

# Ofcom's approach to implementing the Online Safety Act

---

[Welsh translation available](#)

**Document**

Published 26 October 2023



# Contents

---

## Section

Our approach .....	3
Updated roadmap.....	11

# Our approach

## About the Online Safety Act

---

### With Royal Assent of the Online Safety Act, Ofcom's powers as online safety regulator have commenced

Many of today's most widely used and best-loved online services are user-to-user services. These include social media, photo and video-sharing services, chat, and instant messaging platforms, online and mobile gaming, and video calling.

These services have created great benefits: open communication, the ability to share videos and photos from anywhere to anyone, new forms of community and instant interaction.

But with these benefits come new risks of harm and illegality, including the use of online services to enable child sexual exploitation and abuse; to disseminate terrorist content and incite hate; to commit fraud; or to allow children to seek or stumble upon content that may be harmful to them.

The UK Online Safety Act 2023 ('the Act') makes companies that operate a wide range of online services (including user-to-user services, search services and pornography services<sup>1</sup>) legally responsible for keeping people, especially children, safe online. This document summarises the key actions companies must take under the Act and explains what Ofcom will do to achieve compliance. It also sets out the outcomes we expect the new rules to deliver.

### We are moving quickly to implement the new rules

We are publishing our first consultation on illegal harms on 9 November 2023. This will contain proposals for how services can comply with the illegal content safety duties and draft **Codes of Practice**.

This is the first of three phases, established by the Act:

- Duties regarding Illegal Harms
- Duties regarding Protection of Children, including from access to pornography
- Duties on 'Categorised' services – i.e., those that meet certain criteria related to their number of users or risk of harm – including to publish transparency reports and empower users to control the content they see<sup>2</sup>

The updated roadmap in the final section of this document explains when we will publish further information and proposals in each of these phases.

---

<sup>1</sup> See Illegal Harms Consultation (November 2023) for a detailed explanation about which services are covered by the legislation.

<sup>2</sup> Criteria for categorisation will be set by the Government in secondary legislation. Once this has happened, Ofcom will decide what services meet these thresholds, and add them to a public register. If a service is not included on this register, they will not have to comply with these additional obligations. We expect that most of the 100,000 in-scope services will *not* be categorised.

## Companies need to assess and manage risks to people's online safety

The Act places duties on companies to assess and manage safety risks arising from content and conduct on their sites and apps. It does not expect harmful and illegal content to be eradicated online, but it does expect services to have suitable measures to keep adults and children in the UK safe. A key aspect of these rules is that they seek changes in services' systems and processes. The presence of harmful or illegal content will not, in itself, establish whether the service has complied with its duties under the Act.

Once the new rules take effect, all in-scope user-to-user and search services, large or small, will need to take action to comply with the new duties. While the precise duties vary between services,<sup>3</sup> most service providers will need to:

- carry out risk assessments, to assess the risk of harm to all users from illegal content and (if a service is likely to be accessed by children<sup>4</sup>), to children, from content harmful to them;
- take effective steps to manage and mitigate the risks identified by these assessments;
- be clear in their terms of service about how users will be protected;
- provide means for users easily to report illegal content and content harmful to children; and for them to complain, including when they believe their posts or account have been wrongly blocked or removed; and
- consider the importance of protecting free expression and privacy, in meeting their new duties.

Providers of online services that publish or display pornography must take steps to ensure children cannot normally access this content.

## The onus is on companies to decide what safety measures they need given the risks they face

Our initial analysis suggests more than 100,000 online services could be subject to the new rules. Organisations ranging from very large and well-resourced companies to small and micro-businesses, in a wide range of sectors, will need to assess what safety measures they need to comply with the new rules, based on the risks they face. All services with a significant number of UK users, or targeting the UK market, are in scope, regardless of where they are based.<sup>5</sup>

The Act recognises that in-scope services are very different, in their size, resources and the risks they pose to people in the UK. Different safety measures will be appropriate for different types of service and our recommendations will vary for services depending on their size and degree of risk. The Act is clear: first and foremost, the onus sits with service providers themselves, to properly assess the risks their users may encounter, and decide what specific steps they need to take, in proportion to the size of the risk, and the resources and capabilities available to them.

As the recent rapid rollout of generative AI illustrates, the sectors the Act tasks Ofcom with regulating are dynamic and fast paced, meaning that the questions that we will need to answer as a regulator will constantly evolve. We will need to strike an appropriate balance, intervening to protect users from harm where necessary, while ensuring that regulation appropriately protects

---

<sup>3</sup> See the Illegal Harms Consultation (November 2023) for a detailed discussion of compliance requirements related to the Illegal Harms duties in the Act.

<sup>4</sup> I.e., under-18s.

<sup>5</sup> These criteria are set out in the Act. The Illegal Harms Consultation (November 2023) will provide some further information about scope.

privacy and freedom of expression, and promotes innovation. We will focus on the services and features that pose the greatest risk of harm to UK users.

## How we will achieve the goals of the Act and support services to comply

---

### We expect industry to work with us, and we have powers to enforce compliance where necessary

We will use our powers and duties under the Act to protect adults and children in the UK, by ensuring services take suitable steps to keep people safe.

Our role is not to instruct firms to remove particular pieces of content or take down specific accounts, nor to investigate individual complaints.<sup>6</sup> Our role is to tackle the root causes of online content that is illegal and harmful for children, by improving the systems and processes that services use to address them. Seeking systemic improvements will reduce risk at scale, rather than focusing on individual instances.

The Act gives us several means of driving improvements in online safety.

**First, we will provide resources to help companies manage risk.** These include:

- analysis of the causes and impacts of online harm, to support services in carrying out their risk assessments;<sup>7</sup>
- guidance on a recommended process for assessing risk; and
- codes of practice, setting out what services can do to mitigate the risk of harm.

Our initial Code of Practice on Illegal Harms will recommend services adopt protections to address all types of illegal content covered by the Act.<sup>8</sup> In addition, the draft Codes will recommend some targeted measures against some of the most egregious illegal harms. These protections include clear, detailed, proportionate and technically feasible measures that services should consider taking, in areas such as content moderation, user reporting and complaints, service design features, governance and terms of service.

Services will not be required to follow the recommendations in our Codes, but if they do, they will be deemed to have complied with the relevant legal duties. If they choose to use other measures, they will need to be able to explain how their chosen approach meets the duties in the Act.

**Second, we will drive industry improvements by engaging with the largest and riskiest services via continuous regulatory supervision.** ‘Supervision’ is a mode of engagement that has proven successful in several regulatory fields, particularly in financial services regulation.<sup>9</sup> Specifically, it involves regularly engaging with the services with the largest impact on UK internet users, including where necessary by making formal and enforceable requests for information, allowing the regulator to:

---

<sup>6</sup> However, we will use complaints to help us assess whether regulated services are appropriately protecting their users.

<sup>7</sup> Described in the Act as Ofcom’s ‘register of risks’.

<sup>8</sup> See Illegal Harms Consultation (November 2023)

<sup>9</sup> Financial Conduct Authority (FCA), April 2019. [FCA Mission: Approach to Supervision](#) [accessed 18 October 2023].

- understand the nature of harms on those services, the mitigations that are already in place to tackle them, and the risk assessment and governance processes that the service has adopted;
- assess the effectiveness of their safety measures, considering the specific circumstances of the individual service (including its risk levels, size, and capacity); and
- where appropriate, work with the service to secure improvements in those measures.

Our regulation of video-sharing platforms (VSPs) has identified that even the biggest services have room for improvement, for example in the content of their user policies and the ways they communicate them.<sup>10</sup> We expect innovation to enable further improvements in online safety over time, including the development of new technologies to mitigate harm. For example, our involvement in the AI and Digital Hub being launched by the Digital Regulation Cooperation Forum (DRCF) aims to provide support for innovators working at the intersections of online safety and other areas such as privacy.<sup>11</sup>

We will also provide information and support to smaller services and start-ups. We are developing plans for digital tools to help small and medium-sized enterprises (SMEs) – who comprise the majority of in-scope services – comply with the regime, including support for firms in determining whether the rules apply to their service, responding to requests for information, and understanding enforcement processes.

**Third, we will assure compliance by using our investigation and enforcement powers when it is the most effective way of protecting the public.** While our preference is to work with services to encourage voluntary compliance, we will, if necessary, launch enforcement action where we determine that a firm is not complying with its duties, for example where we consider it is not taking appropriate steps to protect users from harm. To support our investigations, we have powers to request information and obtain skilled person’s reports.

Where we identify compliance failures, we can impose fines of up to £18m or 10% of qualifying worldwide revenue (whichever is greater). In the most serious cases of non-compliance, we can seek a court order imposing business disruption measures, which may require third parties (such as providers of payment or advertising services, or ISPs) to withdraw, or limit access to, their services in the UK. Furthermore, service providers may commit a criminal offence if they fail to comply with an information notice or if they fail without reasonable excuse to take compliance action which is specified in an Ofcom decision finding that the service is in breach of certain duties relating to CSEA and child safety. In such cases, directors and other senior managers of the provider may also be criminally liable for the failures.

While we will use our enforcement powers in a proportionate, evidence-based and targeted way, these powers are vital to ensure we can take effective action when necessary to protect users. We explain below when we expect the relevant duties to come into effect once our final guidance and codes become enforceable.

**Finally, we will hold services to account, by using transparency to shine a light on safety matters, share good practice, and highlight where improvements can be made.** The Act gives Ofcom wide-ranging powers to require certain services to be more transparent about their trust and safety measures, including how they evaluate the impact of these measures, and their implications for user rights and freedoms.

---

<sup>10</sup> Ofcom, October 2022. [Ofcom’s first year of video-sharing platform regulation](#) [accessed 18 October 2023].

<sup>11</sup> UK Government, September 2023. [UK Government Advisory Services to Help Businesses Launch AI](#) [accessed 18 October 2023].

## Protecting fundamental rights

As a public body, Ofcom must act compatibly with the European Convention on Human Rights (ECHR). We will ensure our approach to regulation upholds the importance of fundamental rights, in particular the rights to freedom of expression and privacy. We have and will continue to assess the potential impact of our proposals and propose to intervene only in ways which do not unduly interfere with rights.

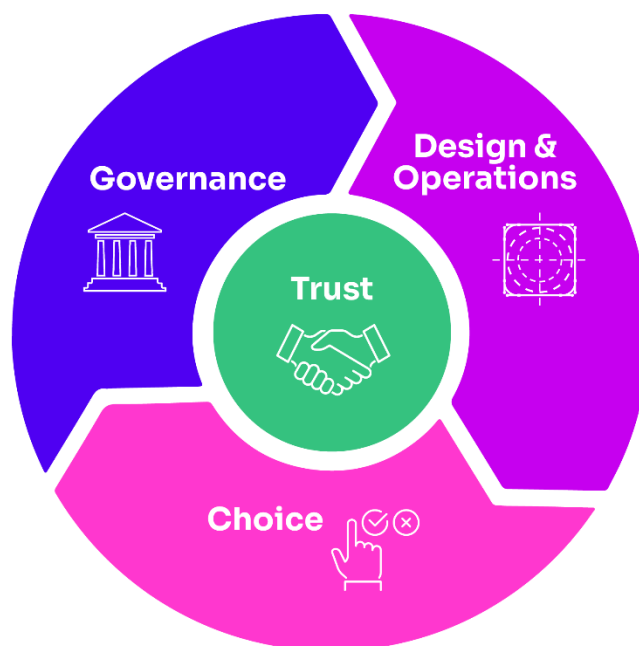
## We expect change

Our assessment, published as part of the consultation on Illegal Harm, shows that illegal and harmful online content and conduct continue to present a severe risk of harm. Children may be particularly vulnerable. While regulation is only one aspect of a broad and complex national and global ecosystem of online safety endeavours (see below), it has a particular role to play: the unique powers granted to Ofcom by the Act enable us to hold online services to account for user safety in the UK, and we expect change.

Specifically, we anticipate implementation of the Act will ensure people in the UK are safer online by delivering four outcomes (Figure 1):

- stronger safety **governance** in online firms;
- online services **designed and operated with safety in mind**;
- **choice** for users so they can have meaningful control over their online experiences; and
- transparency regarding the safety measures services use, and the action Ofcom is taking to improve them, in order to build **trust**.

**Figure 1: Key outcomes**



## Key outcome 1: Stronger governance

In response to our proposals regarding risk assessment and governance,<sup>12</sup> we want to see firms improve how they understand and prioritise the risk of harm, and build the structures, culture, and processes needed to embed user safety in strategic and day-to-day decisions. In the biggest services, we expect to see user safety represented at all levels of the organisation – from the Board down to product and engineering teams.

## Key outcome 2: Designing and operating services with safety in mind

We expect all services to have appropriate trust and safety measures tackling the full range of harms listed in the Act. We particularly want to see improvements in, and wider deployment of, measures to address areas of greatest potential risk to people, especially children:

- child sexual exploitation and abuse, including grooming;
- online terrorism;
- incitement to hatred;
- fraud and scams;
- underage access to pornography; and
- protection of children from legal content that may be harmful to them, for example material regarding eating disorders, self-harm, and suicide.

In line with the Act, we will have a particular focus on content and activity with a disproportionately negative impact on women and girls, and produce guidance on this.

In recent years, several notable technological innovations have been developed and deployed to reduce the risk of harm. Many services use automated tools, or classifiers, to identify and remove illegal and harmful content, albeit typically with ongoing human oversight.<sup>13</sup> However, no such tool is perfect, and the choice to use them involves a trade-off between the benefits of removing harmful material, and their limitations, including the risk of erroneous takedown of legitimate material, and the implications for privacy.

Given these risks, while automated tools have an essential role to play in mitigating risks to online safety, our aim is to promote the use of tools that are sufficiently accurate, effective, and lacking in bias to perform their intended function, and which do not have disproportionate impacts on freedom of expression and privacy. We want firms to assess their automated content moderation tools with respect to these tests and will consider how they can be more transparent about how they use these tools, and their effectiveness.

## Key outcome 3: Choice for users

The Act also expects that services enable users to have more choice and control when navigating their online experience.<sup>14</sup> We will look to ensure the biggest and riskiest services provide users with the tools to better understand their choices online, and the ability to adjust the content they see and who they interact with online. Empowering UK users to have more control and choice online will also contribute to the protection of users' right to freedom of expression online. In developing our policy in this area, we will draw on insights from Ofcom's substantial body of behavioural insights research

---

<sup>12</sup> See the Illegal Harms Consultation (November 2023).

<sup>13</sup> Ofcom, January 2023. [Automated Content Classification Systems](#) [accessed 18 October 2023].

<sup>14</sup> Ofcom has duties under section 11 of the Communications Act 2003 to promote and carry out research into media literacy. These duties have been amended by the Online Safety Act to give Ofcom new responsibilities to increase media literacy in connection with the use of regulated services.



and our long-standing Making Sense of Media (MSOM) programme, which helps improve the online skills, knowledge and understanding of UK adults and children.<sup>15</sup>

## Key outcome 4: Transparency to drive trust

Our final outcome is to promote transparency, to ensure this regulatory framework is trustworthy and trusted by all stakeholders. There are three dimensions of this.

First, transparency about services' safety measures. We know that many stakeholders, and users, feel that online services are opaque and their safety measures, and decision-making processes are unclear. While many companies have launched transparency reports in recent years, these could go further in shedding light on the actions they take to protect users. Our VSP report is one of the first comprehensive assessments by a regulator, identifying the trust and safety measures that notified VSPs employ to protect users – particularly children – from harm.<sup>16</sup> Additionally, our report on the livestreaming of the terrible shooting in Buffalo, New York in May 2022 provided independent analysis of how this footage came to spread across the Internet, identified lessons learned since the similar livestreaming of the Christchurch atrocity in 2019, and recommended ways to strengthen industry collaboration to further manage risks.<sup>17</sup>

Second, Ofcom's own transparency. Independent research has found that when regulated firms and other stakeholders share the purpose of regulation and see it as fair and effective, they are more likely to support its implementation and contribute to achieving its goals.<sup>18</sup> Ofcom is accountable to Parliament and to the public, and we have always been committed to being fully transparent in our work as a regulator. We will seek to build the public's confidence in the ability of regulation to deliver a safer life online by being clear about how changes are implemented across the services in scope. We will track the impact of regulation and its benefits to users.

Third, open engagement with civil society groups, academics, expert bodies, law enforcement agencies and international policymakers, to understand their perspectives, ensure our regulatory policy is informed by their expertise, and achieve shared goals. We will also ensure we have a range of means to hear the voices of users themselves, especially children.

## The Act is part of a broader national and international move to regulate online safety

---

We recognise the vital importance of ensuring coherence between the new Online Safety regime and other UK regulatory frameworks and have been working particularly closely with the Information Commissioner's Office (ICO), the Competition and Markets Authority (CMA) and the Financial Conduct Authority (FCA) under the auspices of the DRCF, established in 2020. We recognise that in tackling online safety, it is essential that users of online services have confidence that their privacy will also be protected, and that service providers comply with their obligations and can continue to innovate and grow, supported by regulatory clarity. We published a joint statement with the ICO about this in 2022 and since then, we have worked closely with them on issues such as age assurance and content moderation. We are consulting them extensively in development of our Codes and guidance to ensure that we take full account of data protection requirements and the impact of our proposals on users' privacy. We also published a joint statement with the CMA in 2022

---

<sup>15</sup> Ofcom, December 2021. [Ofcom's approach to online media literacy](#) [accessed 18 October 2023].

<sup>16</sup> Ofcom, October 2022. [Ofcom's first year of video-sharing platform regulation](#) [accessed 18 October 2023].

<sup>17</sup> Ofcom, October 2022. [The Buffalo attack: Implications for online safety](#) [accessed 18 October 2023].

<sup>18</sup> 2017, Hodges. [Outcome-Based Cooperation: In Communities, Business, Regulation, and Dispute Resolution](#).

which set out our shared view on interactions between safety and competition in digital markets. We are keen to leverage opportunities for streamlining requirements across these UK regulatory frameworks to find synergies and reduce the burden of regulatory compliance for services.

While our responsibility will be to ensure that in-scope services meet UK legal requirements, we have also built strong relationships with our counterparts in other jurisdictions and will seek to align our policy with international approaches where appropriate. As co-founders of the new Global Online Safety Regulators Network, which Ofcom will chair in 2024, we collaborate with international regulators with the aim of making the approach to online safety between countries as consistent and coherent as possible.

The new regulatory framework in the UK is one of several developments worldwide in online safety regulation, including the EU's Digital Services Act (DSA) and Australia's Online Safety Act. In working internationally, we aim to help develop a common regulatory toolkit of norms and standards that is informed by international best practice. This will ultimately help reduce compliance costs for in-scope services as we improve protections for UK internet users.

# Updated roadmap

## As the Parliamentary process has evolved, so has our timetable

---

In July 2022 we published our roadmap to regulation, setting out our overall approach as the online safety regulator.<sup>19</sup> In June 2023, we published an update on our timescales for implementing the Act.<sup>20</sup> Now that the Act has passed, we have revised our roadmap once again.

As before the new rules roll out in three phases, with the timing driven by the requirements of the Act and relevant secondary legislation. The implementation plan reflects this phased approach. We will act as swiftly as possible while also ensuring we test our work through fair and transparent consultation.

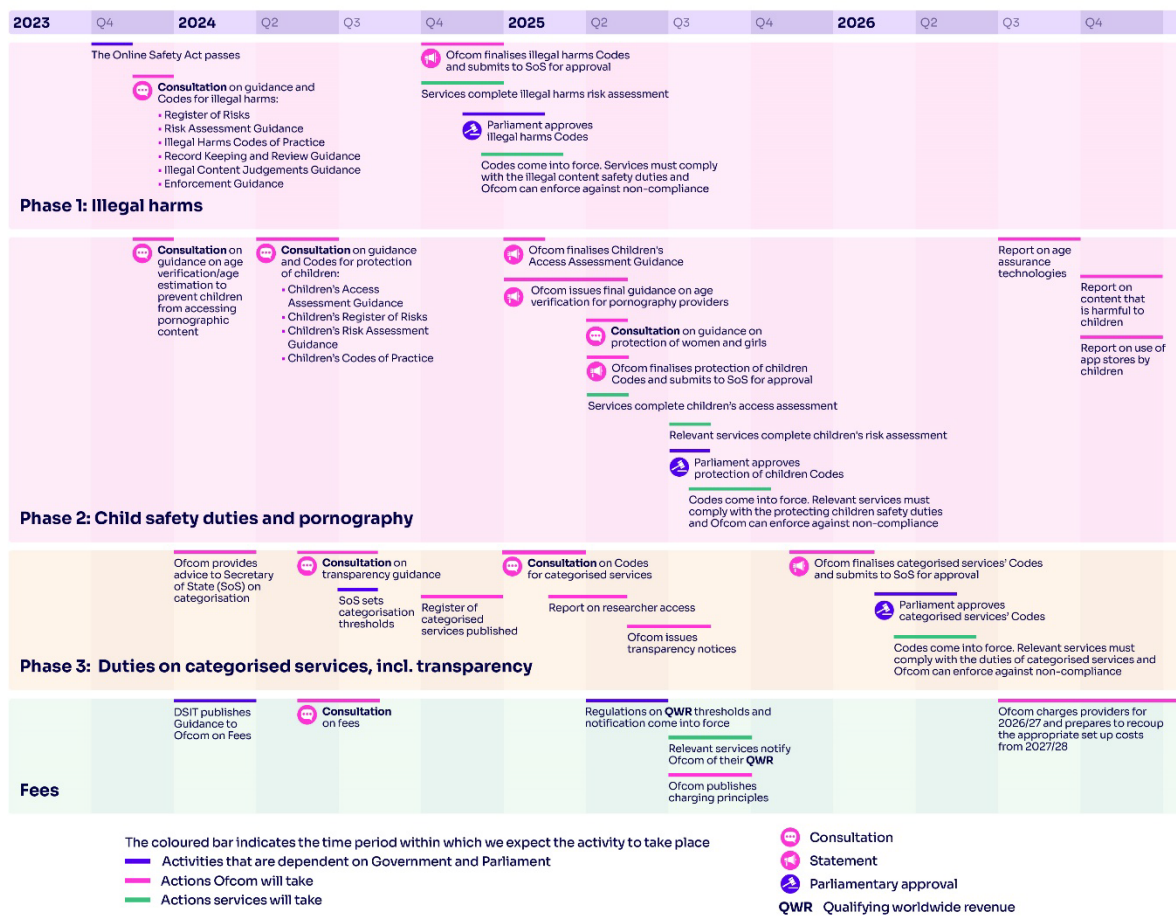
These dates reflect our current implementation plans. As we continue to engage with stakeholders and as Government puts in place necessary secondary legislation, we anticipate that some timelines may shift. There will be a General Election at some point before the end of 2024. Given uncertainty about the precise timing of the election, we have not factored that into our detailed planning, but the timetable may change once the date of the election is confirmed, given the need for secondary legislation to establish some aspects of the new rules, and the roles of the Secretary of State for Science, Innovation and Technology, and Parliament, in approving Codes of Practice.

---

<sup>19</sup> Ofcom, June 2022. [Online Safety Bill: Ofcom's roadmap to regulation](#) [accessed 18 October 2023].

<sup>20</sup> Ofcom, June 2023. [Update: How Ofcom is preparing to regulate online safety](#) [accessed 18 October 2023].

Figure 2: Our timeline for online safety implementation <sup>21</sup>



## Phase one: Illegal content

The focus of this first phase are Codes and guidance related to the illegal content duties. This will address the most significant dangers online such as terrorism and fraud and includes measures to protect children from child sexual exploitation and abuse.

Once the consultation has closed, we will consider stakeholders' responses and decide our final position in relation to the policy issues raised in the consultation. We will then publish a statement setting out our decisions, together with final versions of the Services Risk Assessment Guidance, Codes of Practice, and related guidance.

Our current planning assumption, based on previous experience of large regulatory publications, is that we may issue the statement around one year from publication of the consultation – that is, in Autumn 2024. The Online Safety Act requires Ofcom to submit our Codes of Practice on illegal harms to the Secretary of State and to publish associated guidance within 18 months of Royal Assent. <sup>22</sup>

Once we issue our statement, services will have three months to undertake their illegal content risk assessments. At this point we will also submit the Codes of Practice to the Secretary of State, which, subject to their approval, are to be laid in Parliament for 40 days. Following approval by Parliament, the Codes will come into force 21 days after they have been issued.

<sup>21</sup> This timeline shows our key milestones and documentation but is not a comprehensive guide to everything we will produce over the first three years of the regime.

<sup>22</sup> This is subject to a possible extension of up to 12 months where this is necessary, following publication of a statement of our reasons why such an extension is necessary.

At this time the illegal harms safety duties become enforceable, and we can begin investigations and – following the conclusion of those – impose sanctions if we find that services are not compliant with these duties. We expect the duties to become enforceable around the end of 2024, assuming Parliament approves the Codes.

We also plan to consult in 2024 on elements of the framework that will underpin our powers to require services to use or develop accredited technology to deal with CSEA/terrorism content. These include Ofcom's advice to the Secretary of State on minimum standards of accuracy for accredited technologies, and guidance on how we will use these powers.

## **Phase two: Child safety, pornography, and protecting women and girls**

The second phase of our work is focused on protecting children from legal content that may be harmful to them, including pornography, content relating to suicide, self-harm and eating disorders, content that is abusive and is targeted at, or incites hatred against, people on the basis of protected characteristics; bullying, and content depicting serious violence.

This phase has several components.

First, **online services that host pornographic content** will have to use age assurance to prevent children from normally being able to access pornographic content. We will consult on draft guidance on how they can do this in December 2023.

Second, regulated **user-to-user and search services** will have to go through a process called a Children's Access Assessment, which will tell them whether they are likely to be accessed by children. If they are, they will have to comply with the children's safety duties in the Act. These include assessing the risks their services pose to children and taking steps to mitigate those risks.

We will publish our proposals for these parts of the regulatory framework for consultation in Spring 2024. This will include:

- Draft guidance for services on carrying out their Children's Access Assessments
- Ofcom's analysis of the causes and impacts of harms to children
- Draft guidance on carrying out Children's Risk Assessments
- Draft Codes of Practice setting out recommended measures to protect children online.

Regulated services will have three months to carry out Children's Access Assessments after we publish our final guidance. If they conclude that they are likely to be accessed by children, then they will have to carry out Children's Risk Assessments. We intend to publish our final guidance on Children's Access Assessments in early 2025. Our main statement on the children's safety duties will follow in Spring 2025. This will allow services to complete their initial Children's Access Assessments and determine whether they need to comply with the children's safety duties, before the requirement to carry out Children's Risk Assessments comes into force.

At this point (Spring 2025), relevant services will have three months to carry out a Children's Risk Assessment. At the same time, we will submit the children's Codes of Practice to the Secretary of State.<sup>23</sup> Subject to the Secretary of State's approval, they will then be laid in Parliament for 40 days. Following approval by Parliament, the codes will come into force 21 days after they have been issued.

---

<sup>23</sup> The Act requires us to do this within 18 months of the Act becoming law.

At this time the child protection safety duties become enforceable, and we can begin investigations and impose sanctions for non-compliance. We expect the duties to become enforceable in Summer 2025 assuming Parliament approves the codes.

By Spring 2025, we will also publish draft guidance on protecting women and girls, containing advice on content and activity which disproportionately affects women and girls, and on assessing and reducing the risk of harm to them.

### **Phase three: Additional duties for categorised services**

The third phase of online safety regulation will focus on the additional duties that will apply to categorised services, including those relating to transparency reporting, user empowerment, fraudulent advertising, and user rights.

We will publish advice to the Secretary of State regarding categorisation, and draft guidance on our approach to transparency reporting, in Spring 2024. The Secretary of State will then set thresholds for categorisation in secondary legislation. Assuming this is achieved by summer 2024, we anticipate publishing a register of categorised services by the end of 2024.

Subject to this timetable being delivered, we plan to publish further proposals regarding duties on categorised services, including a draft Code of Practice on fraudulent advertising, in early 2025, and will issue transparency notices in mid-2025, dependent on the timing of secondary legislation. As with the other areas, we will consult carefully and fully, and expect our final codes and guidance to be published around the end of 2025.

## **Repeal of video-sharing platform (VSP) regulation**

---

In May 2023 we published an update on repeal of the VSP regime, which will be superseded by Online Safety regulation.<sup>24</sup> The Secretary of State will set out in secondary legislation the date on which the VSP regime will be repealed. The Act requires the Secretary of State to give platforms at least six months' notice of the repeal date. The Secretary of State will also set out in secondary legislation the timing for when VSP providers will need to conduct risk assessments and the child access assessment – they will be given at least three months to do each of these assessments, the same as other regulated services. Ofcom will support VSP providers in moving to the online safety regime; more information about this can be found in our update on repeal of VSP regulation.<sup>25</sup>

## **Fees**

---

The online safety regime will be funded by fees paid by providers of regulated services whose qualifying worldwide revenue (QWR) meets or exceeds a certain threshold, and who are not otherwise exempt. Providers liable to pay fees will be required to notify Ofcom of their QWR and invoiced accordingly. Fees will be calculated, among other things, with reference to the provider's QWR.

Ofcom and the Secretary of State for the Department of Science, Innovation and Technology (DSIT) are both responsible for implementing the fees regime. Ofcom will determine QWR, any exemptions from the liability to pay fees, and how the fees should be calculated. The Secretary of State will set the QWR threshold, having received advice from Ofcom. We will consult publicly on the definition of

---

<sup>24</sup> Ofcom, May 2023. [Repeal of the VSP regime: what you need to know](#) [accessed 18 October 2023].

<sup>25</sup> Ofcom, May 2023. [Repeal of the VSP regime: what you need to know](#) [accessed 18 October 2023].

QWR, any exemptions, and our approach to calculating fees, as well as the advice we will give the Secretary of State on the QWR threshold.

Much of the funding regime will be implemented via secondary legislation which will be scrutinised by Parliament. We are working with DSIT with the aim of implementing the funding regime by the 2026/27 financial year.