Technical briefing note for the Joint Committee on the draft Online Safety Bill

This note responds to a number of the questions raised in the informal briefing Ofcom provided to the Joint Committee on 16 September. These are:

1. **Risk assessments** and whether the Bill should be strengthened to ensure that risk assessments are sufficiently robust.
2. The approach to **enforcement** in the Bill and the differences between the Online Safety Bill and the Broadcasting regime.
3. Our thoughts on the **use of technology power** and how this could be further clarified in the Bill.
4. How we are approaching the inclusion of **fraud** in the Bill and other potential expansions in scope, including how we intend to work with other regulators.

Risk assessments

In the session on the 16th September 2021, the Committee asked for Ofcom's view on whether the provisions on risk assessments are sufficiently robust.

What does the draft Bill require?

The draft Bill requires providers to carry out and keep up-to-date risk assessments relating to illegal content (all in-scope services), content that is harmful to children (services that are likely to be accessed by children) and content that is legal but harmful to adults (Category 1 services only). The draft Bill specifies that this must be an assessment to identify, assess and understand a number of considerations relating to the risks of harm to users posed by the service, including the level of risk of harm posed by encountering illegal content, content that is harmful to children and content that is harmful to adults (as relevant) and how the design and operation of the service may reduce or increase those risks.

Ofcom will be required to issue guidance to companies on their risk assessments and this will give further detail on what we expect providers to do. The guidance will be informed by the system/sector-wide risk assessment that Ofcom must carry out in accordance with the Bill, which will assess the types and levels of harm presented by different kinds of regulated services. However, by its nature as guidance, Ofcom's risk assessment guidance will not impose any binding standards or be directly enforceable. The draft Bill also provides Ofcom with powers to take enforcement action against platforms that do not undertake a risk assessment in accordance with the risk assessment duties.

The risk assessment duties are also closely tied to the steps that providers are required to take under the safety duties. In particular, in-scope providers will be required to take proportionate steps to mitigate and effectively manage the risk of harm as identified in illegal content risk assessments and children's risk assessments (as set out in clauses 9(2) and 10(2)). Providers will also have to use proportionate systems and processes designed to minimise the presence and dissemination of priority illegal content and swiftly remove all illegal content once they are aware of it, and to prevent

children from encountering primary priority content that is harmful to children, and protect children in relevant age groups from encountering other content that is harmful to children (as set out in clauses 9(3) and 10(3)). The draft Bill makes clear that, when considering what steps or systems and processes may be 'proportionate' to meet these duties, it is necessary to consider all the findings of the provider's most recent risk assessments, as well as the size and capacity of the provider (as set out in clauses 9(6) and 10(6)). Ofcom will set out recommended steps relating to this in codes of practice, which will give guidance as to how providers may comply with these duties.

How might these powers work in practice?

The Committee has expressed an interest in whether or not the provisions sufficiently cover the quality of the risk assessments. The draft Bill does not explicitly set an objective standard against which the quality of the risk assessment will be assessed. However, we understand that Government shares our objective of ensuring providers are required to identify and assess all relevant risks to a suitably high standard. To secure this objective, we think it will be important to ensure that the Bill is as clear as possible as to what platforms must do to meet their risk assessment duties. We also think it will be important for the Bill to ensure that it would not be possible for providers to either deliberately or recklessly underestimate the level of risk posed by the design or operation of their service, or to overestimate the effectiveness of their systems and processes for dealing with those risks in their risk assessments. Otherwise it is possible they might seek to do this with a view to avoiding having to go further under the safety duties to protect their users from harm.

We consider that under the draft Bill we could take enforcement action in circumstances where providers fail to carry out risk assessments at all, or within the required time limits, or fail to address the specified areas that the risk assessments must cover (for example, if a risk assessment failed to consider at all the risks posed by a particular category of priority illegal or harmful content). However, it would be more difficult for Ofcom to seek to enforce against a platform that undertakes a risk assessment within the required time limit and which addresses the specified areas, but does not adequately identify the level or nature of particular risks, or the need for further mitigating steps, which were reasonably foreseeable. This, in turn, could influence Ofcom's ability to take enforcement action against a provider for breach of the safety duties, given the close ties between the clause 9(2) and 10(2) safety duties and the risk assessment duties. We also think there could be benefits if Ofcom could take enforcement action against providers to secure directly the necessary improvements to inadequate systems and processes, without having to first demonstrate a specific breach of the risk assessment duty and then wait for providers to re-do their risk assessments properly.

We anticipate that Parliament will want to consider carefully whether the Bill will ensure that providers take steps to deal with the reasonably foreseeable risks of harm actually posed by their services, and sufficiently limits the scope for providers to underestimate the degree of risk in a particular area, or overestimate the effectiveness of the provider's safety processes in their risk assessments, so as to avoid having to make improvements to inadequate systems and processes to protect their users from harm. We expect that key to this will be ensuring the risk assessment and safety duties, taken together, make clear that providers have to take steps to identify and act upon the reasonably foreseeable risks of harm posed by their services.

The approach to enforcement in the draft Bill

In our discussions on 16 September, we talked about the approach to enforcement in the Online Safety regime and differences between this regime and the broadcasting regime. The approach to enforcement within the Online Safety regime will mirror the approach taken in other regulated sectors, focusing on incentivising regulated companies to comply with their regulatory obligations.

A key measure of success of the Online Safety regime will be the extent to which regulated providers develop and embed a strong culture of proactive risk management. Along with other regulatory levers such as transparency, formal enforcement action – used in a strategic and effective way – is a key component to drive improvements in providers' safety practices. Enforcement action promotes compliance with the duties of care set out in the Bill and serves as a deterrent against future breaches, as well as offering a route to requiring improvements, remedying harm or holding wrongdoing to account. As such, it is critical that the Bill provides Ofcom with effective enforcement tools that represent a credible threat, to incentivise regulated providers to improve standards.

What does the draft Bill require?

The draft Bill provides Ofcom with a number of enforcement tools which can be used where a regulated service has failed to discharge its duty of care towards its users. These include investigatory powers, such as powers to obtain information and require skilled person reports; and a range of sanctions, including the ability to impose significant financial penalties. The draft Bill also enables Ofcom to impose a range of remedies on providers where their systems are not working effectively to protect users from harm. These include direct requirements to improve systems or processes where Ofcom considers these are necessary to comply with a duty under the Bill or to remedy a failure. In the most serious of cases, for example where we have identified persistent failures by a regulated service to take appropriate measures to protect their users, we will be able to apply to the courts for business disruption orders. Such orders can restrict the provision of business-critical services provided to regulated services, or block access by UK users altogether. The draft Bill also includes the possibility for individual criminal liability to be introduced for senior managers who fail to comply with information notices, which could be a powerful incentive towards compliance with information requests.

However, our enforcement powers are closely tied to the duties placed on platforms by the draft Bill. If Ofcom is successfully to identify breaches and take enforcement action, it is essential that the legislation provides sufficient clarity about what is required from platforms to meet their duties.

While many of the duties are defined clearly in the draft Bill, the key safety duties currently focus on high level obligations, in order to provide additional flexibility to companies as to the steps they can take to protect users from harm. We note that the Government's proposed approach is for Ofcom to set out recommended steps in codes of practice that providers can follow to comply with the duties, while remaining free to choose to adopt a different route to compliance with their safety duties. As our written evidence set out, it would not be appropriate for regulation of online platforms to be based solely on enforcement against fixed rules and we believe it is right that the Bill leans towards granting platforms flexibility. However, with the safety duties specified at a high level, it will be harder for Ofcom to assess compliance, and to demonstrate non-compliance in situations where platforms take a different approach to the codes of practice.

It is not straightforward to strike the right balance: the Bill needs to provide enough flexibility for services to take a different route to compliance where this is needed, while at the same time enabling Ofcom to enforce effectively where platforms are not meeting the duties required by the legislation.

One option could be to add more clarity/detail to the safety duties, to spell out the types of steps that companies may be required to take in order to fulfil their safety duties.

For example, the Bill could set out a non-exhaustive list of steps and systems and processes which providers should consider taking, where proportionate (these might include having in place risk and corporate governance systems, age assurance or access controls, content moderation processes, etc). This would provide extra clarity on what providers should be doing if they take a different approach to compliance to that set out in the codes. To ensure the list was futureproofed, provision could be given for it to be changed over time via secondary legislation.

Comparison with the broadcasting standards regime

As we set out in our letter to the committee, Ofcom has significant experience of making decisions in this area, operating as an impartial and independent regulator. Ofcom will apply many of the overarching regulatory principles which we use in other sectors, including broadcasting and online content, to our regulation of online safety. These include the need for proportionality, and to strike the right balance between ensuring adequate protection for UK citizens against harm and upholding the fundamental right to freedom of expression.[1] In the new regime we will be seeking to ensure that we apply this experience throughout to uphold the importance of freedom of expression online.

As we set out in our briefing session, it is worth noting that the broadcasting regime is a licence-based, content focused regime. We assess individual broadcast programmes and consider whether the broadcasting of this content constitutes a breach of a broadcaster's licence conditions (which require, among other things, broadcasters to comply with Ofcom's Code which sets a number of content standards rules). We have a range of enforcement tools at our disposal, including financial penalties, and in the most extreme cases we can withdraw licences to broadcast.

By contrast, the online safety regime is focused on systemic improvements to companies' safety practices and will impose duties of care on regulated services to manage the risk of harm to their users. As with Ofcom's role under the new VSP regime, our role in online safety will be to assess whether regulated companies have appropriate systems and processes in place to protect their users from harm – not to investigate the actual or potential harm caused by particular pieces of content or to require individual pieces of content to be removed. While the presence of harmful content on online platforms may provide evidence of a systemic failure, in enforcement action we will be focusing on whether there has been a failure of the *systems and processes* a service has in place to minimise or prevent the presence of harmful content.

As with the VSP regime, we intend to take an evolving approach to enforcement as we embed the new regime and develop our supervisory relationships with regulated platforms. As we set out in our written evidence, we will expect to work constructively with platforms in the first instance but use

[1] The right to freedom of expression exists at Common Law and in Article 10 of the European Convention on Human Rights.

our enforcement tools where they are necessary and justified based on the evidence we have available, as well as considering the conduct of the provider and their willingness to engage.

The use of technology power

We have two key challenges with the 'Use of Technology Power' as currently drafted:

1. Lack of clarity in the relationship between i) the use of technology power and the safety duties, and ii) the codes of practice and the safety duties; and
2. The threshold at which we are able to mandate use of technology, and how this can be evidenced without using technology.

As we set out in our written evidence, it is clearly for Parliament to decide whether and in what circumstances Ofcom should be given a power to require the use of technologies to detect seriously harmful material, particularly on private channels, taking account of the important concerns about risks to individuals' privacy and freedom of expression online that can arise through their use. We also believe that the bar for Ofcom to be able to require the use of these technologies should be high, and they should only be required where proportionate and justified in the circumstances.

What does the draft Bill require?

The draft Bill provides Ofcom with a specific power to require regulated providers to use accredited technology to identify and take down child sexual exploitation and abuse (CSEA) and/or terrorism content via a 'use of technology notice', but only where certain strict conditions are met, and in accordance with procedural safeguards (as set out in clauses 63-68). Those conditions include that Ofcom must have evidence of CSEA and/or terrorism content being prevalent and persistently present on the service. In addition, Ofcom could only issue a use of technology notice where it is proportionate to prevent the harm associated with such content on the service, and there are no other less intrusive measures available to address the problem. Ofcom understands that the policy intention behind this power is to ensure that high thresholds and safeguards will apply before Ofcom could mandate use of technology which could interfere with users' rights to privacy and freedom of expression. We understand the importance of ensuring that any interference with fundamental rights as a result of requiring such a measure is justified by the risk of harm from such content.

Ofcom's concerns with the current drafting

Taking the points set out above in turn:

1. It is important that the online safety regime is able to set clear expectations for providers about what they must do to comply with their duties. The illegal content safety duties, as set out in clause 9(3)(a)-(c), would require providers of user-to-user services to use proportionate systems and processes to minimise the presence and dissemination of priority illegal content. Some commentators have suggested that these duties anticipate that providers may need to deploy proactive use of technology to achieve this in some cases (assuming this would be proportionate). Some forms of automated technologies – for example hashing tools – are of course presently widespread across the industry, particularly as a way of tackling child sexual abuse imagery and it is not clear what other proactive steps that do not involve use of technologies could be taken to significantly minimise the presence of CSEA imagery, particularly on non-public services.

However, the draft Bill is clear that Ofcom could only mandate the use of technology to identify particular content on a service, with a view to it being taken down, via a 'use of technology notice', as noted above. Such a step would only be available in very limited circumstances, and only in respect of CSEA and terrorism content. Ofcom would have no power under the draft Bill to require providers to make use of technology to identify illegal or harmful content, with a view to it being taken down, in any other circumstances. Ofcom could not, for example, require providers to use technology to identify and remove such content as part of general enforcement action for failure to comply with the safety duties (per clause 83(11)).

Whether and in what circumstances such measures should be required of providers is ultimately a question for Parliament. However, we think it is important that the Bill is clear about the intended interaction between the use of technology power and the proactive steps to identify priority illegal content envisaged in the illegal content safety duties. In particular, we think it is important the Bill is clear whether there may be any circumstances where providers may be expected to use technology to identify and remove illegal or harmful content without being required to do so by Ofcom via a use of technology notice, and where failing to do could mean that they are in breach of their duties.

It is also important that the Bill is clear that Ofcom can require some forms of use of technology, which are not so squarely focused on identification and takedown of illegal or harmful content, outside of this specific power, where appropriate and proportionate – for example, use of age assurance technologies to secure compliance with the child protection safety duties.

It will be important for providers to be clear on these points, and essential for Ofcom in deciding whether it may be appropriate to include such measures as recommended steps in codes of practice, where proportionate in the circumstances.

Options for providing even more clarity on this issue in the Bill could include: (i) more tightly defining what the scope of the use of technology power is intended to be, (ii) more tightly defining what actions Ofcom would be unable to require as part of general enforcement action and/or (iii) more detail in the illegal content safety duties.

2. As we have discussed, if we are given powers to require use of technology to identify seriously harmful content, we will need to be able to use them effectively. At present, the draft Bill requires us to demonstrate that there is evidence of persistent and prevalent CSEA and/or terrorism content on a service before Ofcom could require use of technologies to identify and remove such content. It is not currently clear how we would obtain evidence that this threshold would be met if services are not using technology to identify such content and its prevalence on the service, particularly in relation to private channels where there may otherwise be very limited visibility. In addition, it is unclear how thresholds might be set consistently across different services.

We think it may be more effective for us to be able to assess a wider range of relevant factors in order to determine whether it is necessary and proportionate for us to mandate the use of such technologies. These factors could include what evidence there is of such content on the service, the risks of harm if the technology isn't used, and the need to take into account protection of fundamental rights to privacy and freedom of expression.

Expansion of the Bill's scope and working with other regulators

The draft Online Safety Bill will enable Ofcom to require online platforms and search providers to improve their systems and processes to mitigate the risks arising from fraud that is enabled by user-generated content. The Committee asked us to write with our thoughts on the inclusion of fraud in the Bill, and how we would work with other regulators to ensure regulatory cooperation and coherence.

Regulatory cooperation

First, strong regulatory partnerships will be essential to our delivery of the regime. As we noted in our written evidence to the committee, the complexity of the Online Safety regime and the global reach of the platforms we will be regulating means that our partnerships with other bodies will be even more important than usual. We are already working closely with our regulatory partners in the UK, both through the Digital Regulator's Cooperation Forum (DRCF) and with wider partners, to learn from their approaches and to understand how we might need to work together in the future. We are also working with international partners to understand their approaches. At present, we are focussing on building our understanding of the harms captured by the Bill, as well as the potential implications of the regime on wider issues such as competition, innovation and privacy rights. We are also building relationships with new partners, in law enforcement and in areas which we need to be able to understand to effectively regulate this area, for example safety tech.

To clarify one area the Committee was interested in, while the draft Online Safety Bill itself doesn't provide for Ofcom to delegate our powers in particular areas to other bodies, this would still be possible in appropriate cases via an Order under the Deregulation and Contracting Out Act 1994.[2] This is the Act that provides the basis, for example, for the contracting out of some of Ofcom's broadcast advertising functions to the ASA. However, a different approach to designating co-regulators is taken under the VSP and on-demand programme service (ODPS) regimes. Under those regimes, the Communications Act 2003 was amended to provide Ofcom with a specific power to designate another body as 'the appropriate regulatory authority' for all or some of our functions. We have used these powers to designate the ASA as the co-regulator for ODPS advertising, and subject to the outcome of our recent consultation, could use them to do the same in respect of VSP advertising. The main difference between these two approaches is that a specific statutory provision – like the ones in the Communications Act 2003 for VSPs and ODPS – can enable us to delegate functions to a co-regulator directly, whereas the other approach requires an Order to be made by the Secretary of State under the Deregulation and Contracting Out Act before Ofcom can authorise a co-regulator to carry out functions.

[2] Section 1(7) of the Communications Act 2003 provides that Part 2 of the Deregulation and Contracting Out Act 1994 has effect in respect of functions conferred on Ofcom.

Earlier this year the DRCF provided evidence to government on areas where further legislative changes might be needed to support regulatory cooperation across the digital landscape . This evidence was intended to inform current regulatory reforms in a number of areas including the Digital Markets regime, where it will be important for sectoral regulators to input expertise. The Online Safety Bill provides another opportunity to develop further Ofcom's cooperation with other regulators, for example with the ICO in relation to privacy issues.

Also relevant is the work we are already doing with the ICO to ensure that the VSP regime and Age Appropriate Design Code (AADC) work together effectively. As we set out in our VSP guidance published on 6 October, the VSP Regulations seek to protect users, particularly under-18s, from harmful material, while the AADC ensures online services likely-to-be-accessed by children respect children's rights when using their data, and build safeguards and privacy into the design of their services. Age assurance is a priority area for both Ofcom and ICO, and we are committed to working very closely together as the code and the VSP regime both go into implementation, and as we develop our approach to age assurance ahead of the Online Safety regime.

Fraud in the Online Safety Bill

The Online Safety Bill will require online user-to-user services and search providers to take adequate steps to mitigate the risks posed to their users by the presence and dissemination of illegal user-generated content, including online fraud and scams. We envisage that this will include companies setting out and consistently implementing terms of service which prohibit illegal user-generated content (including fraudulent content), identifying the potential harm caused by online fraud and scams in their risk assessments, and putting in place proportionate systems and processes to mitigate those risks.

This regime will be focused on the end point where fraudulent user-generated content is delivered to individuals via user-to-user services (e.g. social media or messaging services) or search services.

The Online Safety Bill can only be part of a wider collaborative strategy to tackle harms caused by fraud and scams

The already complex stakeholder landscape of online fraud and scams presents a useful example of just one of the complex and evolving range of consumer harms which are perpetrated across multiple communications platforms and delivery channels. To address such complex issues, we will need to work closely with other regulators, cross sector industry players (including online, financial and telecoms service providers) and law enforcement. The regime proposed under the draft Online Safety Bill will enable Ofcom to require online platforms and search providers to take proportionate steps to mitigate the risks posed by fraud enabled by user generated content. However, these interventions will need to be part of a wider collaborative strategy for addressing the problems posed by online fraud and scams as a whole.

In isolation, it will not be possible for a regime of this nature to disrupt the entire value chain through which online fraud is undertaken. This is particularly relevant when the focal point of a scam occurs via offline and out-of-scope channels (e.g. telephone calls, emails or SMS/MMS) or via out of scope content (including paid-for advertising or cloned websites which do not comprise user-generated content). Further limitations may arise when seeking to apply the regime to scams which start with apparently benign or legitimate interactions on online services, which have the purpose of

enabling the fraudster to move the potential victim to out-of-scope communications channels so as to perpetrate a fraud or scam, but are not necessarily themselves identifiable as examples of illegal activity.

We are already working closely with the FCA, CMA and law enforcement to understand better their current approaches, areas of complementarity with the draft Bill, and how to address areas of potential divergence most effectively. We will continue to work closely with them and other partners as the final shape of the legislation develops to ensure we maximise coherence between the online safety regime and existing interventions across fraud and scams as well as the wide range of other areas that we will need to consider when implementing the Bill (in particular privacy and consumer protection).

Paid-for advertising

We understand that the Committee is considering the advantages and disadvantages of broadening the scope of the Bill to include paid-for advertising. We appreciate that paid for adverts are a significant vector for online fraud and an area of key concern. In considering recommendations in this area, we think it will be important for Parliament to consider both the complexity and scope of the Online Safety regime, as well as how it will fit with existing and future regulation. In expanding the regime further to include paid for advertising, there may be a risk that platforms, and Ofcom, are less able to focus on other priority areas, such as protecting children. Depending on the approach taken, considerable additional resource could be required to ensure that we could effectively implement the regime if paid for advertising were brought into scope. We also note that Government is planning to consider the online advertising landscape as a whole and think there could be advantages to considering the future of online advertising regulation holistically to avoid the risks of regulatory overlaps and potential increased burdens for businesses.

It is of course a decision for Government and Parliament to assess whether the coherence and effectiveness of the online safety regime would be optimised through amending or maintaining its current scope.

If Government and Parliament did choose to explore removing the exemption for paid for advertising, then the important principles for us are that:

- **Our responsibilities remain focused on systems and processes, rather than content;**
- **Our oversight remains centred on regulated user to user and search services within the current scope of the draft Bill (I.e. does not expand to include advertisers, online advertising networks, and other types of demand-side or supply-side online advertising intermediaries).**
- **Any addition to the scope of the Bill comes with a proportionate increase in resource for us to be able to effectively regulate and enforce the regime, including through collaboration with other regulators.**