

| | |
|---|-------------|
| <p>Your response: Please indicate how much of your response you want to keep confidential. Delete as appropriate.</p> | <p>None</p> |
| <p>For confidential responses, can Ofcom publish a reference to the contents of your response?</p> | <p>Yes</p> |

Your response

| Question | Your response |
|---|---|
| <p>Question 1: Ofcom’s general approach to information gathering (Section 3 of the draft guidance)</p> <p>Do you have any comments on Ofcom’s proposed general approach to information gathering, as outlined in Section 3 of the draft guidance?</p> | <p>TechUK has spoken to this previously in our response to the Illegal Harms Consultation.</p> <p>We have concerns about some of the information gathering powers proposed, particularly the ability to remotely view information demonstrating the real-time operation of a system (Volume 6). This capability raises valid concerns about risks to user privacy and security threats to the functionality of the site. Therefore, techUK requests clarification as to how this right will be used and suggest implementing guardrails to prevent misuse. Addressing these concerns is essential to strike a balance between effective regulatory oversight and protecting user privacy and the functionality of online services.</p> <p>Additionally, techUK emphasises the sparing and proportionate use of these tools, agreeing with the notion that they should only be deployed when absolutely necessary, without reasonable alternatives. It is crucial to stress that these intense tools should be used sparingly, giving services an opportunity to correct first. This approach aligns with the consultative spirit of the regulatory framework,</p> |

| | |
|--|---|
| | <p>ensuring a fair and judicious application of information gathering tools.</p> <p>techUK asks that Ofcom follows the lead of other regulators, such as the CMA, which use their information gathering powers in a proportionate and targeted way in recognition of the burden and cost they place on businesses. Requests should be narrowly framed by default. Ofcom should avoid unnecessarily broad requests to ‘fish’ for information and data not directly related to an individual provider’s compliance.</p> <p>Additionally, techUK would ask that Ofcom commits to the standard practice of sending draft Requests for Information (RFI’s), which it has stated it may do, so that providers can comment on their scope and request reasonable modifications.</p> <p>techUK believes this is key to making the operation of the UK’s online safety regime equitable for providers of services of all sizes and to correct misunderstandings about individual services which operate differently from the ones Ofcom may be most familiar with.</p> |
| <p>Question 2: Information notices (Section 4 of the draft guidance)</p> <p>a) Information notices</p> <p>Do you have any comments on Ofcom’s proposed approach to the process for issuing and responding to information notices.</p> <p>b) Requiring a test</p> <p>Do you have any comments on our proposed approach to information notices that require recipients to perform a test?</p> <p>c) Remote viewing</p> | <p>techUK acknowledges the structured approach proposed by Ofcom for issuing and responding to information notices. It is important that the process remains transparent and consistent, providing clear timelines and criteria for compliance. As mentioned above, Ofcom should commit to sending draft information notices so that providers can comment and engage with Ofcom before the final notice is released. We also recommend further clarity on the expectations for the format and scope of information to be provided and tests to be conducted, ensuring that it aligns with the operational realities of diverse digital services.</p> <p><u>Remote Viewing</u></p> <p>Clear criteria and safeguards should be in place to protect privacy and ensure that remote viewing is only used when absolutely</p> |

| | |
|--|---|
| <p>Do you have any comments on our proposed approach to Remote Viewing Information Notices? For example, to the factors that we may take into account when considering whether to issue a Remote Viewing Information Notice.</p> <p>d) Coroner Information Notices</p> <p>Do you have any comments on our proposed approach to issuing Coroner Information Notices for the purpose of responding to requests for information by investigating authorities in connection with an investigation or inquest into the death of a child?</p> <p>e) Naming a senior manager</p> <p>Do you have any comments on the section relating to naming a senior manager who is in a position to ensure compliance with an information notice?</p> | <p>necessary, and in line with privacy laws, particularly for sensitive or personal data.</p> <p><u>Coroner Information Notices</u></p> <p>techUK supports the use of these notices in a manner that respects privacy and legal requirements and processes while aiding in investigations. Ofcom should ensure that there is a clear framework for determining what information can be shared, considering both the urgency of the investigation and the rights of those involved.</p> <p><u>Naming a Senior Manager</u></p> <p>While members recognise the importance of having strong governance and accountability procedures, as well as open lines of communication with Ofcom, members note that in practice accountability for compliance with information notices will be spread across a team of people e.g. in house and external lawyers, product managers, engineers and policy and government relations teams, so it may be practically more appropriate to allow services to nominate a team or a group of individuals as responsible for the different aspects of compliance. It is also unclear what accountability would entail. Individuals are not legally responsible under the Act, unless named in an information request. If their names were to be made public, there would be a significant concern of abuse in that case.</p> <p>Rather than naming a single accountable individual, we suggest that companies provide Ofcom with a primary point of contact (which, as mentioned above, could also be a team or group of individuals).</p> |
| <p>Question 3: Skilled persons' reports (Section 5 of the draft guidance)</p> <p>Do you have any comments on our approach to skilled persons'</p> | <p>Tech UK agrees that the use of external, skilled experts will be important in developing an objective understanding of the nature and level of risk, particularly in cases where there has been a suspected compliance failure.</p> |

| | |
|--|--|
| <p>reports? This might include when we might decide to require a skilled person’s report, and the typical process that we propose to follow.</p> | <p>However, we would strongly suggest that the appointment of these experts should be a collaborative process between Ofcom and the service in question. Technology service providers are very close to the issues at hand and have developed the appropriate networks to correctly identify the required expertise. Service providers may also have legitimate confidentiality and trade secret concerns with certain third parties being appointed as skilled Persons.</p> <p>From a practical perspective, there may be occasions where a short-list of experts is required, as availability of expertise may be a constraint. Therefore, we propose that the service provider offers a short-list of experts, which they can discuss and finalise with Ofcom’s approval.</p> <p>Furthermore, in order to protect service providers’ confidentiality and trade secrets, we would propose that Ofcom’s guidance contains additional details of skilled persons’ confidentiality obligations or a requirement for such skilled persons to enter into a contract with service providers before producing a report.</p> |
| <p>Question 4: Interviews (Section 6 of the draft guidance)</p> <p>Do you have any comments on the section of guidance dealing with the power to require an individual to attend an interview?</p> | <p>TechUK would ask that Ofcom commits to the standard practice of sending draft notices to individuals, so that individuals can comment on their scope and request reasonable modifications. Clear criteria and safeguards should be in place to protect the privacy of the individuals, particularly for sensitive or personal data, in line with privacy laws. Individuals are not legally responsible under the Act, unless they fail to attend the interview or respond to Ofcom’s questions. If their names were to be made public, there would be a significant concern of abuse in that case.</p> |
| <p>Question 5: Entry with or without a warrant (Section 7 of the draft guidance)</p> | <p>The proposed approach to entry with or without a warrant should be carefully balanced to protect both public safety and individual rights (including the use of force, which should be</p> |

| | |
|--|--|
| <p>Do you have any comments on our proposed approach to entry either with or without a warrant? This might include the typical process and our interpretation of the requirement to have regard to the Home Office’s code of practice on powers of entry.</p> | <p>limited to scenarios of last resort, where no other option is available, and always within the remit of proportionality). techUK supports Ofcom’s intent to follow the Home Office’s code of practice and urges that warrants be sought only when necessary and with due regard for privacy and the potential impact on business operations.</p> |
| <p>Question 6: Audit (Section 7 of the draft guidance)</p> <p>Do you have any comments on our proposed approach to the power for Ofcom to carry out an audit to assess compliance?</p> | <p>techUK recommends that the guidance emphasizes proportionality and cooperation. Audits should be risk-based and take into account the size and nature of the service being audited. A collaborative approach will foster compliance and constructive engagement between Ofcom and service providers.</p> <p>We also recommend further clarity on the expectations for the showcasing of how systems, processes or features work, as well as the format and scope of tests and demonstrations to be conducted, ensuring that it aligns with the operational realities of diverse digital services.</p> |
| <p>Question 7: Consequences of failure to comply with an information power (Section 8 of the draft guidance)</p> <p>Do you have any comments on the potential consequences of a failure to comply with any of the information gathering powers covered in the draft guidance? This might be either on breaches that may be subject to enforcement action by Ofcom, or those that may constitute criminal offences.</p> | <p>techUK acknowledges the importance of enforcing compliance with information gathering powers. However, Ofcom should ensure that enforcement actions are proportionate to the nature of the breach. It is also crucial that service providers have clear avenues for appeal or remediation before punitive measures are taken (particularly in the context of significant financial penalties or criminal liability).</p> |
| <p>Question 8: Additional comments</p> <p>Do you have any other comments on the draft guidance?</p> | <p>N/A</p> |

| | |
|---|--|
| Please provide any information or evidence in support of your views. | |
|---|--|

Please complete this form in full and return to OSinfoguidance@ofcom.org.uk