LATHAM&WATKINS

UK Online Safety Act 2023

A primer on the new law for relevant service providers.

October 2024

Introduction

The Online Safety Act (the OSA) received Royal Assent on 26 October 2023 and is now in force.

The OSA establishes an extensive regulatory framework for providers of online user-to-user services and search services with links to the UK (see applicability flowchart in Schedule 2). The OSA aims to protect children and adults online by imposing duties of care on such service providers to prevent the proliferation of illegal content and activity online and of content and activity that is harmful to children, and to protect against fraudulent advertising.

The OSA is a significant departure from the existing regulatory regime in the UK applicable to online intermediaries, which is derived from the e-Commerce Directive, as obligations have moved from being reactive (i.e., notice and takedown) to proactive (i.e., requirements to implement policies/procedures to protect users). Ofcom, which will have regulatory powers to enforce sanctions, will enforce the OSA.

Certain provisions and obligations under the OSA, including some of the main duties on providers of online user-to-user services and search services, will only become enforceable once the Secretary of State and Ofcom have finalised, and parliament has approved, the applicable codes of practice and guidance (together referred to as COPs) as required by the OSA. Ofcom has published details on its three-phased approach to such COPs for putting the OSA into practice (see timeline in Schedule 1).

Ofcom will have wide-ranging enforcement powers, including issuing fines of up to £18 million or 10% of worldwide revenue (whichever is greater). Senior managers may also face potential criminal liability in certain situations, including if they fail to ensure their organisation follows information requests from Ofcom.

Contents

Applicability

The OSA imposes obligations on providers of online user-to-user services (which allow users to post content online or interact with other users) and search services (which allow users to search websites/databases) that have links with the UK and do not fall within one of the exceptions (Part 3 services).

A service is considered to have links with the UK if: (i) it has a significant number of UK users; (ii) the UK is a target market; or (iii) it is capable of being accessed by UK users and there is a material risk of significant harm to UK users. The OSA can therefore apply to companies established outside the UK (if one of these criteria are met). The exceptions include when the service is limited in functionality or when the service is an internal resource or tool for business available to a closed group of personnel or those specifically authorised.

We have set out the key exceptions as well as the applicability test in a flowchart to help you determine if your service is in scope of the OSA (see Schedule 2).

Additional obligations apply to providers of Category 1, 2A, and 2B services, which are services that meet certain threshold criteria set by reference to both user numbers and functionalities (see further below) and are formally designated by Ofcom as such service.

Next Steps

Determine whether any of your services are in scope of the OSA using the applicability flowchart in Schedule 2.

If your service has more than 3 million UK users, it meets the user number threshold criteria for Category 1, 2A, and 2B categorisation based on the draft criteria proposed by Ofcom. Providers of such service should review whether it meets the functionality threshold criteria. If so, they should start to review and assess the obligations that the service may be subject to as a Category 1, 2A, or 2B service. They must also keep track of when the final threshold criteria is set by the Secretary of State in secondary legislation to assess whether the service meets the final threshold criteria. If so, it may be formally designated as a Category 1, 2A, or 2B service and must meet the obligations applicable to such services.

Key Obligations and Liability

A. Obligations and liability applying to providers of Part 3 services

Part 3 services are “regulated user-to-user services” and “regulated search services”.

- A user-to-user service: an internet service that allows content (that is generated directly on the service or uploaded to or shared on the service by a user of the service) to be encountered by another user or other users of the service.
- A search service: an internet service that is, or includes, a service enabling a person to search more than one website or database.

User-to-user services and search services are regulated if they have links with the UK and do not fall within any of the exemptions (see applicability flowchart in Schedule 2).

I. Payment of annual fees and related notifications (Part 6)

Under the OSA, Ofcom may charge an annual fee to providers of Part 3 services, if the provider’s qualifying worldwide revenue is at or above a specified threshold. Ofcom will be required to publish statements about this threshold, including what comprises qualifying worldwide revenue and to carry out a consultation to inform the setting of the specified threshold. Following the consultation, the Secretary of State will set regulations specifying the threshold figure and keep this under review.

If a provider of a Part 3 service’s qualifying worldwide revenue[1] is at or above the specified threshold, it will be required to notify Ofcom within four months of the date of the first regulations specifying the threshold figure (and in subsequent years, at least six months before the beginning of the charging year).

When determining the quantum of the annual fee, Ofcom will take into consideration the provider's qualifying worldwide revenue for the relevant year and any other factors it considers appropriate, in line with Ofcom's published "statement of principles" (which includes considerations such as whether the fees payable are justifiable and proportionate and meet but do not exceed the cost of exercising Ofcom's online safety functions).

Next Steps

Fees are not payable until the specified threshold is determined and Ofcom publishes the required relevant statements on qualifying worldwide revenue and its principles for determining fees payable. However, providers of Part 3 services should be aware of the duty to notify Ofcom of whether or not it meets the specified threshold (once such threshold is published).

II. Illegal content risk assessment *(s.9 and s.26)*

Providers of Part 3 services are under a duty to conduct a "suitable and sufficient" illegal content risk assessment (ICRA) in relation to that service. The ICRA must be kept up to date to reflect the latest: (i) COPs and risk profiles from Ofcom; and (ii) business practices. Prior to any significant changes to the service's design or operation, providers of Part 3 services must prepare an uplift or supplement to the ICRA, assessing the impacts of the proposed change. Notably, the ICRA is a "living" document that should be updated on an ongoing basis; in contrast to the annual risk assessment obligation under the Digital Services Act.

Such assessment should assess the risk profile of the service. As part of this, providers of Part 3 services should consider the following:

- User base
- Risk of users *encountering* illegal content[2] (with the risk of encountering *each kind* of priority illegal content[3] individually assessed), taking into consideration the algorithms used by the service and how quickly and widely content may be disseminated on the service
- Risk of the service being used for the commission or facilitation of a priority offence[4]
- Risk of the service's functionalities facilitating the dissemination of illegal content or the commission or facilitation of a priority offence (identifying each functionality that presents a high level of risk)
- Ways the service is used
- The risk of harm to individuals (due to the above risks around illegal content and priority offences) and the nature and severity of such harm
- Mitigation measures, i.e., the design and operation of the service (including the governance, business model, use of proactive technology, measures to promote media literacy and safe use, and other systems and processes)

On 9 November 2023, Ofcom published its draft COPs on illegal harm duties,[5] which includes further detail on how the ICRA should be conducted;[6] it plans to finalise this towards the end of 2024 and the COPs are expected to come into force before the end of 2024 or early 2025. Providers of Part 3 services will be required to complete their ICRAs within three months of the relevant COP being approved by parliament.

In its draft COP for risk assessments,[7] Ofcom proposes a four-step risk assessment process (though we note this may be subject to change in the final COP):

1. **Understand the harms:** The OSA specifies a range of priority offences which Ofcom has grouped into 15 types of priority illegal harms. The IRCA must consider the level of risk of illegal content appearing on the service based on the characteristics of the service and, for user-to-user services, the risk the service could be used to commit or facilitate and offence set out in the OSA. Ofcom will publish "risk profiles" which identifies the risk factors associated with each of the priority offences to assist providers of Part 3 services in understanding the harms.
2. **Assess the risk of harm:** Providers of Part 3 services should consider characteristics of their service that may increase or decrease risks of harm, such as, user base, design features, and user protection or risk mitigation measures.
3. **Decide measures, implement, and record:** Providers of Part 3 services should implement measures to reduce risks of harm to individuals and consider any additional measures that may be appropriate for your service.
4. **Review, report, and update:** Report risk assessment findings through appropriate governance

channels, monitor the effectiveness of safety measures, establish an annual review cycle, and understand and act on the triggers set out in the OSA.

Next Steps

Providers of Part 3 services that are in operation before the day the final ICRA guidance is published will be required to complete their first ICRA within three months beginning on the day the guidance is approved by Parliament. Providers of Part 3 services that start up the service after such guidance is approved by Parliament will have three months from the day they become a Part 3 service to carry out their first ICRA.

III. Children's Access Assessment *(s.36 and s.37)*

Providers of Part 3 services are required to carry out a Children's Access Assessment (CAA). This written and recorded assessment should detail: (i) whether it is possible for children in the UK to access all or part of the service; and (ii) if so, whether there is a significant number[8] of child users in the UK or whether the service is likely to attract a significant number of child users in the UK (the child user condition). Children are defined as persons under the age of 18 and for the purposes of the CAA, as children in the UK.

For the purposes of step (i) above, the OSA states that providers of Part 3 services can only conclude that it is "not possible" for children to access the service if age verification or age estimation technology is deployed such that children "are not normally able to access" the service.

If a CAA concludes that the above thresholds are met (i.e., children in the UK are able to access the service and the child user condition is met), then the Part 3 service (or relevant part of that service) is considered "likely to be accessed by children" for the purposes of the OSA, meaning that the obligations in Part B below apply to the provider of that Part 3 service.[9]

A Part 3 service will also be considered "likely to be accessed by children" (and therefore the obligations set out in Part B below will apply to the provider) in the following circumstances:

a) if the provider fails to carry out the CAA as required — in such case, the service is treated as "likely to be accessed by children" from the date on which the first CAA was required to be completed and until such time as the provider completes the required CAA; or

b) if, following an investigation by Ofcom into a failure by the provider of the Part 3 service to comply with the timing and formality requirements of a CAA, Ofcom determines the service should be treated as "likely to be accessed by children" — in such case, the service is treated as "likely to be accessed by children" from the date of (or as specified in) the Ofcom decision given to the provider.

Ofcom's draft guidance on CAAs[10] identifies a non-exhaustive list of indicative factors for determining whether a Part 3 service is likely to attract a significant number of children. These factors include whether the Part 3 service offers benefits to children, whether it is appealing to children in terms of colours, presentation, features, and functionalities, as well as evidence from internal sources (e.g., reporting of users under the age of 18) and independent sources (e.g., market research, or quantitative evidence from third parties that track child media consumption).

Providers of Part 3 services must carry out an initial CAA once the obligation to do so comes into force (see next steps below) and keep a written record of its CAAs. If a provider provides more than one Part 3 service, a CAA must be conducted for each service separately.

Providers of Part 3 services that treat their services as not "likely to be accessed by children" (e.g., following completion of the CAA) must carry out a CAA at least once annually and before making any significant change to any aspect of the services' design or operation to which the CAA is relevant, or in response to evidence about reduced effectiveness of any systems and processes for age verification or age assurance, or in response to evidence about a significant increase of child users of the service in the UK.

Next Steps

Ofcom intends to finalise its guidance on the CAA in early 2025. Providers of Part 3 services in operation before the day the CAA guidance is published will be required to complete their first CAA within three months beginning on the day the guidance is published. Part 3 services that start up when such guidance is published will have three months from the day they become a Part 3 service to carry out their first CAA.

IV. Safety duties / safety by design *(s.10 and s.27)*

Providers of Part 3 services have a duty to:

- take or use proportionate measures relating to the design or operation of the service to prevent individuals from encountering priority illegal content, to mitigate and manage the risk of the service being used to commit or facilitate a priority offence (as identified in the latest IRCA), and to mitigate and manage the risk of harm to individuals (as identified in the latest IRCA); and
- operate the service using proportionate systems and processes to minimise the length of time such priority illegal content is present on Part 3 services, and enable the swift takedown of any illegal content when alerted or otherwise becoming aware of its presence.[11]

Under s.121, if Ofcom considers it necessary and proportionate to do so, it may issue a notice requiring a provider of a Part 3 service to use "accredited technology" to detect and prevent individuals from encountering terrorism content or child sexual exploitation and abuse (CSEA) content (which could potentially require providers to monitor encrypted content). The UK government has noted that it does not intend to enforce its powers under s.121 until effective technologies are available.

In Ofcom's draft illegal content COP for user-to-user services,[12] Ofcom has set out recommended measures such as: (i) establishing a content moderation team to swiftly takedown illegal content and appointing an accountable person for illegal content safety duties and reporting and complaints duties; (ii) enabling complaints via an easy-to-find, access and use complaints system and taking appropriate action for relevant complaints; (iii) ensuring clarity and accessibility of terms of service; (iv) safety metrics for on-platform testing of recommender systems (if applicable); and (v) removing accounts of proscribed terrorist organisations (those proscribed by the UK Home Secretary under the Terrorism Act 2000).

In Ofcom's draft illegal content COP for search services,[13] Ofcom has set out similar governance and accountability measures and complaints procedures as above, and additionally recommends: (i) having a search moderation function designed to deindex or downrank illegal content and CSEA URLs (a list of which should be identified by a person with expertise in the identification of CSEA); (ii) for large search services, (a) provision of CSEA content warnings in response to search requests that suggest a user may be seeking to encounter CSEA; and (b) removal of predictive search suggestions which may direct users to priority illegal content.

Next Steps

Whilst this duty is technically in force, it will not be applicable or enforceable by Ofcom until the relevant COP is approved by Parliament. As such, providers of Part 3 services should review draft COPs and consider how they can adopt these recommended measures.

V. Terms and conditions / public statement *(s.10 and s.25, s.27)*

Providers of Part 3 services must also include certain provisions in their terms of service (TOS), specifying how individuals are protected from illegal content, and for providers of user-to-user services, the TOS should include specific separate provisions addressing terrorism content, CSEA content, and other priority illegal content.

The TOS must also include provisions that give information about how any proactive technology is used by such a service for the purpose of complying with its safety duties set out above. Additionally, the TOS must be clear and accessible, and for providers of Category 1 user-to-user services and Category 2A search services, the TOS must summarise the findings of the most recent IRCA.

For providers of online search services, these provisions may be contained in a publicly available statement, which can be part of the TOS but can also be a separate statement.

The draft COPs for both user-to-user services and search services[14] recommend that provisions included in TOS should be clearly signposted for the general public, written to a reading age comprehensible for the youngest person permitted to access the service to understand and agree to them, and designed to be accessible for people using assistive technologies.

Next Steps

Whilst this duty is technically in force, it will not be applicable or enforceable by Ofcom until the date on which the relevant COP is approved by parliament. As such, providers of Part 3 services should review draft COPs and consider how they can adopt these recommended measures.

VI. Content reporting mechanisms *(s.20 and s.31)*

Providers of Part 3 services have a duty to maintain appropriate reporting and systems and processes to allow users and affected persons to easily report illegal content. The draft COPs for both user-to-user services and search services[15] recommend that providers of Part 3 services implement complaints systems that are easy to find, access, and use and take appropriate action upon receipt of complaints including sending indicative timelines to the complainant.

Next Steps

Whilst this duty is technically in force, it will not be applicable or enforceable by Ofcom until the date on which the relevant COP is approved by parliament. As such, providers of Part 3 services should review draft COPs and consider how they can adopt these recommended measures.

VII. Complaints procedures *(s.21 and s.32)*

Providers of Part 3 services must maintain a complaints procedure that allows users and "affected persons"[16] to complain to the provider of the Part 3 service about the following topics in relation to that service:

- Content present on the Part 3 service, which the user considers to be illegal content
- Breaches by the provider of the Part 3 service of their illegal content duties, content reporting duties, or the duty to have particular regard to freedom of expression and privacy when implementing safety measures and policies
- Actions taken by the provider of the Part 3 service in relation to the user or the user's content (e.g., takedown of content, de-prioritisation of content, or ban or suspension of the user), including when such action was taken following the use of proactive technology or when proactive technology was used in a way that is not contemplated by or in breach of the TOS

For search services, "interested persons"[17] may also complain if the search service provider takes or uses measures in relation to its illegal content duties that result in the interested person's content no longer appearing in search results or being given a lower priority in the search results (including if this occurs due to the use of proactive technology). Interested person may also complain if they consider the proactive technology to be used in a way that is not contemplated by or in breach of the provider's policies on its use.

This complaints procedure must be easy to access, easy to use (including by children, if relevant), and transparent. The provider of the Part 3 service must also include in the TOS provisions specifying the policies and processes that govern the handling and resolution of complaints (for search services this must be publicly available and need not be contained in the TOS).

The draft COPs for both user-to-user services and search services[18] also recommends that when a user makes a complaint, the provider of the Part 3 service should acknowledge receipt of each complaint and provide the complainant with an indicative timeline for deciding the complaint. Action taken with respect to each complaint should also be appropriate with respect to the content, and appropriate action for appeals is also recommended. Following a determination, the provider of the Part 3 service should take appropriate action with respect to what was decided.

Dedicated reporting channels should also be established for "trusted flaggers" which include government departments such as HM Revenue & Customs (HMRC), the Department for Work and Pensions (DWP), the National Crime Agency (NCA), the National Cyber Security Centre (NSCE), and the Financial Conduct Authority (FCA). The provider of the Part 3 service must also ensure its complaints procedure provides for appropriate action to be taken by the provider of the service in response to the complaints.

Next Steps

Whilst this duty is technically in force, it will not be applicable or enforceable by Ofcom until the date on which the relevant COP is published. In the interim, providers of Part 3 services should ensure they have implemented a complaints procedure and complaints forms that allow for users to raise the issues set out in this section. Inboxes for such complaints should be monitored and the complaints procedure followed to ensure compliance.

VIII. Recordkeeping *(s.23 and s.34)*

Providers of Part 3 services must keep written records of their ICRAs and CAAs (see above) as well as a written record of any measures taken or in use to comply applicable codes of practice published by Ofcom. The draft guidance[19] on recordkeeping and review recommends that these written records should demonstrate that a provider's risk assessment is suitable and sufficient.

If alternative measures are taken, the Part 3 service must keep a written record of which measures have not been complied with and the alternative measures that have been taken. Under this duty, Part 3 service must review compliance with all duties that apply to them. If the Part 3 service makes any significant change to its design or operations, it must ensure that written records are updated to reflect how the Part 3 service remains compliant with its duties.

Next Steps

Whilst this duty is technically in force, it will not be applicable or enforceable by Ofcom until the date on which the relevant COP is published. As such, providers of Part 3 services should review draft COPs and consider how they can adopt these recommended measures.

IX. Reporting CSEA content to the NCA *(s.66)*

A UK provider[20] of Part 3 services must operate its service using systems and processes to secure (so far as possible) that the provider reports all detected and unreported CSEA content present on its service to the NCA. For non-UK providers of Part 3 services, this obligation is limited to ensuring relevant UK-linked CSEA content[21] (and only UK-linked CSEA content) is reported to the NCA. The Secretary of State will issue further regulations on practical aspects of how and when CSEA is to be reported to the NCA.

Next Steps

This duty is currently not yet in force. Providers of Part 3 services should be aware of this prospective obligations and implement steps to ensure it can comply once in force.

B. Additional cumulative obligations and liability applying to providers of regulated user-to-user services and search services that are "likely to be accessed by children"

Services "likely to be accessed by children": Services in which: (i) the CAA concludes that it is possible for children to access the service and the "child user condition" is met; (ii) the provider fails to carry out the CAA as required; or (iii) following an investigation into a failure to comply with the timing and formality requirements for a CAA, Ofcom determines that a service should be treated as likely to be accessed by children (see above)

Providers of Part 3 services that are "likely to be accessed by children" are subject to additional obligations. In this section, we refer to these services as "Child Accessed Services". Ofcom will prepare and issue COPs with respect to the child safety duties.

I. Children's Risk Assessment and notification to Ofcom *(s.11 and s.28)*

Child Accessed Services must complete a "suitable and sufficient" Children's Risk Assessment (CRA). Much like the IRCA, this is intended to be a "living" document. The CRA must be kept up to date to reflect latest business practices and guidance and risk profiles from Ofcom. Prior to any significant changes to the service's design or operation, providers of Part 3 services must prepare an uplift or supplement the CRA, assessing the impacts of the proposed change.

This written and recorded CRA should detail:

- User base, including number of children users (i.e., users under 18) in different age groups
- Risk of child users encountering: (i) primary priority content that is harmful to children[22] (with each kind

separately assessed); (ii) priority content that is harmful to children[23] (with each kind separately assessed); or (iii) non-designated content that is harmful to children (i.e., content that presents material risk of significant harm to an appreciable number of children in the UK), in each case giving separate consideration to different age groups, and taking into account algorithms used and how quickly and widely content may be disseminated on the service

- The level of risk of harm presented by content that is harmful to children, giving separate consideration to children in different age groups, or characteristics or members of a certain group
- The extent to which the design of the service affects the level of risk of harm to children, in particular, functionalities that enable adults to search for and contact other users including children
- The risk that the service's functionalities increase a child's use of the service that might impact the level of risk of harm
- The nature, severity, and level of harm that child users may suffer (due to the above), given separate consideration to children in different age groups
- Mitigation measures, i.e., the design and operation of the service (including the governance, business model, use of proactive technology, measures to promote media literacy and safe use, and other systems and processes)

If the provider of a Child Accessed Service identifies the presence of non-designated content that is harmful to children, it must notify Ofcom of the kinds of content identified and the incidence of those kinds of content on the service.

Ofcom's draft guidance on CRAs[24] provides further details on how to complete the CRA and sets out a four-step methodology, and notes the CRA is separate and additional to the IRCA (see above). Hence, Child Accessed Services will have to complete both an IRCA and a CRA.

Next Steps

Part 3 services in operation before the day the first CRA guidance is published by Ofcom will be required to complete their first CRA within three months beginning on the day the guidance is published. Part 3 services that start up when such guidance is published will have three months from the day they become a Part 3 service to carry out their first CRA.

II. Child safety duties / child safety by design *(s.12 and s.29)*

Providers of Child Accessed Services have a duty to take or use proportionate measures relating to the design or operation of the service to effectively mitigate and manage the risks of harm to children identified in the risk assessment and mitigate the impact of harm to such children.

As part of this, providers of Child Accessed Services are explicitly required to:

- take or use proportionate measures relating to the design or operation of the service to effectively mitigate and manage the risks of harm to children in different age groups, as identified in the CRA and mitigate the impact of harm to children in different age groups presented by content on the service that is harmful to children; and
- operate the service using proporionate systems and processes designed to (i) prevent children of any age from encountering primary priority content that is harmful to children on the service by using "highly effective" age verification or age estimation technologies (or both); and (ii) protect children in age groups judged to be at risk of harm from other content that is harmful to children from encountering it by means of the service.[25]

Ofcom is mandated to prepare and issue COPs in relation to this duty. The draft COPs for user-to-user services set out reccomendations in respect of this duty including: (i) default settings for child users to ensure that they are not included in network expansion prompts or reccomended connection lists of other users and that other users are not reccomended to children; and (ii) provide support to child users including measures such as ensuring that information is given to child users regarding the consequences of disabling a default setting and notifications when directly communicating with a new connection for the first time.

Ofcom's published consultation provides guidance on the forms of age assurance that Ofcom considers capable of being highly effective. Examples of recommended methods include credit card checks, the use of open banking, and photo ID matching. Providers of Child Accessed Services should ensure that their chosen age assurance process fulfils Ofcom's criteria of technical accuracy, robustness, reliability, and fairness in order to be consdiered highly effective. Ofcom will not consider self-declared age verification or restrictions on child access

outlined in a platform's terms of use as being adequate measures.

Next Steps

Whilst this duty is technically in force, it will not be applicable or enforceable by Ofcom until the date on which the relevant COP is published. As such, providers of Child Accessed Services should review the draft COPs and consider how content that is harmful to children can be quickly detected and removed from circulation on their sites. Ofcom may also provide further guidance on whether "proactive technology" needs to be implemented by the provider of a particular Part 3 service.

III. Terms and conditions / public statement *(s.12 and s.29)*

Providers of user-to-user services that are Child Accessed Services must update their TOS to specify how children are prevented from encountering priority content that is harmful to them. This means information on any proactive technology used to comply with OSA duties should be included in the TOS and the provider of the Child Accessed Service must consistently comply with the TOS. Search services that are Child Accessed Services must similarly make a public statement, covering the same topics as above. For Category 1 services, the TOS should also summarise the CRA (including the level of risk, nature, severity, and potential harm to children) and Category 2A services must include a summary of the CRA in the TOS or a public statement.

IV. Content reporting and complaints procedures *(s.20, s.21, and s.31)*

The following requirements apply in addition to the requirements set out above for all providers of Part 3 services relating to content reporting mechanisms and complaints procedures:

- **Content reporting mechanism:** The content reporting mechanism (requirements set out above) must allow users and affected persons easily to report content that is harmful to children (if present on the service that is possible for children to access). The Secretary of State has the right to publish secondary legislation setting out the kinds of content that fall within this description.
- **Complaints procedure:** The complaints procedure (requirements set out above) must also allow users and affected persons to complain if they: (i) identify content on the service (that a child can access) which is considered harmful to children; (ii) identify that the provider of the Child Accessed Service is not complying with their child safety duties; (iii) feel that they have been incorrectly affected by a decision of the provider of the Child Accessed Service relating to their content (e.g., ban or suspension of the user, takedown or de-prioritisation of their content); or (iv) cannot access content due to an incorrect assessment of the user's age. Search services that are Child Accessed Services must also allow interested persons to make a complaint if the provider of the Child Accessed Service took measures so that the interested person is no longer appearing in search results or is given lower priority by virtue of measures used to comply with child safety duties.

Next Steps

Whilst this duty is technically in force, it will not be applicable or enforceable by Ofcom until the date on which the relevant COP is published. As such, providers of Part 3 services should review draft COPs and consider how they can adopt these recommended measures.

C. Additional cumulative obligations and liability applying to providers of Category 2A and 2B services

Ofcom is yet to establish a definitive register of Category 2A and 2B services. Whether a service constitutes a Category 2A or Category 2B service will depend on threshold conditions to be specified by the Secretary of State in secondary legislation (taking into consideration Ofcom's recommendations on the threshold conditions, as set out below). Ofcom is empowered under the OSA to require providers of Part 3 services to provide Ofcom with the information it requires to determine whether a service meets the relevant threshold conditions. It is not yet clear whether there will be a ramp-up period between the publication of the register of Category 2A and 2B services and the day when Part 3 services categorised as Category 2A or 2B services will need to begin full compliance with the below obligations.

- **Category 2A:** To be finalised, but Ofcom has recommended that this capture a search service which (i) is a search service but not a "vertical" [26] search service; and (ii) has more than 7 million UK users on the search engine part of the service, representing approximately 10% of the UK population.
- **Category 2B:** To be finalised, but Ofcom has recommended that this capture user-to-user services which: (i) allow users to send direct messages; and (ii) have more than 3 million UK users on the user-to-user part of the service, representing approximately 5% of the UK population.

I. Prevent fraudulent advertising *(s.39)*

Providers of a Category 2A service must implement systems and processes designed to prevent individuals from encountering fraudulent advertisements, minimise the length of time any such content is available, and swiftly take down such content when becoming aware of it. Providers must also tell users (in a publicly available statement) about any proactive technology they use for the purpose of compliance with these duties.

A fraudulent advertisement is one that is: (i) paid for; and (ii) amounts to an offence under certain sections of the Financial Services and Markets Act 2000, Fraud Act 2006, or Financial Services Act 2012 (including encouraging, assisting, inciting, aiding, or procuring such an offence).

Next Steps

Whilst this duty is technically in force, it will not be applicable or enforceable by Ofcom until services are designated by Ofcom as a Category 2A or 2B service, which will not occur until the threshold conditions are specified by the Secretary of State in secondary legislation (expected to occur by the end of 2024). Ofcom expects to publish its register of Category 1, 2A, and 2B services in summer 2025. Even if a service is designated, the obligations will not be applicable or enforceable until the relevant COP is published. Ofcom has stated it expects to publish draft COPs for additional duties for Category 1, 2A, and 2B services by early 2026 at the latest.

II. Transparency reports *(s.77)*

Once a year, Ofcom will serve providers of Category 2A and 2B services with a notice that requires such providers to produce a transparency report about the service.

These reports must:

- contain information of a kind specified or described in the notice;

  The information required in the transparency report will be specified in the notice provided by Ofcom. The transparency report should contain detailed information about the service, including its design, operation, and use, as well as the content present on the service. This includes information about regulatory compliance and risk management arrangements, design of functionalities, algorithms and other features, policies on terms of use, content moderation, functionalities allowing users to control the content they encounter, user support measures, and staff policies and practices.

- be in the format specified by the notice;

  The report should adhere to the format specified in the notice. While the exact format may vary depending on the notice, it should be easily understandable and include all the necessary details about the service and its operation.

- be submitted by the deadline specified in the notice; and
- be published in the manner and date specified in the notice.

The report should be published in the manner specified in the notice, which could include publication on the service provider's website or another specified platform.

Next Steps

The specific requirements of how to comply with this duty will only be clear once Ofcom serves a provider of a Category 2A or 2B service a notice. Ofcom has stated it expects to issue transparency notices in mid-2025. In the meantime, providers of such services should ensure that their governance and recordkeeping processes enable them to meet the high-level transparency requirements set out in the OSA (as above), and should reserve sufficient resource to respond in full and on time to the specific requirements of such notices when the need arises.

D. Additional cumulative obligations and liability applying to providers of Category 1 services

Ofcom is yet to establish a definitive register of Category 1 services. Whether a service constitutes a Category 1 service will, as above with Category 2A and 2B services, depend on threshold conditions to be specified by the Secretary of State in secondary legislation (taking into consideration Ofcom's recommendations on the threshold conditions, as set out below). Besides publishing and maintaining a register of Category 1 services, Ofcom will also publish and maintain a list of "emerging services", which meet 75% of the Category 1 user number threshold in addition to certain other threshold conditions that may be set out in the regulations.

- **Category 1:** To be finalised, but Ofcom has recommended that this capture services that meet either of the following conditions: (i) uses content recommender systems and has more than 34 million UK users on the user-to-user part of the service (representing approximately 50% of the UK population); **or** (ii) allows users to forward or reshare user-generated content, uses content recommender systems, and has more than 7 million UK users on the user-to-user part of the service (representing approximately 10% of the UK population).

I. Prevent fraudulent advertising *(s.38)*

Providers of Category 1 services will be subject to similar obligations with respect to the prevention of fraudulent advertising as providers of Category 2A and 2B services (as set out above). The primary difference is that, in relation to Category 1 services, user-generated content is excluded from the definition of a fraudulent advertisement (which is set out above in relation to Category 2A and 2B services).

Next Steps

Whilst this duty is technically in force, it will not be applicable or enforceable by Ofcom until services are designated by Ofcom as a Category 1 service, which will not occur until the threshold conditions are specified by the Secretary of State in secondary legislation (expected to occur by the end of 2024). Ofcom expects to publish its register of Category 1, 2A, and 2B services in summer 2025. Even if a service is designated, the obligations will not be applicable or enforceable until the relevant COP is published. Ofcom has stated it expects to publish draft COPs for additional duties for Category 1, 2A, and 2B services by early 2026 at the latest.

II. Transparency reports *(s.77)*

Providers of Category 1 services will be under the same obligations with respect to transparency reports as providers of Category 2A and 2B services (as set out above).

Next Steps

Whilst this duty is technically in force, it will not be applicable or enforceable by Ofcom until services are designated by Ofcom as a Category 1 service, which will not occur until the threshold conditions are specified by the Secretary of State in secondary legislation (expected to occur by the end of 2024). Ofcom expects to publish its register of Category 1, 2A, and 2B services in summer 2025. Ofcom has stated it intends to issue transparency report notices in mid-2025.

III. Impact assessments on the protection of freedom of expression and privacy *(s.22)*

Providers of Category 1 services are required to carry out impact assessments detailing how adopted safety measures or policies designed to ensure compliance with their duties affect their users' freedom of expression and privacy. These impact assessments must specifically consider the impact of these safety measures and policies on the treatment of news publisher content[27] or journalistic content in relation to the service.

Providers of Category 1 services must keep impact assessments up to date, and publish these impact assessments periodically, including publishing the positive steps they have taken to protect users' privacy and right to freedom of expression.

Next Steps

Whilst this duty is technically in force, it will not be applicable or enforceable by Ofcom until services are designated by Ofcom as a Category 1 service, which will not occur until the threshold conditions are specified by the Secretary of State in secondary legislation (expected to occur by the end of 2024). Ofcom expects to publish its register of Category 1, 2A, and 2B services in summer 2025.

IV. User identity verification and user empowerment (s.64)

A provider of a Category 1 service must offer all adult users the option to verify their identity (if identity verification is not already necessary for access to the service). Verification need not require documentation to be provided. Providers of Category 1 services must include in their TOS clear and accessible provisions that explain how verification works.

In addition, to the extent proportionate to do so, a provider of a Category 1 service must include features which give adult users increased control over harmful content, and the ability to choose whether they can interact with content uploaded by non-verified users. These features (if used) must reduce the likelihood of such content appearing, and alert the user to the presence of such content on the service. Adult users must also have the ability to filter out non-verified users. These features must be easy to access to all adult users. The TOS must include clear and accessible provisions specifying which features are available and set out how users can use them.

The draft COP for user-to-user services includes recommendations such as labelling verified users and allowing every registered user to block or mute other user accounts, and to disable comments on posted content.

Next Steps

Whilst this duty is technically in force, it will not be applicable or enforceable by Ofcom until services are designated by Ofcom as a Category 1 service, which will not occur until the threshold conditions are specified by the Secretary of State in secondary legislation (expected to occur by the end of 2024). Ofcom expects to publish its register of Category 1, 2A, and 2B services in summer 2025. Even if a service is designated, the obligations will not be applicable or enforceable until the relevant COP is published. Ofcom has stated it expects to publish draft COPs for additional duties for Category 1, 2A, and 2B services by early 2026 at the latest.

V. Complaints procedures *(s.21)*

In addition to the requirements set out above for all providers of Part 3 services relating to complaints procedures, providers of Category 1 services must also allow users to complain about: (i) breach of their user empowerment rights; or (ii) breaches with respect to content of democratic importance, news publisher content, journalistic content, and additional freedom of expression duties (e.g., if a user finds that they are unable to exercise their freedom of speech on the Category 1 service).

Next Steps

Whilst this duty is technically in force, it will not be applicable or enforceable by Ofcom until services are designated by Ofcom as a Category 1 service, which will not occur until the threshold conditions are specified by the Secretary of State in secondary legislation (expected to occur by the end of 2024). Ofcom expects to publish its register of Category 1, 2A, and 2B services in summer 2025.

VI. Protecting content of democratic importance *(s.17)*

Providers of Category 1 services must protect content of democratic importance[28] by implementing proportionate systems and processes to ensure that the importance of free expression of such content is taken into account when making decisions about how to treat such content and whether to take action against a user generating, uploading, or sharing such content. In implementing these processes, providers of Category 1 services must ensure that they give equal treatment to a wide diversity of political opinion. Providers of Category 1 services must explain how they comply with this duty in their TOS.

Next Steps

Whilst this duty is technically in force, it will not be applicable or enforceable by Ofcom until services are designated by Ofcom as a Category 1 service, which will not occur until the threshold conditions are specified by the Secretary of State in secondary legislation (expected to occur by the end of 2024). Ofcom expects to publish its register of Category 1, 2A, and 2B services in summer 2025. Even if a service is designated, the obligations will not be applicable or enforceable until the relevant COP is published. Ofcom has stated it expects to publish draft COPs for additional duties for Category 1, 2A, and 2B services by early 2026 at the latest.

VII. Protecting news publisher content (*s.18*)

A provider of a Category 1 service is subject to strict requirements under the OSA if it wants to take action in relation to news publisher content, or take action against a recognised news publisher.[29] Before taking such action, such provider must first notify the recognized news publisher as to: (i) the specific action the provider of the Category 1 service is considering; (ii) the reasons for taking such proposed action; (iii) how the service provider took into account free expression of journalistic content (if applicable); and (iv) specify a reasonable period for the recognised news publisher to make representations. It must then consider any representations made, before notifying the recognised news publisher of the decision and the reasons for it.

If the service provider reasonably considers that it would incur criminal or civil liability in relation to the news publisher content on its service if it is not taken down swiftly, it may take down that content without taking the above steps. However, it must still provide notice on the actions taken and meet the requirements of that notice as set out in the OSA.

Next Steps

This duty is not yet in force. Providers that consider themselves likely to meet the threshold conditions to be categorised as a Category 1 service should be aware of this prospective obligation and implement steps to ensure it can comply once in force.

VIII. Protecting journalistic content (*s.19*)

Providers of Category 1 services must first state in their TOS in clear and accessible language what constitutes journalistic content and how it is identified as such. The policies and processes for handling complaints as to the treatment of journalistic content must also be made clear. Providers of Category 1 services must implement proportionate systems and processes to ensure the importance of the free expression of journalistic content is taken into account when making decisions about how to treat such content and whether to take action against a user generating, uploading, or sharing such content.

If a provider of a Category 1 service takes down or restricts access to journalistic content, it must ensure that the user who generated or created such content has access to the provider of the Category 1 service's dedicated and expedited complaints procedure. These expedited channels for complaints must also be available to users who consider content they generated or uploaded to be journalistic content. If a complaint is upheld, the provider of the Category 1 service must swiftly reinstate that content and reverse any actions taken.

Next Steps

Whilst this duty is technically in force, it will not be applicable or enforceable by Ofcom until services are designated by Ofcom as a Category 1 service, which will not occur until the threshold conditions are specified by the Secretary of State in secondary legislation (expected to occur by the end of 2024). Ofcom expects to publish its register of Category 1, 2A, and 2B services in summer 2025. Even if a service is designated, the obligations will not be applicable or enforceable until the relevant COP is published. Ofcom has stated it expects to publish draft COPs for additional duties for Category 1, 2A, and 2B services by early 2026 at the latest.

IX. Acting against users in accordance with terms of service (*s.71 and s.72*)

A provider of a Category 1 service must implement proportionate systems and processes to ensure that it does not take down user-generated content, restrict access to user-generated content, or suspend or ban users other than in accordance with its TOS. Exceptions apply if the provider needs to take such actions to comply with its duties to protect against illegal content and protect children from harmful content, or to avoid criminal or civil liability.

To the extent a provider of a Category 1 service does include such terms in its TOS (i.e., commitments that it will take down a particular kind of content, restrict certain user-generated content, or suspend or ban users), it must implement proportionate systems and processes to ensure that it complies with those terms in practice. These processes and systems must allow users and affected persons to easily report relevant content and/or users.

A provider of a Category 1 service must operate an easily accessible complaints procedure that allows users to make complaints about content or users they consider should be removed/restricted/banned. The procedure should also allow users to make complaints against the provider if their content has been removed or if they have been suspended or banned from the service. The TOS must explain in an accessible way how such complaints can be made and how they will be handled and resolved.

Next Steps

Whilst this duty is technically in force, it will not be applicable or enforceable by Ofcom until services are designated by Ofcom as a Category 1 service, which will not occur until the threshold conditions are specified by the Secretary of State in secondary legislation (expected to occur by the end of 2024). Ofcom expects to publish its register of Category 1, 2A, and 2B services in summer 2025. Even if a service is designated, the obligations will not be applicable or enforceable until the relevant COP is published. Ofcom has stated it expects to publish draft COPs for additional duties for Category 1, 2A, and 2B services by early 2026 at the latest.

Enforcement and Sanctions

The OSA will grant Ofcom a number of powers to fulfil its duties as the regulator. The key enforcement powers are set out below:

- **Fines:** If organisations do not comply with their duties under the OSA, Ofcom can impose fines of up to £18 million or 10% of annual global turnover, whichever is greater. Annual global turnover is calculated by reference to the turnover of the service provider. However, if Ofcom considers that two or more group entities are jointly/severally liable for the penalty, the 10% figure is calculated by reference to the qualifying worldwide revenue of the provider and every other group entity of the provider that is considered jointly/severally liable.
- **Senior manager criminal liability:** Named senior managers[30] can be held criminally liable if (i) the service provider entity commits certain offences (e.g., failing to comply with information notices, providing false information); and (ii) the individual failed to take all reasonable steps to prevent the commission of the offence.
- **Information notices and investigations:** Ofcom may issue information notices to entities requiring them to provide information to assess compliance with OSA obligations, so long as the information requested is proportionate to the purpose of Ofcom exercising (or deciding whether to exercise) its online safety functions. Ofcom may open an investigation into whether a provider of a Part 3 service has failed (or is failing) to comply with its duties under the OSA. Similarly, Ofcom has the power to require interviews with officers and employees of an entity as well as powers of entry, inspection, and audit.

- **Correctional orders:** Ofcom may (after serving a "provisional notice of contravention" and the period for representations from the entity having expired) require a provider of a Part 3 service to comply with the notified requirement or remedy the failure to comply. As part of this, Ofcom may require a provider of a Part 3 service to take steps to use a kind, or one of the kinds, of proactive technology. Ofcom can only require proactive technology to be used on user-generated content or metadata that is communicated publicly.
- **Business disruption:** In limited circumstances, Ofcom has the power, with the agreement of the courts, to take the following actions:
  - **Service restriction:** Require ancillary service providers (e.g., payment providers, advertisers, search engines, and internet service providers) to stop working with/providing services to non-compliant providers.
  - **Access restriction:** Require access providers to take steps to withdraw, adapt, or manipulate access to impede users' access to the non-compliant providers' service.
- **Group companies:** If Ofcom determines that a provider of a Part 3 service has breached its obligations under the OSA, it may issue a joint notice of contravention to any of the entities in the corporate group structure of the provider of the Part 3 service. A parent entity, subsidiary entities, and fellow subsidiary entities can also be held liable for the breach by Ofcom. However, the entity that Ofcom is looking to prosecute will be given the opportunity to make representations about whether joint or several liability is appropriate. Ofcom may also issue a penalty notice against a controlling individual of the Part 3 service provider (as defined in the Companies Act 2006).
- **Corporate officers:** Corporate officers of Part 3 services providers may also be held liable for breaches of the OSA if the breach was committed with the consent or connivance of the officer or is attributable to neglect of the officer. A corporate officer means a director, manager, associate, secretary, or other similar officer or person purporting to act in any such capacity.

Finally, an eligible entity can make a complaint to Ofcom about any feature or conduct of one or more regulated services that is causing significant harm to users or the public, significantly affecting the right to freedom of expression, or otherwise having a significant adverse impact (Super Complaints). However, a complaint about a single service or provider of a Part 3 service is only admissible if Ofcom considers it of particular importance or if it impacts a large number of users or the public. An entity is considered eligible if it meets criteria specified in regulations issued by the Secretary of State, one of which must be that the entity represents the interests of users or the public.

The Secretary of State must issue regulations about procedural matters relating to such Super Complaints. These regulations may include provisions about notification to Ofcom of an intention to make a complaint, the form and manner of such a complaint, steps that Ofcom must take in relation to such a complaint, and time limits for taking steps in relation to such a complaint.

Ofcom is mandated to produce guidance about Super Complaints, including the criteria specified in regulations made by the Secretary of State, procedural matters relating to such complaints, and any other aspect of such complaints that Ofcom considers appropriate.

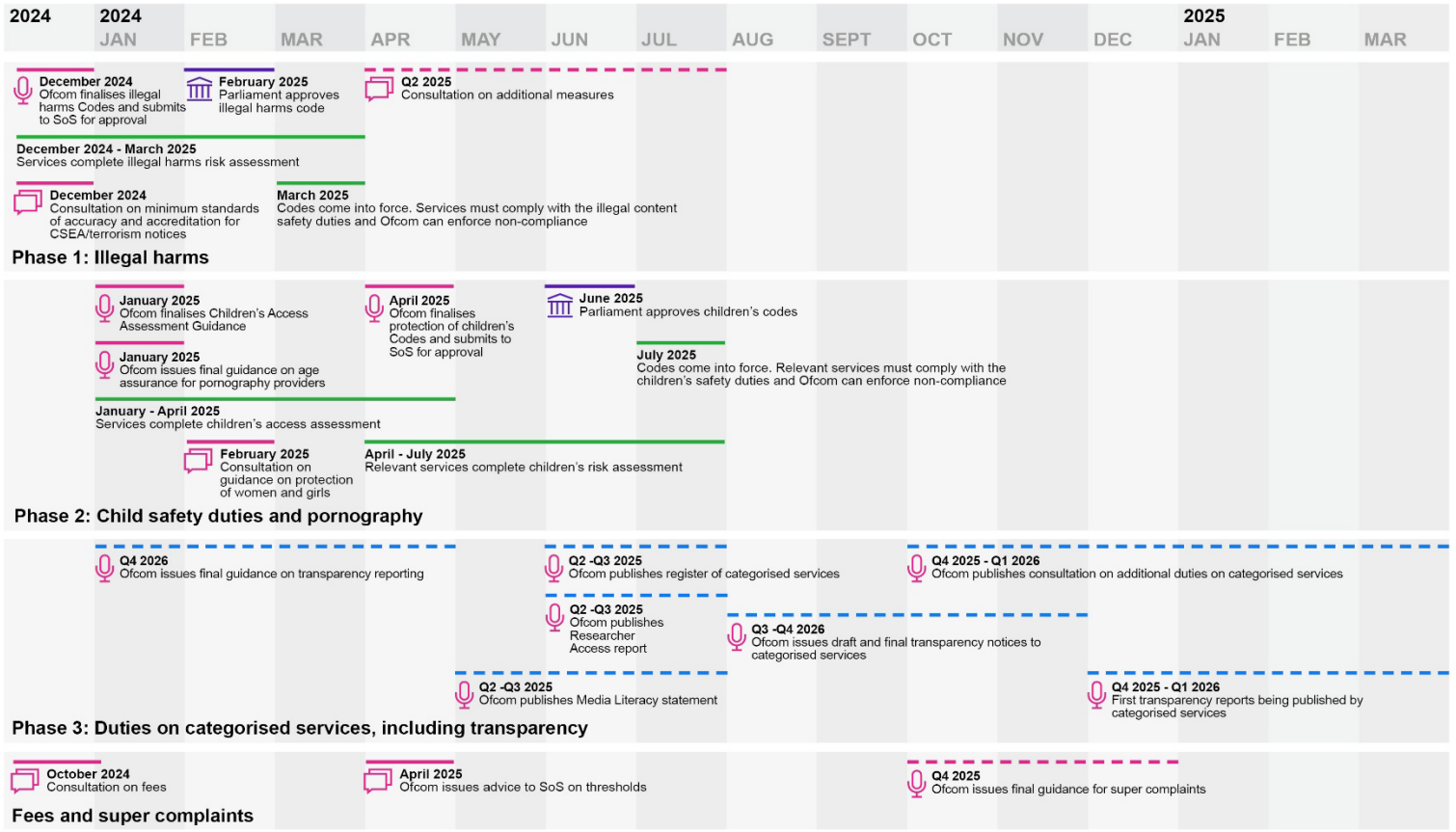
Practical Considerations

- Providers of user-to-user services or search services with links to the UK should consider how the OSA will apply to their specific services in order to plan a future strategy to ensure compliance.
- Ofcom's advice to the Secretary of State regarding categorisation will be helpful to Part 3 services as it offers a good indication of what category their service(s) are likely to fall into (if any) and insights into Ofcom's key concerns.
- The provisions of the OSA are operative immediately, so relevant service providers should prioritise their compliance actions now, based on compliance risk for the service and practical implementation timelines.
- Providers of Part 3 services should make necessary updates to their TOS to comply with transparency requirements.
- Ahead of the COPs being finalised, providers of Part 3 services can gather preliminary information to carry out risk assessments and determine if their service is likely to be accessed by children. This step allows providers of Part 3 services to implement preliminary measures to mitigate potential harm and assess the need for additional safeguards.

- Providers of Part 3 services can review the draft illegal content COPs for indications of Ofcom's expectations and carry out initial gap analysis against current content monitoring, recordkeeping, and safety duties. This process will help identify areas within internal processes that may require enhancement to align with the initial requirements outlined in the COPs.
- Providers of Part 3 services should also review the draft COPs for both user-to-user services and search services to identify best practices on reporting and complaints procedures, and determine whether improvements are needed to these current procedures.

Annex

Schedule 1: Timeline: When Will We Need to Comply?



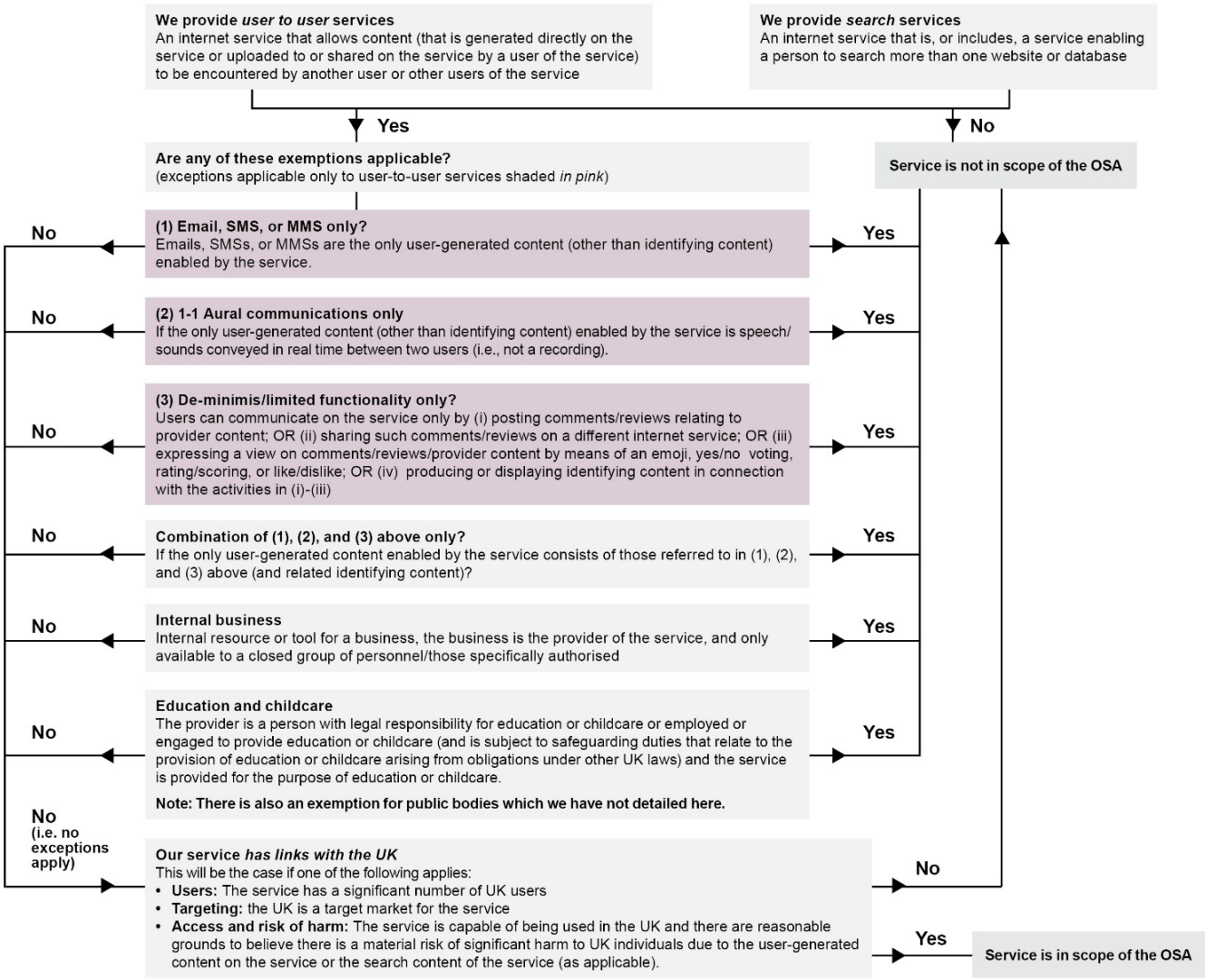
Source: Ofcom (17 October 2024)

COPs/Guidance List

No.	Title	Status	Published Date	Expected Date in Force
1	**Protecting people from illegal harms online** • Vol. 1: Background to the new Online Safety regime (introduction, illegal content duties and offences, and overview of regulated services) • Vol. 2: The causes and impacts of online harm • Vol. 3: How should services assess the risk of online harms? • Vol. 4: How to mitigate the risk of illegal harms — the illegal content Codes of Practice • Vol. 5: How to judge whether content is illegal or not (Illegal Content Judgements Guidance) • Vol. 6: Information gathering and enforcement powers and approach to supervision • A1-4: Responding to this consultation • A5: Draft service risk assessment guidance • A6: Draft guidance on recordkeeping and review • A7: Draft illegal content codes of practice for user-to-user services • A8: Draft illegal content codes of practice for search services • A9: Draft guidance on content communicated "publicly" and "privately" under the Online Safety Act • A10: Draft guidance on judgement for illegal content • A11: Draft enforcement guidance • A12-16: Other annexes	**Draft** available here	9 November 2023	March 2025
2	**Protecting children from harms online** • Vol. 1: Overview, scope, and regulatory approach • Vol. 2: Identifying the services children are using • Vol. 3: The causes and impacts of harms to children • Vol. 4: Assessing the risks of harm to children online • Vol. 5: What should services do to mitigate the risks of online harm to children? • A1-4: Responding to this consultation • A5: Draft Children's Access Assessments Guidance • A6: Draft Children's Risk Assessment Guidance (including Children's Risk Profiles) • A7: Draft Children's Safety Code: user-to-user services • A8: Draft Children's Safety Code: search services • A9: Proposed addenda to illegal codes • A10-A15: Other annexes	**Draft** available here	8 May 2024	July 2025
3	**Transparency guidance and categorised services**	**Draft** not yet available	Expected summer 2025	Q3 2026

Source: Ofcom (18 April 2024)

Schedule 2: Applicability Flowchart



Contacts

Gail E. Crawford
Partner

gail.crawford@lw.com
+44.20.7710.3001

Fiona M. Maclean
Partner

fiona.maclean@lw.com
+44.20.7710.1822

Alain Traill
Counsel

alain.traill@lw.com
+44.20.7710.4737

Victoria Wan
Associate

victoria.wan@lw.com
+44.20.7710.4686

Amy Smyth
Knowledge Management Counsel

amy.smyth@lw.com
+44.20.7710.4772

Endnotes

[1] Ofcom will make regulations specifying how the qualifying worldwide revenue of a provider is to be determined. If the provider is a member of a group of companies, the OSA specifically states such regulations may provide that the "qualifying worldwide revenue" includes the revenue of any group undertaking if such revenue relates to the provider's service.

[2] "Illegal content" means content amounting to: (i) a priority offence; or (ii) an offence in which the victim or intended victim is an individual (or individuals) and the offence is created by the OSA or before or after the OSA is passed by other rules, regulations, orders, acts, or laws.

[3] "Priority Illegal Content" means content relating to terrorism, child sexual exploitation and abuse, assisting suicide, threats to kill, public order offences, harassment, stalking and fear or provocation of violence, drugs and psychoactive substances, firearms and other weapons, assisting illegal immigration, human trafficking, sexual exploitation, sexual images, proceeds of crime, fraud, financial services crimes, foreign interference, animal welfare, or inchoate offences.

[4] A "priority offence" means an offence relating to terrorism, child sexual exploitation and abuse, assisting suicide, threats to kill, public order offences, harassment, stalking and fear or provocation of violence, drugs and psychoactive substances, firearms and other weapons, assisting illegal immigration, human trafficking, sexual exploitation, sexual images, proceeds of crime, fraud, financial services crimes, foreign interference, animal welfare, or inchoate offences.

[5] "Protecting people from illegal harms online" (available here); see also Schedule 1 for a summary of all draft COPs.

[6] See Annex 5: Service Risk Assessment Guidance of "Protecting people from illegal harms online" (available here).

[7] See Annex 5: Service Risk Assessment Guidance of "Protecting people from illegal harms online" (available here).

[8] "Significant number" means significant in proportion to the total number of UK users of the service.

[9] In these circumstances, the service is treated as "likely to be accessed by children" from the date the CAA is completed.

[10] See Annex 5: Children's Access Assessments Guidance (available here) of "Protecting Children from Harms Online" (available here); see also Schedule 1 for a summary of all draft COPs.

[11] S. 10 and s. 27 OSA set out non-exhaustive lists of specific areas in which a provider (of a user-to-user service under s.10 and of a search service under s. 27) must take measures in order to fulfil these duties (if proportionate): regulatory compliance and risk management arrangements; design of functionalities, algorithms and other features; content moderation/prioritisation; functionalities allowing users to control the content they encounter; user support measures; and staff policies and practices, and additionally in relation to user-to-user services only: policies on terms of use and policies on user access/ blocking users.

[12] See Annex 7: Illegal Content Codes of Practice for User-to-User Services (available here) of "Protecting people from illegal harms online" (available here); see also Schedule 1 for a summary of all draft COPs.

[13] See Annex 8: Illegal Content Codes of Practice for Search Services (available here) of "Protecting people from illegal harms online" (available here); see also Schedule 1 for a summary of all draft COPs.

[14] See Annex 7: Illegal Content Codes of Practice for User-to-User Services (available here) and Annex 8: Illegal Content Codes of Practice for Search Services (available here) of "Protecting people from illegal harms online" (available here); see also Schedule 1 for a summary of all draft COPs.

[15] See Annex 7: Illegal Content Codes of Practice for User-to-User Services (available here) and Annex 8: Illegal Content Codes of Practice for Search Services (available here) of "Protecting people from illegal harms online" (available here); see also Schedule 1 for a summary of all draft COPs.

[16] An "affected person" is a person (other than a user of the service) who is in the UK and: (i) is the subject of the content; OR (ii) a member of a class or group of people with certain characteristics targeted by the content; (c) a parent of, or other adult with responsibility for, a child who is a user of the service or is the subject of the content; or (d) an adult providing assistance in using the service to another adult who requires such assistance if that adult is a user or is subject to the content.

[17] An "interested person" means a person responsible for a website or database capable of being searched by the search engine, provided that the individual is in the UK or the entity is incorporated or formed under the laws of the UK.

[18] See Annex 7: Illegal Content Codes of Practice for User-to-User Services (available here) and Annex 8: Illegal Content Codes of Practice for Search Services (available here) of "Protecting people from illegal harms online" (available here); see also Schedule 1 for a summary of all draft COPs.

[19] See Annex 6: Guidance on Record Keeping and Review of "Protecting people from illegal harms online" (available here); see also Schedule 1 for a summary of all draft COPs.

[20] A "UK provider" is a provider that is incorporated or formed under the law of the UK or (in the case of providers that are individuals) habitually resident in the UK.

[21] Content is "UK-linked" if the provider has evidence of a link between the content and the UK based on the place where the content was published, generated, uploaded, or shared; the nationality or location of the person suspected of committing the related offence; and the location of the child who is a suspected victim of the related offence.

[22] "Primary priority content that is harmful to children" means pornographic content, content that encourages, promotes, or provides instruction for suicide or deliberate self-injury, eating disorders, or behaviours associated with an eating disorder.

[23] "Priority content that is harmful to children" means content that is: (i) abusive and which targets any of the following

characteristics: race, religion, sex, sexual orientation, disability, gender reassignment; (ii) inciting hatred against people of a particular race, religion, sex, or sexual orientation, who have a disability or who have the characteristic of gender reassignment; (iii) content which encourages, promotes, or provides instructions for an act of serious violence against a person; (iv) bullying content; (v) content which depicts real or realistic serious violence against an animal, injury of an animal in graphic detail, or realistically depicts serious violence against a fictional creature or serious injury of a fictional creature in graphic detail; (vi) content which encourages, promotes, or provides instructions for a challenge or stunt highly likely to result in serious injury to a person who does it or to someone else; and (vii) content which encourages a person to ingest, inject, inhale, or in any way self-administer a physically harmful substance or a substance in such quantity as to be physically harmful.

[24] See Annex 6: Children's Risk Assessment Guidance (available here) of "Protecting Children from Harms Online" (available here); see also Schedule 1 for a summary of all draft COPs.

[25] Similar to the safety duties applicable to all providers of Part 3 services in relation to illegal content, the OSA set out non-exhaustive lists of specific areas in which a provider of a Child Accessed Service (of a user-to-user service under s.12 and of a search service under s. 29) must take measures to fulfil the child safety duties (if proportionate): regulatory compliance and risk management arrangements; design of functionalities, algorithms and other features; content moderation/ prioritisation; functionalities allowing users to control the content they encounter; user support measures; and staff policies and practices, and additionally in relation to user-to-user services only: policies on terms of use and policies on user access/ blocking users.

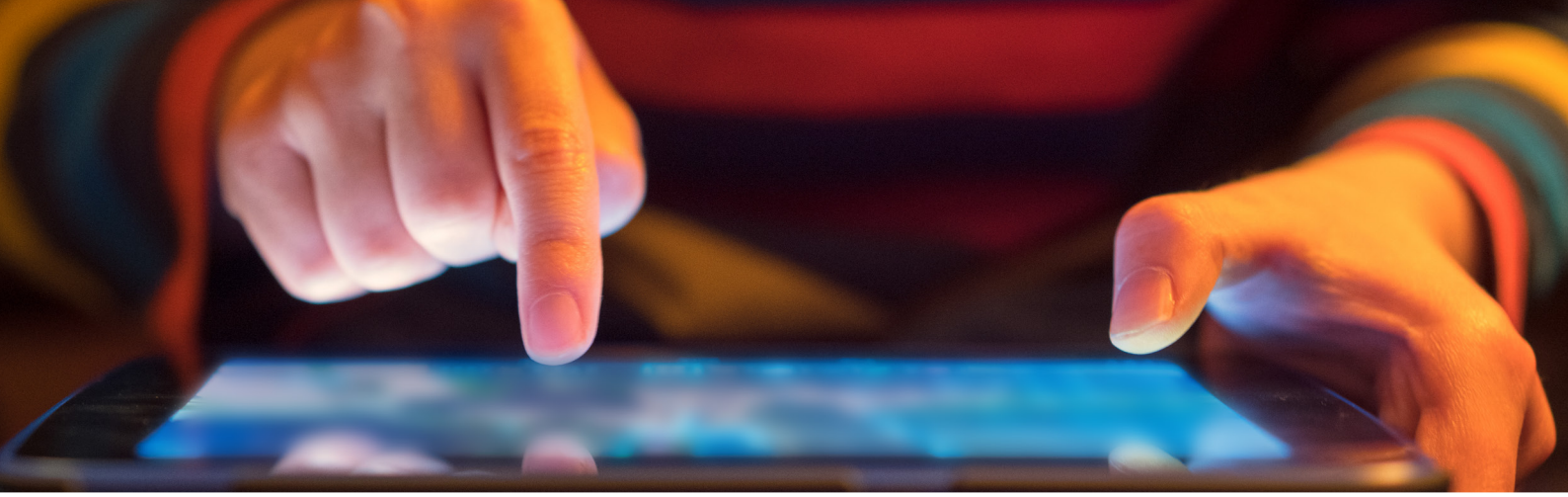
[26] "Vertical" search services are specialty search engines enabling users to search for specific topics or genres of content, or products or services offered to third-party providers. They present users with results only from selected websites with which they have a contract, API, or equivalent technical means is used to return the relevant content to users. Common vertical search services include price comparison and job listing sites.

[27] "News publisher content" is content on the service that is generated directly on the service by a user of the service that is a recognised news publisher or that is uploaded or shared to the service by a user of the service and the content: (i) reproduces in full an article or written item that was originally published by a recognised news publisher (not a screenshot or photograph of it or part of it); (ii) is video or audio content originally published by a recognised news publisher (not clipped or edited, unless the news publisher did so); or (iii) is a link to an article or item within (i) or (ii).

[28] Content of democratic importance refers to: (i) news publisher content; (ii) user-generated content; and (iii) content that is or appears to be specifically intended to contribute to the political debate in the UK.

[29] A "recognised news publisher" is the British Broadcasting Corporation, Sianel Pedwar Cymru, and holders of a licence under the Broadcasting Act 1990 or 1996 who publishes news-related material in connection with the broadcasting activities under the licence and any other entity which means certain criteria under section 56 of the OSA.

[30] Ofcom may serve information notices on providers of in-scope user to user services or search services requiring the entity to name an individual the provider considers to be a senior manager of the entity and who may reasonably be expected to be in a position to ensure compliance with the requirements of the notice. The individual must play a significant role in: (i) making decisions about how the entity's relevant activities are to be managed or organised; or (ii) the actual managing or organising of the entity's relevant activities. The individual should be informed of this appointment and be provided information about the consequences for the individual if the entity fails to comply with the requirements of the relevant information notice. It is a valid defence for an individual charged with an offence under OSA if the individual had no knowledge of being named as a senior manager in response to the information notice in question.



LW.com

Austin
Beijing
Boston
Brussels
Century City
Chicago
Dubai
Düsseldorf
Frankfurt
Hamburg
Hong Kong
Houston
London
Los Angeles
Madrid
Milan
Munich
New York
Orange County
Paris
Riyadh
San Diego
San Francisco
Seoul
Silicon Valley
Singapore
Tel Aviv
Tokyo
Washington, D.C.

LATHAM&WATKINS