making communications work
for everyone

Online Safety Bill: Ofcom's roadmap to regulation

Online Safety Bill: Ofcom's roadmap to regulation – Welsh translation

Publication date: 6 July 2022

Contents

Section

1. Introduction

Background to Ofcom's preparations

This document sets out our current thinking about our plan for implementing online safety regulation, based on the Online Safety Bill as introduced in the UK Parliament on 17 March 2022. It describes our view of the role of regulation in tackling online harm, how we envisage engaging with regulated services and how we will work with other regulators. It is primarily intended to be useful for services in scope of the Bill, and includes initial illustrative timelines for implementation of each element of the regime.

In February 2020, the Government announced it was minded to appoint Ofcom as the regulator for online safety in the UK. We have been working since then to develop our understanding of the opportunities and challenges of online safety regulation, build our internal capability and begin planning for our regulatory approach.

Since December 2020, we have been funded by Government to strengthen our capabilities to prepare for this role, including creating an Online Safety Policy team and a Trust & Safety Technology function and growing our Enforcement, Legal, Research & Insight and Data teams. We have started to build out a hub in Manchester, where we aim to create 150 new jobs out of an estimated 300-350 roles required to deliver the regulations by the end of 2024.

We have been informed by our experience in regulating video-sharing platforms (VSPs), for which we already have powers under transposed European legislation. In October 2021, we published guidance for VSPs established in the UK, which are legally required to take appropriate measures to protect users. We also published our Plan and Approach to the VSP rules which outlined five initial regulatory priorities: reducing the risk of child sexual abuse material on adult sites; laying the foundations for age verification on those sites; tackling online hate and terror; ensuring an age-appropriate experience on platforms popular with under-18s; and ensuring VSPs' processes for reporting harmful content are effective.

About this document

We're working hard to get ready for our new role. This document provides details of our current plan for implementation, based on the requirements of the Bill and the insight we have gained from our research and stakeholder engagement so far.

However, this plan is based on our current understanding of the Bill as it stands and of the likely timing for passage of legislation (including secondary legislation under the Bill). At the time of publication, the Bill has passed Committee stage in the House of Commons and is subject to amendment as it passes through the rest of the Parliamentary process. Consequently, the timelines and requirements described in this document remain provisional.

As the timing or substance of the Bill evolves, and as our preparatory work progresses, so will our plans. We will continue to look for opportunities to bring forward implementation as the legislative timetable becomes clearer (including the likely timing of relevant secondary legislation), where it is

possible to do so consistent with our commitment to robust, evidence-based and consultative policy making. We will provide a further update on our implementation plans if they change significantly.

In preparing this Roadmap, we have focused on the key duties of greatest significance to industry and the wider public, and the key milestones in-scope services will need to work towards in order to prepare for regulation. We have not addressed every aspect of the Bill, and this document is not intended to provide guidance for services about what they will need to do to comply.

We will provide more information on what services can do to comply with their duties in the Codes and guidance we publish after the Bill receives Royal Assent.

2. Our approach to online safety regulation

The role of regulation

The Online Safety Bill, as currently drafted, will require services which host user-generated content and search engines to have systems and processes for protecting individuals from certain types of harm online, and require pornography providers to ensure children are not normally able to encounter pornographic content. Any such service which has significant numbers of UK users or which is targeted at the UK market will have new duties and must comply with the new law.

Our research reveals how people have benefited greatly from the wave of technological innovation that built many of today's most widely used and best-loved online services. Online platforms have supported the free flow of news and information; helped businesses reach new markets; and created unprecedented potential for self-expression and global community. Six in ten UK Internet users agree that being online helps them pursue their interests and hobbies in a way they couldn't do offline, and nearly half agree they can share their opinions and have a voice online more easily or effectively than they can offline.[1]

However, the very rapid growth of new services – the unprecedented scale and diversity of online activity, and the removal of barriers to dissemination of harmful content – has created undoubted challenges. Our own evidence shows how online harms have affected UK internet users, with over six in ten users having encountered at least one incidence of potentially harmful online behaviour or content in the last four weeks, and women especially being less confident about their online safety.[2] Half of adults support further steps being taken to improve user safety online, with less than a quarter of the view that current online safety measures are sufficient to protect users.[3]

Ofcom's core duty under the Bill is to **adequately protect citizens from harm by ensuring online services make appropriate use of systems and processes to keep users safe**. In doing so, we will ensure our approach upholds the importance of freedom of expression online. Over the last two and a half years, we have been engaging extensively with industry, civil society, public bodies, and independent experts, as well as policy makers and other regulators around the world. We know that many services already take measures aimed at protecting their users. Most services have terms of service that prohibit sharing of harmful or illegal content, and moderate content in response to user complaints. Some services use sophisticated automated content detection tools. Many work closely with civil society, protection agencies and law enforcement to help address the most serious harms such as child sexual abuse.

Although welcome, these initiatives have not been sufficient to allay concern about online harms. In our discussions with stakeholders, we have heard criticism that industry action is too reactive; that there is a gap between what platforms' terms say they prohibit, and the reality of users'

[1] Ofcom, Online Nation 2022, 1 June 2022, pg. 57.
[2] Ofcom, Online Experiences Tracker. Among UK internet users aged 13+
[3] Ofcom, Online Nation 2022, pg. 77.

experiences; and that there is not enough transparency and independent assessment of platforms' policies.

The Bill addresses these concerns by requiring services to take a **comprehensive, proactive approach to managing risk** of online harm, and to ensure that risks to the safety of users are considered as part of product and service design. For example, services will need to consider the risk that algorithms might promote harmful content, especially to vulnerable users, or expose children to dangerous engagement with adults. The Bill will require services to have robust governance processes to identify and manage such risks, and effective systems for users to report harmful content, and to complain and seek redress. The highest reach services will need to be much more transparent about the risks they identify and the actions they take in response.

There is no one-size-fits-all approach to managing online risks. But we will expect all firms to consider how they prioritise user protection, incorporate safety considerations into product and engineering design decisions, and consider the needs and rights of all users as they do so. We will want to know how firms respond to risks of harm and consider any trade-offs with other objectives such as user engagement. In our view, these issues should be discussed regularly by senior decision-makers, and owned at the most senior levels.

Building a stronger culture and practice of risk management in online services is a long-term project and will not solve the problems of online harm overnight. So, we plan to complement our cross-cutting focus on risk management with **early action to address the most significant online harms**. The Government, and industry itself, have identified several priorities, and we will build on work already underway in those areas. These include action to prevent dissemination of child sexual abuse material and combat grooming online; to bolster industry efforts to prevent terrorism online; to work with other agencies in support of efforts to tackle online fraud; and to prevent children's access to content that is not appropriate and potentially harmful to them.

In some of these areas, there are already mature technologies and established industry initiatives to prevent dissemination of harmful content. For example, the Internet Watch Foundation has worked for many years to detect, disrupt, remove, and prevent online child sexual abuse material. More recently, the Global Internet Forum to Counter Terrorism has been established by some of the leading technology firms to foster collaboration and information-sharing to counter terrorist and violent extremist activity online. But in many other areas solutions are nascent.

We will work with industry, civil society, and other public bodies, in the UK and beyond, to develop targeted responses to harm which focus on the nature of the harm in question. Where proportionate solutions are readily available, we'll reflect these in clear recommendations in Codes of Practice. But almost all online harms are complex and multi-faceted, and require similarly complex, multi-faceted solutions. We will work with relevant stakeholders to build shared understanding and identify opportunities to collaborate to develop new approaches and, if relevant, standards.

This is novel regulation which will require both us and industry to work in new ways. It is important to understand what the Bill does and does not require. **Ofcom will not censor online content**: the Bill does not empower us to adjudicate on individual items of content or accounts. More generally, while we will seek to understand the prevalence and impact of harmful and illegal content to inform

our policy, **the presence of harmful or illegal content will not, in itself, establish whether the service has complied with its duties under the Bill.** Instead, we will be concerned with the adequacy of services' systems and processes to protect users, recognising that no platform that allows users freely to communicate and share content can entirely prevent harm, and that the requirement on services is to minimise, not eradicate the risk of harm.

We are working hard to prepare for our new duties, and we look forward to continued close engagement with stakeholders as we develop our policies and plans.

A differentiated and proportionate approach

The Government has estimated the total number of services in scope in the UK alone at around 25,000. Many more services located abroad will be in scope. The Bill sets **different requirements on different types of service**.

Every in-scope user-to-user and search service must assess the risks of harm related to illegal content and take proportionate steps to mitigate those risks. All services likely to be accessed by children will have to assess risks of harm to children and take proportionate steps to mitigate those risks.

We recognise that smaller services and start-ups do not have the resources to manage risk in the way the biggest platforms do. In many cases, they will be able to use less burdensome or costly approaches to compliance. The Bill is clear that proportionality is central to the regime; each service's chosen approach should reflect its characteristics and the risks it faces. **The Bill does not necessarily require that services are able to stop all instances of harmful content or assess every item of content** for their potential to cause harm – again the duties on services are limited by what is proportionate and technically feasible.

Some services will be assigned a category which bring additional duties. There are three special categories:

- **Category 1:** the highest reach user-to-user services with the highest risk functionalities, with transparency requirements, a duty to assess risks to adults of legal but harmful content, requirements relating to fraudulent advertising and a variety of other duties.
- **Category 2a services:** the highest reach search services, with transparency and fraudulent advertising requirements.
- **Category 2b services:** other services with potentially risky functionalities or other factors, with transparency requirements, but no other additional duties.

The Government has estimated[4] that around 30 to 40 services will meet the threshold to be assigned a category based on current policy intention. **As such, we anticipate that most in-scope services will not fall into any of these special categories.**

The thresholds for inclusion in these categories will be linked to size, functionality and other factors, and will be set by Government in secondary legislation, in consultation with Ofcom. Ofcom will then

[4] Online Safety Bill: Impact Assessment, January 2022.

determine which services meet the threshold conditions for each category and publish a register of the services in each category.

We anticipate that the transparency reports produced by Category 1, 2a and 2b services will be a powerful vehicle for driving change in the online sector. While many services already produce transparency reports, the new transparency reporting requirements will mean they will need to publish more information about how they are tackling online harms and the effectiveness of their safety measures. Transparency reports will provide us with further evidence to refine our regulatory approach over time. In addition, by shining a light on what services are doing to combat harm to users they will help hold services to account and generate reputational incentives for them to strengthen their systems and processes.

Under the Bill, **services can choose whether to host content that is legal but harmful to adults, and Ofcom cannot compel them to remove it.** Category 1 firms must assess risks associated with certain types of legal content that may be harmful to adults, have clear terms of service explaining how they handle it, and apply those terms consistently. They must also provide 'user empowerment' tools to enable users to reduce their likelihood of encountering this content. This does not require services to block or remove any legal content unless they choose to do so under their terms of service.

3. Putting the Online Safety Bill into practice

Immediate action once our powers commence

We plan to **move as rapidly as possible after the Bill is passed**, consistent with the sequencing established by the Bill and secondary legislation, and our commitment to robust, evidence-based and consultative policy-making processes that ensure effective protections for users.

The exact timeline for implementation will be primarily driven by the Parliamentary process and Government decisions regarding secondary legislation. Our current planning assumptions are grounded in the Bill as introduced and are subject to change as the Bill continues through Parliament. Details and timings of our current plan are included in the section covering our implementation plan below.

We expect our powers to come into force two months after the Bill passes into law. Shortly after that we aim to publish for consultation our first draft **guidance for risk assessments** and **Codes of Practice covering illegal content**, which will assist services in understanding how they can comply with their duties. In order to help services identify and understand the risks they may face, we will carry out a sector risk assessment. We are also likely to issue formal information requests to some services that we have identified as facing particular risks.

As in all our work, we will consult fully and transparently on our plans, giving companies sufficient time to comment and ensuring we consider the feedback we get carefully. Our current thinking on the details of this process, which could take around a year, given the wide range of issues the consultation will cover, is set out in our implementation plan. After consultation we will publish final guidance and Codes on illegal content. The Secretary of State will review our Codes and either lay them before Parliament or direct us to modify them.

Some elements of the regime depend on secondary legislation to specify priority legal harms and set categorisation thresholds. Our planning assumption is that secondary legislation will pass into law sometime in the year after Royal Assent. Shortly after this, we will publish **draft Codes and guidance on protection of children**, and **protection of adults from legal harms**, as well as a sector risk assessment related to legal harms to children and adults. We will consult publicly on these documents and finalise them around a year after we publish drafts. As with illegal content Codes, the Secretary of State must either lay the Codes before Parliament or direct us to modify them.

The Codes are key documents, which set out the steps services can take to comply with their duties. Services can choose to take an alternative approach, provided this is consistent with the duties in the Bill. But Codes will provide a clear route to compliance, and we envisage that many services will take advantage of this.

Given this, Codes must strike a balance. On the one hand, we want them to provide **sufficient clarity and simplicity** that any service, no matter how small, can reasonably be expected to follow the steps they describe. At the same time, they will need to be **suitably flexible** to be appropriate for the diverse range of services in scope of the regime and to allow for services' approaches to evolve over time as technology, and harms, evolve. We recognise that safety solutions, and our understanding of them, will improve over time – and consequently our Codes will also need to evolve.

The largest online services have capabilities and resources that vastly outstrip those of most in-scope services, and we will want to issue clear expectations of the biggest firms without imposing a disproportionate burden on smaller or lower-risk services.

In preparing our Codes we will take into account the **risks to free expression and privacy** that our recommended measures might pose and will incorporate appropriate safeguards for the protection of these fundamental rights.

Focused engagement with services that pose particular risk

In parallel with publication of draft Codes, we will prioritise engagement with **high-risk or high-impact services** to understand their existing safety systems and how they plan to improve them. While this structured engagement will only be possible for a small proportion of the services in scope, it will not be restricted to services in Category 1, 2a, or 2b; we will also engage with some smaller services, that we have identified as posing particular risks of harm by virtue of their content offer, userbase or service features. We will notify specific services in advance of this engagement beginning.

This risk-based 'supervisory' approach will help us identify systemic issues early, rather than simply reacting to emerging controversies. We will expect such services to be open with us about the risks they face; the action they've taken to address them; how they've evaluated the effectiveness of their action; and what more they might consider doing to keep users safe. We will also seek to understand users' attitudes to those services, and consider evidence from civil society organisations, researchers, and expert bodies.

We expect platforms to engage constructively with us and to comply with their regulatory obligations, including making improvements that help protect users where needed. Where possible, we will seek to engage constructively with companies to resolve any issues we identify and ensure that we take the quickest and most efficient route to ensuring users are adequately protected.

However, where we consider that a platform is not taking appropriate steps to protect users from significant harm, the Bill gives us a range of investigation and enforcement powers. These include powers to request information from services for the purposes of our functions and to obtain skilled person's reports. We also have power to impose fines of up to £18m or 10% of qualifying worldwide revenue (whichever is greater) where we find non-compliance. 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 impede access to, their services to the non-compliant service. 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.

Alignment with other regulators

We have long recognised the potential for different digital regulatory regimes within the UK to interact, and the importance of streamlining efforts with other regulatory bodies. That's why we

worked with the ICO, CMA and FCA to establish the **Digital Regulation Cooperation Forum (DRCF)** to support coordination across online regulatory efforts in the UK.

Now in its second year, this collaboration helps us promote coherence between our regimes, collaborate on projects and build capability in areas such as age assurance, market supervision and algorithmic transparency, and to work through any areas of potential tension. An important part of our work is to promote innovation, and to support the development of products, services and technologies which support our online safety aims. Over the next year, Ofcom and DRCF partners will focus work on tackling complex digital challenges, including how we collaborate with the ICO to make online safety and privacy work together to protect children. We have also stepped up our joint work programme with the FCA to explore how we work together to mitigate the risk of illegal financial promotions delivered via user-generated content or paid-for fraudulent advertising on in-scope online services. And we will shortly publish a joint statement with the CMA on interactions between online safety and competition, explaining how we will cooperate to ensure consumers and citizens benefit as much as possible from both competitive markets and online safety protections.

Several of the other regulators in the DRCF already have responsibilities, and have undertaken work, relevant to online safety. We have a particularly **strong collaborative relationship with the ICO**, including an information-sharing arrangement covering the Children's Code and the VSP regime, which is currently being strengthened to focus on the supervision of platforms. The ICO has done a great deal of work to protect children online, including producing guidance on age assurance and how firms should assess whether their services are likely to be accessed by children. We will use this work to inform our own approach to guidance and Codes of Practice, and to ensure we have a common understanding of the interactions between online safety and privacy. We will consult the ICO before publishing relevant online safety guidance.

While our responsibility will be to ensure that in-scope services meet UK legal requirements, **we recognise the importance of aligning international approaches** where appropriate and possible. Given the highly globalised nature of the technology sector, international alignment can help ensure clarity for consumers, protect users' rights, promote compliance and reduce the regulatory burden on companies and other stakeholders.

Several other jurisdictions have or are in the process of introducing new legal requirements on online services to address online harms. Australia established the eSafety Commissioner in 2015, whose scope of activity has gradually expanded since then. The EU has recently adopted the EU Digital Services Act, and other countries including Canada are currently considering legislation in this area.

We have already built strong relationships with our counterparts in other jurisdictions and will continue to follow legislative and regulatory developments elsewhere and consider the potential for compatibility and consistency between emerging regimes. While the architecture of different national regimes might vary, the regulatory tools (e.g. transparency, risk assessment, audit) are likely to be common to most or all of them, and international cooperation, including through multistakeholder fora, can help us to develop a common regulatory toolkit informed by international best practice.

We are also engaging in several voluntary initiatives to promote international cooperation on online safety, including as a member of the World Economic Forum's **Global Coalition for Digital Safety**, which aims to encourage public-private cooperation to tackling harmful content online.

Moving forward this year

We want to **move as quickly as possible to implement the new regime** and improve protections for users. We are already engaging with key services, large and small, that will be in scope of the regime and will ramp this up over the course of this year. In addition, under our media literacy duties, we are undertaking a range of research studies on online safety and technology which will inform our work when the new regime starts – including research on the drivers and prevalence of some of the most serious and impactful harms in scope of the Bill. We plan to publish this work over the course of the year. We are continuing to develop our operational processes and teams, building on the expertise we have brought in from industry, academia and the third sector.

Finally, we will continue to regulate VSPs established in the UK.[5] Lessons we learn from VSP regulation will be a key input into our thinking on online safety regulation. In Autumn 2022 we'll publish our first VSP report, assessing progress against our aims for VSP regulation and enabling users to see how their services are working to tackle harm.

[5] As it stands, the Bill will ultimately repeal the VSP regime, although the exact date of repeal has not yet been set. Ofcom will provide support to services which will eventually transition between the two regimes.

4. Implementation plan in detail

Purpose of this section

This section describes the process we will follow when setting up this new regulatory regime and explains what services will need to do, and when, in order to prepare for regulation. It is not intended as formal guidance for regulated services on their duties. We will provide more information on what services can do to comply with their duties in the Codes and guidance we publish after Royal Assent.

Scope of the regime

Who is in scope for the online safety regime?

The online safety regime is international in its reach. It will cover all services with the characteristics set out below that have links with the UK[6], regardless of where the entity providing the service is based or registered.

Broadly speaking, services where users may encounter content (such as messages, images, videos and comments) that has been generated, uploaded or shared by other users will be in scope of the online safety regime. This includes services which allow private messaging between users. Some specific service types are excluded from the regime, as listed below.

In addition, the Bill imposes duties on search services or search engines which enable users to search more than one website and/or database.

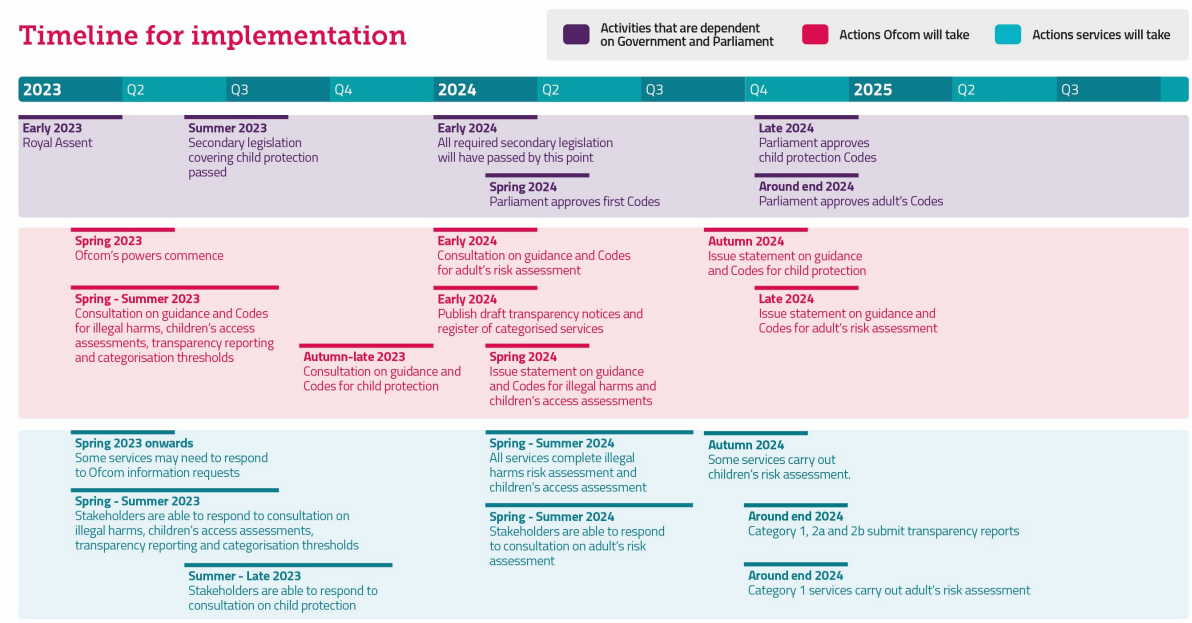
The Bill also imposes a duty on providers of pornographic content, defined as services which publish or display material produced primarily for the purpose of sexual arousal, to ensure under-18s are not normally able to encounter such material.

As mentioned above, there are some important service exemptions outlined in the Bill, which are not in scope for regulation. These include the following:

- Email services;
- SMS and MMS services;
- Services offering only one-to-one live aural communications;
- Internal business user-to-user or search services;
- Services with limited functionality for user-to-user sharing, e.g. enabling users to post product reviews;
- Services providing education and childcare;
- Services provided by public bodies.

[6] This means where: (i) the service has a significant number of UK users; (ii) UK users form one of its target markets or its only target market; or (iii) it is capable of being used in the UK by individuals and there are reasonable grounds to believe that there is a material risk of significant harm to individuals in the UK presented by user-generated content present on the service or search content of the service.

Elements and timings for implementation



Our plans following Royal Assent

Our current planning assumption is that the Online Safety Act will pass by early 2023. We expect our powers to come into force two months after Royal Assent. Once our powers come into force, we will publish a series of consultations on our approach to online safety regulation. We explain the timelines and focus for these documents below.

We would encourage all service providers to read these documents carefully as they will provide an early indication of the likely requirements of the regime and will aid services' preparatory efforts. Services will also be able to consider whether and how they will respond to our consultation.

Our plan for the first 100 days after we receive our powers:

- Publish draft Codes on illegal content harms, including Child Sexual Exploitation and Abuse (CSEA) and terrorist content;
- Publish a sector risk assessment related to illegal content harms, including risk profiles for groups of regulated firms, setting out the possible risks associated with their services;
- Publish draft guidance on illegal content risk assessments;
- Publish draft guidance on children's access assessments;
- Publish draft guidance on transparency reporting;
- Publish draft enforcement guidelines;
- Publish draft guidance on record keeping and review;
- Publish a consultation on advice to Government on categorisation thresholds;
- Publish a consultation on how Ofcom will determine who pays fees for online safety regulation;
- Start targeted engagement with the highest risk services.

Our plans for each area of the regime

The online safety regime can be thought of as being divided into four key areas. Each of these areas will have specific requirements on services, and a timeline for implementation. These areas are:

1. Protecting people from illegal content;
2. Protecting children from age inappropriate content;
3. Empowering adults to protect themselves from legal but harmful content; and
4. Increasing public transparency of categorised services' actions to protect.

The Bill covers additional duties that fall outside of these key areas, including specific duties on all services to have regard to the importance of protecting users' rights to freedom of expression within the law, and to protect users from a breach of relevant statutory provisions or rules of law concerning privacy when deciding on and implementing safety measures and policies.

There will also be duties on Category 1 and 2A services regarding fraudulent advertising, and duties on Category 1 services regarding user empowerment and user identity verification. Category 1 services will have additional duties relating to assessing impacts of their safety measures and policies on users' rights to freedom of expression and privacy, journalistic content and content of democratic importance.

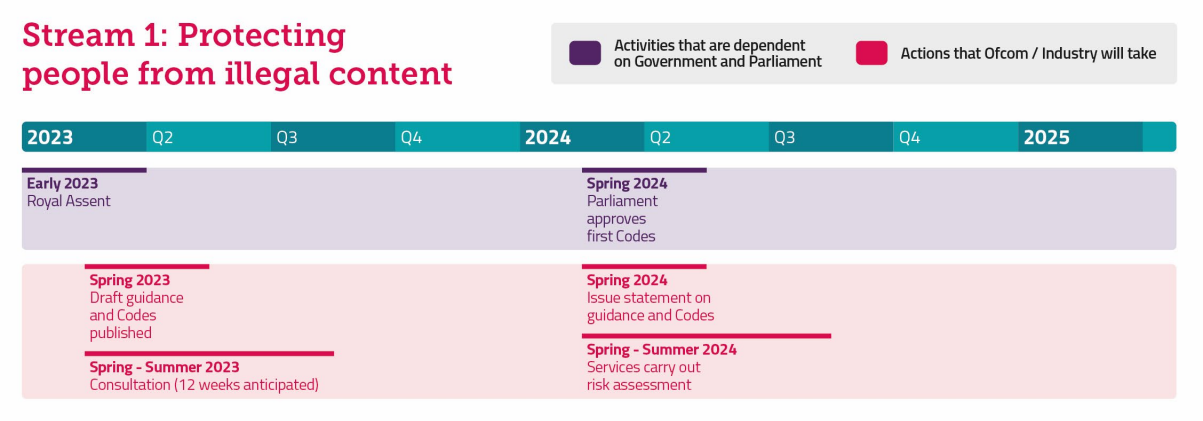
All services will have duties regarding review and record keeping. All UK-based service providers will have duties regarding CSEA reporting. Non-UK based service providers who do not already report CSEA content to other foreign agencies will also be expected to report to UK public authorities on this content.

The implementation plan focuses on the milestones that apply to the four key areas listed above and is not exhaustive in its coverage of every area of the Bill as introduced. Further detail on how we plan to approach and implement other areas covered by the Bill will be provided in due course.

Stream 1: Protecting people from illegal content

These provisions apply to all in-scope services.

The core elements of the illegal content part of the regime are set out in primary legislation. This element of the regime will therefore be implemented earliest. Our current planning assumption is that we will publish draft Codes regarding illegal content harms in Spring 2023 and the relevant duties will become enforceable around mid-2024.



What services will have duties to protect users from illegal content?

All in-scope user-to-user and search services have a duty to protect users from illegal content, regardless of their category.

All services will need to conduct an 'illegal content risk assessment'. This must assess, amongst other things, the risk of individuals encountering illegal content on a service, the risk of harm presented by illegal content and how the operations and functionalities of a service may reduce or increase these risks.

All services will need to put in place proportionate measures to effectively mitigate and manage the risks of harm from illegal content. This will include systems and processes to take down illegal content when a service becomes aware of it.

Related to this, all services will need to put in place systems and processes that allow users and affected people to report illegal content. They must also provide a complaints procedure for users who consider that they are not complying with their duties, and provide for appropriate action to be taken in response to complaints. These systems must be easy to access, easy to use, and clearly described in a service's terms of service.

What is the process for setting up this part of the regime and when will services need to take action?

We will move quickly to start implementing the illegal content component of the regime as soon as our powers commence. We will publish draft guidance setting out our proposals for how we expect

services to undertake their illegal content risk assessment, and draft Codes of Practice explaining how services can comply with their duties to tackle illegal content. We will consult publicly on these documents before finalising them.

Services and other interested stakeholders should therefore be prepared to **start engaging with our consultation on draft Codes and risk assessment guidance in Spring 2023**. Our current expectation is that the consultation will be open for three months. Services and stakeholders can respond to the consultation in this timeframe should they wish to do so.

We will also have our information gathering powers and we may use these if needed to gather evidence for our work on implementing the regime. Services should be ready to respond to these requests, and we will advise services that we intend to request information from them as early as possible.

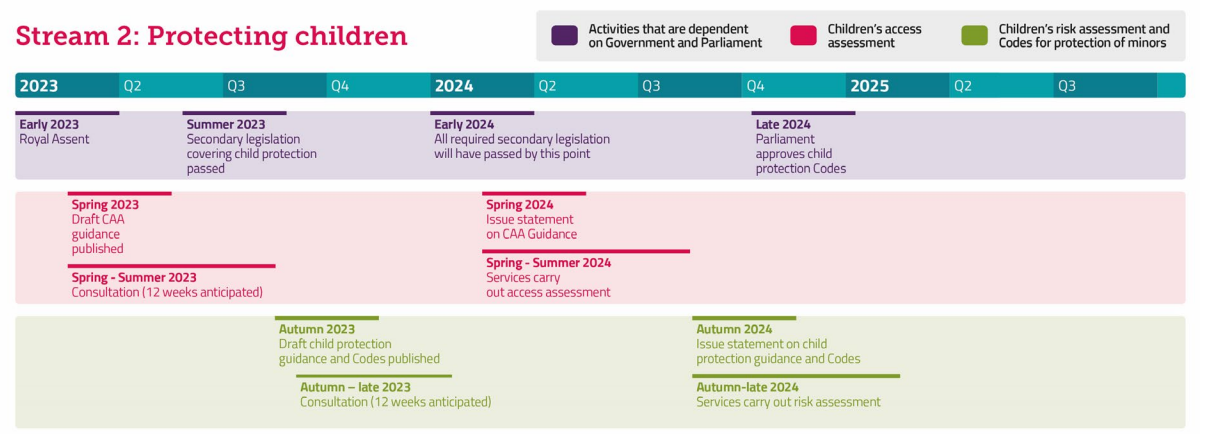
We expect to issue a statement finalising our illegal content risk assessment guidance and our illegal content Codes of Practice in Spring 2024 around a year after we publish the documents in draft for consultation. Services will then have three months to complete their illegal content risk assessment. In parallel to this we will submit our illegal content Codes of Practice to the Secretary of State to be laid in Parliament. Our current planning assumption is that the **first illegal content Codes of Practice are likely to be issued around mid-2024** at around the same time that services will be completing their illegal content risk assessments. The Codes of Practice will come into force 21 days after they have been issued. Companies will be required to comply with the illegal content safety duties from that point and we will have the power to take enforcement action if necessary.

Once the Codes of Practice are issued and services have completed their risk assessments, services will need to ensure that the mitigations they have in place to address illegal content are sufficiently robust to meet their safety duties.

As well as being prepared to respond to the consultation referred to above, **services that we propose to prioritise for focused supervisory engagement should be ready to start engaging with us regarding their systems and processes, and our draft Codes, as soon as our powers commence around Spring 2023**. As part of this engagement, we will want to understand what action services currently take to assess risks of harm arising from illegal content, what this assessment shows and what steps they are taking to mitigate risks of illegal content on their platforms.

Stream 2: Protecting children

These provisions apply to all services likely to be accessed by children.



What services will have duties to protect children?

All in-scope user-to-user and search services have a duty to establish whether children are likely to access their service or part of their service, regardless of category. To do this, services will need to conduct a 'children's access assessment'.

Services which find that they are likely to be accessed by children will also need to undertake a 'children's risk assessment' assessing the risk of child users being exposed to content that is harmful to children, and to put in place measures to mitigate risks identified. Certain specific action is required under the children's risk assessment and safety duties in respect of 'primary priority' and 'priority' content that is harmful to children. For example, user-to-user services that are likely to be accessed by children must use proportionate systems and processes to prevent children of any age from encountering primary priority content.

Priority and primary priority content that is harmful to children will be defined in secondary legislation rather than on the face of the Online Safety Act. Therefore, these duties relating to protection of children will come into effect later than the duties relating to illegal content, only after the secondary legislation is in place.

Services that are likely to be accessed by children will also need to put in place systems and processes that allow users and affected people to report content that may be harmful to children. They must also operate a complaints procedure, and provide for appropriate action to be taken in response to complaints. These systems must be easy to access, easy to use, and clearly described in a service's terms of service.

Separately, providers of pornographic content, defined as services which publish or display material produced primarily for the purpose of sexual arousal, will have a duty to ensure children are not normally able to encounter pornographic material on their services.

What is the process for setting up this part of the regime and when will services need to take action?

Shortly after our powers commence, we aim to publish draft guidance for consultation explaining how we expect services to undertake their children's access assessment. This will set out which factors services need to consider to determine whether they are likely to be accessed by children. We will consult publicly on this document.

As with the illegal content risk assessment guidance and Codes, services and other interested stakeholders should be prepared to **start engaging with our consultation on children's access assessments in Spring 2023**. Our current expectation is that the consultation will be open for three months. Services and stakeholders can respond to the consultation in this timeframe should they wish to do so.

We would expect to issue a statement finalising our children's access assessment guidance in Spring 2024, around a year after we publish the document in draft. Services will then have three months to complete their children's access assessment. If our powers commence in Spring 2023, this would mean that **services are likely to need to have completed their children's access assessment by mid-2024**.

The priority and primary priority content that is harmful to children will be defined in secondary legislation; we will not be able to consult on our draft risk assessment guidance or Codes of Practice relating to content that is harmful to children until after this secondary legislation has been finalised. Shortly after this is passed, we will publish draft guidance setting out our proposals for how we expect services that are likely to be accessed by children to undertake their children's risk assessment and draft Codes of Practice explaining how services can comply with their duties to protect children from harm. We will consult publicly on these documents.

We will also have our information gathering powers and we may use these if needed to gather evidence for our work on implementing the regime. Services should be ready to respond to these requests, and we will advise services that we intend to request information from them as early as possible.

Our current planning assumption is that the relevant secondary legislation covering content that is harmful to children will be in place by mid-2023 and that services and other interested stakeholders should therefore be prepared to start engaging with our consultation on child protection in Autumn 2023. Our current expectation is that the consultation will be open for three months. Services and stakeholders can respond to the consultation in this timeframe should they wish to do so.

We expect that **guidance and Codes on harms to children would be finalised in Autumn 2024** around a year after we publish the consultation. Services that are likely to be accessed by children will then have three months to complete their children's risk assessment. In parallel to this we will submit our Codes of Practice on harms to children to the Secretary of State to be laid in Parliament. Our current planning assumption is that this code will be issued in late 2024 at about the same time that services will be completing their first children's risk assessments.

Once the Codes of Practice have been issued and services have completed their children's risks assessments, services will need to ensure that the mitigations they have in place to address harms to children are sufficiently robust to meet their safety duties.

By the estimated timeline, this would mean that services would be expected to have completed their children's risk assessment and to be **starting to implement measures to comply with their safety duty in late 2024.**

Providers of pornographic material have a standalone duty in the Bill as drafted to ensure that children cannot normally access their services. This duty is separate from the requirements that apply to user-to-user and search services in relation to protection of children, as described above.

However, Government has indicated it is their intention that user-to-user and search services will also need to take action under their duty of care in respect of pornographic content which they host (i.e. user-generated content or in search results), as an example of a type of content that is harmful to children.

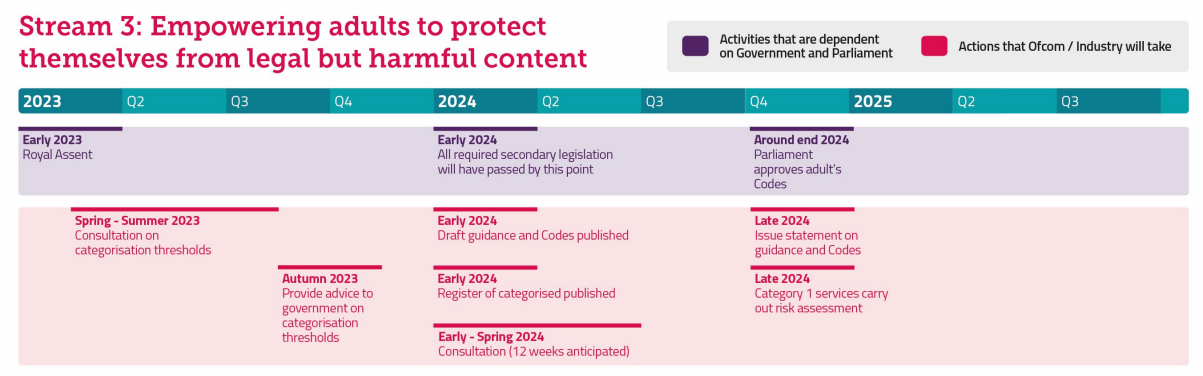
To ensure consistency in our approach to regulating pornographic content across the board – whether provider pornographic content or user-generated pornographic content - we are currently planning to consult on guidance and Codes covering the protection of children from pornographic material produced by providers of pornographic content and the protection of children from user generated pornographic content together.

According to current planning assumptions, this would mean that commercial pornography providers, services hosting user-generated pornography and search services **should prepare to engage with our consultation regarding measures to prevent children accessing pornographic material around Autumn 2023.**

Stream 3: Empowering adults to protect themselves from legal but harmful content

> These provisions apply to Category 1 services only.

Duties relating to content which is legal but harmful to adults rely on secondary legislation relating to categorisation thresholds and priority content that is harmful to adults, and will therefore be implemented later than illegal content duties.



What services will have duties to protect adults from legal but harmful content?

Services which fall into Category 1 will need to conduct 'adults' risk assessments' to assess the risks to adults from legal but harmful content on their services.

Services undertaking adults' risk assessments will have to take account of several factors, including their user base, the risk of adults encountering priority legal but harmful content, service functionalities and how the design of the service might increase or reduce the risks identified. Category 1 services will have to set out in clear and accessible terms of service a summary of their risk assessments, their approach to addressing priority legal harms to adults and to enforce their terms of service consistently.

Category 1 services will also need to put in place systems and processes that allow users and affected people to report legal but harmful content. They must also operate a complaints procedure, and provide for appropriate action to be taken in response to complaints. These systems must be easy to access, easy to use, and clearly set out in a service's terms of service.

What is the process for setting up this part of the regime and when will services need to take action?

Setting up the process for duties around harms will rely on two pieces of secondary legislation:

- Secondary legislation defining the thresholds for which services fall into Category 1; and
- Secondary legislation stipulating the priority harms to adults that services will need to consider.

Prior to this secondary legislation being introduced, we will provide advice to Government on where we recommend the threshold for Category 1 should be set. We intend to consult publicly on this advice shortly after our powers commence. **Services should be prepared to engage with this consultation around Spring 2023**.

Our planning assumption is that both pieces of secondary legislation will be in place by early 2024. As soon as possible after the threshold regulations have been made, and allowing for any necessary evidence gathering, Ofcom will publish a register listing which services fall above the threshold and are therefore in Category 1. We will also publish for consultation our draft guidance on how to undertake an adults' risk assessment and draft Codes of Practice on the steps that Category 1 services can take to meet their duties in respect of content that is legal but harmful to adults. We will consult on these draft documents and allow approximately three months for responses. Once again, Category 1 services and other interested stakeholders should be prepared to engage with our consultation in early 2024.

We will also have our information gathering powers and we may use these if needed to gather evidence for our work on implementing the regime. Services should be ready to respond to these requests, and we will advise services that we intend to request information from them as early as possible.

We expect to issue a statement finalising our adult risk assessment guidance and our adults Codes in late 2024,. Once this happens, Category 1 services will then have three months to complete their adults' risk assessment.

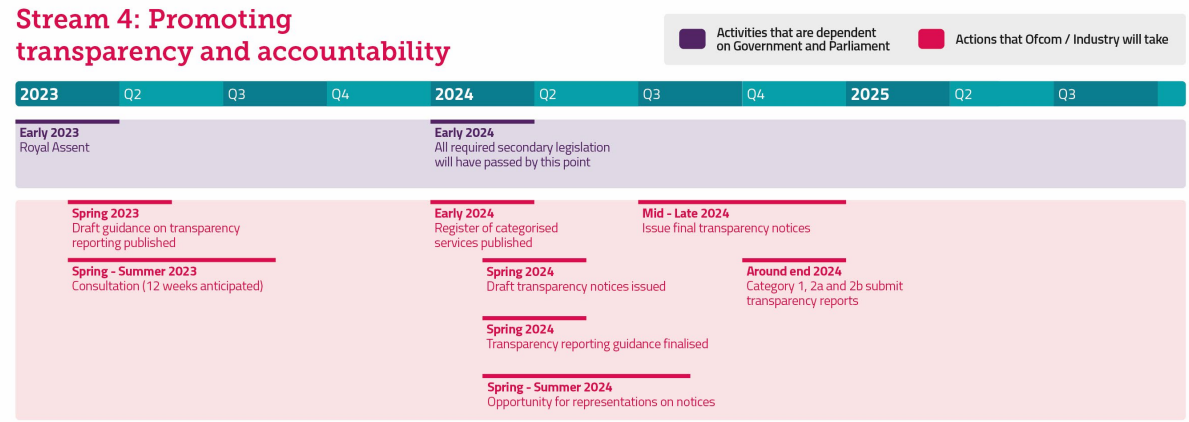
In parallel to this we will submit our Codes of Practice in respect of these safety duties to the Secretary of State to be laid in Parliament. Our current planning assumption is that **these Codes of Practice will be in force by around the end of 2024**, at roughly the same time that Category 1 services will be completing their first adults' risk assessments. Once they have done this, they will need to set out clearly in their terms of service how they will address priority content that is harmful to adults and ensure they are applying these terms consistently.

Ultimately it will be up to services to determine whether to host content that is harmful to adults provided that they are clear about their approach to this content in their terms of service. The aim of this part of the Bill is not to censor legal speech: rather it is to give users the ability to make informed choices about their engagement with online services, through transparent disclosure of the types of content that may be hosted by a service.

Stream 4: Promoting transparency and accountability

> These provisions apply to Category 1, Category 2a and Category 2b services only.

Duties to produce transparency reports rely on secondary legislation relating to categorisation thresholds and will therefore be introduced later than illegal content duties.



What services will have duties to produce transparency reports?

Ofcom will require companies in Category 1, 2a and 2b to produce and publish transparency reports regarding their service once a year. These reports will be used to inform our regulatory approach, and for the preparation of Ofcom's own annual transparency reports.

What is the process for setting up this part of the regime and when will services need to take action?

Shortly after our powers commence, we aim to publish draft guidance on transparency reporting. We will consult publicly on this guidance, allowing services approximately three months to respond.

We expect to finalise the guidance around a year after the consultation is open. If our powers commence in Spring 2023, this means that the transparency reporting guidance could be finalised by Spring 2024. As we have set out above, by this point in time we expect to have published a register setting out which services are in Category 1, 2a and 2b.

Following this, **in Spring to mid-2024, we will issue draft transparency notices** to services in these categories. We will engage with relevant services before issuing a final transparency notice to them.

Transparency notices will detail the information required in platforms' transparency reports and reporting deadlines. The types of information that may be required in a notice may include (but are not limited to) measures regarding the incidence of illegal and harmful content on a service, how terms of services are applied and functionalities in place to help users manage risks in relation to harmful content. Notices may also specify information regarding broader systems and processes in place to support users in relation to illegal and harmful content, and how a service is working with other government, regulatory or public sector bodies in the United Kingdom.

Once the notices have been finalised and issued to platforms, they will have a set amount of time to publish their transparency reports in a manner and format specified in each notice. Ofcom will issue these notices once a year. Services must ensure that their transparency reports are complete and accurate when submitting.

By the estimated timeline, this would mean that **Category 1, 2a and 2b services should be prepared to submit their first transparency reports around the end of 2024**.

Fees

The online safety regime will be funded by contributions from regulated services. Fees will be paid by those services who exceed a certain threshold of qualifying worldwide revenue (QWR).

We will consult publicly on the definition of QWR, thresholds for fee payments and our approach to calculating fees in our charging principles. Services and other interested stakeholders should be prepared to engage with this consultation in the first half of 2023/24. We anticipate that the fee structure will be confirmed in the following year, and that services which exceed the threshold of QWR to begin paying fees in 2024/25.

Next steps

Alongside the Roadmap, we have published a call for evidence asking for information about the assessment of the risk of harm from illegal content, about options for mitigating online harms, child access assessments and transparency requirements. We are interested in hearing from providers whose services are likely to fall within scope of the online safety framework, as well as regulators, academics, civil society organisations, consumer representatives and other stakeholders with interest and expertise in this area. We request responses back by **5pm on 13 September 2022**.

We will continue to engage with stakeholders from industry, civil society and other public bodies as we develop our planning for the implementation of the regime. We will be able to provide updates to services on our implementation plan and illustrative timelines as the legislative process around the Bill progresses.

We will publish our first consultation, which will focus on illegal content duties, following Royal Assent. We anticipate this process will start in Spring 2023.