balance civil and human rights, such as privacy rights and freedom of expression, with safety regulations? If so, what measures are required or advised?

The OSA explicitly requires providers of regulated user-to-user services to have particular regard to the importance of protecting users' rights to freedom of expression and privacy when deciding on and implementing safety measures. Ofcom's COPs include recommended measures that act as safeguards for users' freedom of expression and privacy.

Category 1 user-to-user services must also assess the impact of their planned or implemented safety measures on such rights, both before and after these measures are implemented. The assessment must be published and kept up to date, and the provider must publish a statement explaining the positive steps taken to protect such rights in response to the assessment.

Law stated - 18 December 2025

Disinformation and misinformation

Are there any specific legal obligations to combat disinformation and misinformation online? If so, what measures are required or advised?

The OSA does not expressly define or address disinformation or misinformation. To the extent that such content is illegal or falls within a particular category of content harmful to children, it will be subject to the OSA's duties regarding such content. For example, where a provider has reasonable grounds to infer that an item of content constitutes illegal disinformation, the content should be swiftly taken down (as with other types of illegal content).

Law stated - 18 December 2025

Notice and takedown

Is there a legislative 'notice and takedown' mechanism or similar in your jurisdiction? If so, how does it operate?

The OSA requires providers to operate their services using proportionate systems and processes that are designed to minimise the length of time for which illegal content remains online and to swiftly take down illegal content once it is identified. Providers of services likely

to be accessed by children are not explicitly required to take down content harmful to children but may do so where such content is prohibited by their terms of service.

In addition, the OSA requires providers to have systems in place that allow users to easily report content which they consider to be illegal or harmful to children.

Taken together, these duties function in a similar way to a 'notice and takedown' system for illegal content and any content harmful to children that is prohibited on a service.

In addition, regulation 19 of the Electronic Commerce (EC Directive) Regulations 2002 (the E-Commerce Regulations) provides hosting providers with a defence against liability, provided that once they are on notice of illegal content, they remove it expeditiously.

Law stated - 18 December 2025

ENFORCEMENT AND PENALTIES

Enforcement
How is the online safety regime enforced in your jurisdiction?

The Office of Communications (Ofcom) is the independent regulator responsible for overseeing compliance with the Online Safety Act 2023 (OSA). It has wide-ranging statutory powers to monitor, investigate, and enforce the OSA's provisions against providers of regulated online services.

The majority of these powers are exercisable by Ofcom without court approval. However, for severe or persistent non-compliance, the OSA empowers Ofcom to seek a 'service restriction order' or 'access restriction order' from the courts (on an interim or permanent basis). Such orders can require search engines, payment providers, advertisers, internet service providers and similar 'ancillary services' to stop working with or block access to non-compliant services in the UK, effectively cutting off access and revenue.

Law stated - 18 December 2025

Authorities
Which authorities are responsible for enforcement? What is the basis, nature and extent of their enforcement powers?

Ofcom has a range of enforcement powers under the OSA, designed to enable it to regulate online service providers effectively and ensure user safety.

These powers include: (1) obtaining information via various means (including compulsory information notices, investigations and interviews), which may be used to identify and investigate potential non-compliance; (2) imposing substantial fines for non-compliance of up to £18 million or 10 per cent of a provider's qualifying worldwide revenue (QWR), whichever is greater; (3) requiring the provider to take specified steps in order to remedy any non-compliance; and (4) 'business disruption measures', in the form of a service or access restriction order.

In addition, certain breaches of the OSA can result in criminal liability for providers and individuals. For example, a provider may be criminally liable for failing to comply with an information notice. If the notice required the provider to name a senior manager, and that senior manager failed to take all reasonable steps to prevent the provider's non-compliance, the senior manager will also be criminally liable. Where there is criminal liability, Ofcom can pursue prosecutions, which may result in fines and/or imprisonment.

Ofcom uses a priority framework to determine when and how to take enforcement action, having regard to factors such as the seriousness or risk of harm of the alleged non-compliance, the strategic significance of addressing such non-compliance (eg, whether it relates to Ofcom's broader strategic goals or is an opportunity to clarify the legal framework), and the resources required. In some cases, Ofcom may decide to take alternative steps – such as sending a warning letter, or accepting assurances that a provider has addressed or will address the non-compliance – rather than pursuing a formal investigation and enforcement action.

Law stated - 18 December 2025

Penalties and liability

What are the potential fines or penalties for non-compliance? Are there risks of liability for employees or directors of online service providers?

Ofcom can impose penalties on providers and other persons of up to £18 million or (for providers) 10 per cent of their QWR, if greater. QWR refers to the total global revenue attributable to the relevant parts of a regulated service, meaning parts on which regulated user-to-user content, search content, or provider pornographic content may be encountered. A provider's group companies and/or controlling individuals (eg, a majority shareholder) can be made jointly and severally liable for such penalties.

Providers may also be subject to criminal liability in certain circumstances – for example, where they fail to provide information required by an information notice – and can be subject to an unlimited fine if convicted.

Employees and directors of a provider can be subject to civil penalties, up to a maximum of £18 million, in certain circumstances – for example, if Ofcom issues an information notice to them (in their personal capacity) and they do not provide the required information.

There are also situations in which individuals may face criminal liability. In particular, a 'named senior manager' can face criminal liability for a provider's failure to comply with an information notice, as discussed above. Individual directors and employees can also be criminally liable if they obstruct the response to an information notice (eg, by destroying or altering documents) or otherwise fail to comply with Ofcom's investigative powers, or if they have some involvement in an offence committed by the provider (eg, if a director consents to a provider's decision not to comply with an information notice). Prosecution can result in fines or imprisonment.

Law stated - 18 December 2025

DISPUTES

Claims

What claims relating to online safety are available and most common in your jurisdiction?

The Online Safety Act 2023 (OSA) is the primary statutory regime for online safety in the UK, establishing a broad framework of duties for online service providers and empowering the Office of Communications (Ofcom) to enforce compliance through regulatory and court-based mechanisms.

However, unlike other jurisdictions' online safety regimes, such as the EU's Digital Services Act, the OSA does not create a general private right of action for individuals harmed by online content or by a provider's failure to comply with its duties. Enforcement is primarily regulatory, with Ofcom as the central authority.

Although private civil claims by individuals against online service providers for breach of statutory duty under the OSA are not generally available, individuals may still bring claims involving online safety under other legal bases, including torts such as defamation, and breach of contract. Section 72 of the OSA includes requirements for providers to inform users, via 'clear and accessible' provisions in their terms of service, about their right to bring a claim for breach of contract if the provider, in breach of its own terms of service, takes action against the user's content or ability to use the service.

The OSA constitutes a distinct regulatory framework that primarily targets the systemic management of online harms, rather than the liability for individual items of content. However, the E-Commerce Regulations remain in force in the UK and continue to provide liability protections for intermediary service providers, including online platforms, in relation to specific pieces of content, in connection with activities such as hosting.

These two regimes are not mutually exclusive and can operate in parallel. The E-Commerce Regulations focus on the circumstances in which platforms may be exempt from liability for third-party content, while the OSA imposes broader obligations on platforms to implement processes and systems to protect users from harm.

Accordingly, the types of potential court claims relating to online safety in the UK are generally split between:

- regulatory enforcement actions by Ofcom under the OSA, including court applications for service restriction orders and proceedings to enforce penalties; and
- civil or criminal claims against intermediaries for failure to act upon notice of illegal content, based on the principles established in case law and earlier regulations.

Law stated - 18 December 2025

Procedure

What is the procedure for claimants to bring actions relating to online safety in your jurisdiction?

The OSA does not provide a specific private right of action for individuals or organisations to directly bring claims against online service providers for failing to comply with their duties

under the OSA. Individuals can bring related claims under other legal bases (including breach of contract or torts such as defamation) through the courts.

Law stated - 18 December 2025

Remedies

What interim and substantive remedies may be imposed in relation to online safety claims?

For private claims in the UK courts relating to online safety – such as defamation, negligence or breach of contract – courts may impose both interim remedies (notably injunctions to prevent ongoing harm) and substantive remedies (including damages, orders for removal of content, publication of judgment summaries and other appropriate relief). The remedies available depend on the cause of action and the facts, but the courts have a broad range of powers to address harm caused by online conduct.

Law stated - 18 December 2025

Defences and exemptions

Does your jurisdiction provide any defences or exemptions from liability for online safety claims? If so, how do they operate and which online services providers may avail of them?

Following the coming into force of the OSA, the E-Commerce Regulations remain in force in the UK and continue to provide liability protections for intermediary service providers, including online platforms, in relation to specific pieces of content, such as those hosted by the platform. While the OSA introduces new duties for platforms to address illegal and harmful content, it does not repeal the E-Commerce Regulations, meaning the existing liability protections still apply. In particular, the E-Commerce Regulations provide a 'safe harbour' exemption for hosting providers that act expeditiously to remove unlawful content upon obtaining knowledge of it.

However, platforms must now comply with both regimes, balancing the new proactive obligations under the OSA with the conditional liability protections under the E-Commerce Regulations.

Law stated - 18 December 2025

UPDATE AND TRENDS

Key trends and future developments

What are the most noteworthy recent trends and developments in online safety regulation in your jurisdiction? What developments are expected in the coming year?

The Online Safety Act 2023 (OSA) has driven several significant trends and developments in UK online safety regulation over the past year, with further changes expected in the near

future. The Act represents a major transformation, placing the Office of Communications (Ofcom) at the centre of a new regulatory regime that imposes comprehensive duties of care on online platforms. Notable recent trends include the transition of video-sharing platforms from the Communications Act 2003 to the OSA, ending the previous dual regulatory regime and subjecting these platforms to the new safety duties. Ofcom has made substantial progress in its phased implementation 'roadmap', and the legislation is now largely in force. Enforcement activity has begun, with Ofcom targeting pornography providers that have failed to implement robust age verification measures, and there is a clear move towards requiring providers to use technology proactively to protect users – particularly as informed by annual risk assessments. Ofcom is already updating its codes of practice and regulatory guidance, reflecting the need for the regime to adapt to emerging risks, evolving online behaviours, and rapid technological change.

A particularly significant upcoming development is the establishment of the register of categorised services, which is overdue; it was previously planned for summer 2025, but is now expected in summer 2026. Once issued, the register will formally identify which services fall into Categories 1, 2A and 2B, triggering the application of additional requirements for those services. This will mark a shift for the largest services from general compliance requirements to more specific and onerous obligations. Alongside this, the introduction of a fee regime based on qualifying worldwide revenue will require larger providers to contribute a proportionately greater amount to Ofcom's regulatory costs, and failure to comply with notification or payment requirements can result in substantial penalties. Another emerging trend is the increasing focus on transparency and accountability, with providers expected to maintain clear reporting and complaints procedures, and to demonstrate ongoing risk mitigation efforts.

In the coming year, providers should expect these trends to continue and potentially accelerate. Ofcom is likely to ramp up its enforcement activity, setting the tone for future regulatory action under the OSA, especially in the adult content sector and in relation to content harmful to children. There is likely to be heightened scrutiny of providers' technological solutions, including the use of AI and automated moderation tools, and a growing emphasis on regular risk assessments and user empowerment features. The regulatory landscape will continue to evolve, with Ofcom refining its codes of practice and guidance to address new risks and advances in technology, and a clear focus on accountability, transparency, and the protection of children and vulnerable users. Finally, as they become increasingly advanced and ubiquitous, we expect to see Ofcom grapple more directly with regulating AI chatbots and other generative AI systems.

Law stated - 18 December 2025