

Question	Your response
We welcome input from industry on the areas listed below. We encourage stakeholders to respond with feedback so that we can ensure that the guidance helps providers and other stakeholders understand:	
A) Ofcom’s powers and providers’ duties for transparency reporting, as well as Ofcom’s approach to implementing the transparency regime. B) Ofcom’s approach for determining what information service providers should produce in their transparency reports. C) Ofcom’s plans to engage with providers prior to issuing transparency notices, and on what matters, and whether the proposed engagement plan will be sufficient for helping services to comply with their duties. D) Ofcom’s plans to use the information in providers’ transparency reports in Ofcom’s own transparency reports.	Confidential? – No Nextdoor supports Ofcom’s consultative approach to the enforcement of the online safety regime, and by extension, to its implementation of transparency reporting duties for services categorised under the Online Safety Act. We also appreciate the regulator’s efforts to understand and consider the perspectives of service providers who may be subject to additional duties under the OSA. In particular, we welcome Ofcom’s commitment to the key principles of “relevance and appropriateness, and proportionality” (points 3.19 and 3.20 of the consultation) for determining the content of transparency notices, and in Ofcom’s decision-making process, respectively. We agree that information requirements need to be tailored to each type of service “to ensure that they are relevant to the way in which a service is designed, used and operated” and to make sure that “the information is useful and meaningful for the public” (3.19). We think that the third principle - “proportionality” - will be especially important for transparency notices addressed to smaller providers, which we delve into in further detail in the subsequent sections of this response. In the meantime, we are reassured that Ofcom is committed to “always tak[ing] steps to ensure that the requests for information in our notices go no further than is necessary to give effect to our policy objectives” (3.20). In what follows, we offer insights to inform and facilitate the implementation of transparency reporting in the UK online safety regime.

Are there any aspects in the draft guidance where it would be helpful for additional detail or clarity to be provided?	Confidential? – No Nextdoor welcomes Ofcom’s efforts to provide sufficient information on the transparency reporting process to services who may be subject to its requirements. We would appreciate and benefit from greater clarity around some of the listed matters in Parts 1 and 2 of Schedule 8 to the Act, which Ofcom may require categorised providers to report information on. Namely, under point 3 of Part 1 (for Category 1) and point 22 of Part 2 (for Category 2B) - “The number of users who are <i>assumed</i> to have encountered illegal content, content that is harmful to children, relevant content or content to which section 15(2) applies by means of the service” - we would appreciate clarity on the regulator’s understanding of the term “assumed”. For example, will Ofcom rely on said providers to set the standards for determining how the “assumed” numbers should be calculated, or will Ofcom offer guidance on best practice or expectations for producing this data? Additionally, under point 7 of Part 1 (for Category 1) and point 26 of Part 2 (for Category 2B) - “ <i>Functionalities</i> designed to help users manage risks relating to content that is harmful to children” - we would appreciate clarity on the regulator’s understanding of the term “functionalities” as well as the differences between the “functionalities” referenced in these points and the “systems and processes” designed to help users report illegal content discussed in point 5 of Part 1 (for Category 1) and point 24 of Part 2 (for Category 2B).
Are the suggested engagement activities set out in the draft guidance sufficient for providers to understand their duties and Ofcom’s expectations?	Confidential? – No We note and understand that Ofcom may only exercise its powers relating to transparency reporting once the register of categorised services has been published. As per section 2.16 of the consultation, we are also aware that Ofcom will “repeat this process at regular intervals when the register is updated, at which point services may be added or removed from the register”.

	The possibility of year-on-year changes relevant to transparency reporting, both in the scope of categorisation thresholds and providers' own categorisation status, as well as the transparency reporting requirements themselves, create a degree of regulatory uncertainty around providers' individual annual compliance needs. To help mitigate this uncertainty, Nextdoor believes that Ofcom's right to update categorisation lists and transparency reporting requirements year-on-year warrants the regulator providing adequate and sufficient advance notices to affected companies, in line with the principles of "proportionality" and "appropriateness". Furthermore, it is our assumption that year-on-year changes will be informed by the Strategic Statement of Priorities (SSP) for online safety matters, and Ofcom's Annual Plan of Work, but we welcome clarity on any further documents that will inform the 'core' and 'thematic' information requirements.
--	---

Question	Your response
We are also seeking input that will help us understand if there are other matters that Ofcom should consider in our approach to determining the notices, beyond those that we set out in the guidance. The questions below seek input about any additional factors Ofcom should take into account in various stages of the process, including: to inform the content of transparency notices; in determining the format of providers' transparency reports; and how the capacity of a provider can be best determined and evidenced.	
Are there any other factors that Ofcom might consider in our approach to determining the contents of notices that are not set out in the draft guidance?	Confidential? – No We strongly welcome Ofcom's identification of and commitment to key factors for consideration when determining the contents of transparency notices, seen in point 2.8 of Annex A. In particular, we support Ofcom's recognition of the need to consider the functionalities of the service, the number of users of the service, the capacity of the provider, and the proportion of users of the service who are children. In what follows, we highlight further aspects of these considerations which merit attention in

	ensuring the relevance and meaningfulness of reported data. <u>Functionalities of the service - content circulation</u> Nextdoor agrees that considering the specific functionalities of services in question - factor (b) under 2.8 in Annex A - is paramount in determining adequate and individually tailored transparency reporting requirements. We would like to take this opportunity to draw the regulator's attention to specific kinds of functionalities affecting the levels of risk posed by certain platforms - namely, functionalities related to content circulation. The algorithms used to determine how content is shared and circulated, how long it remains relevant to users, and how many users it's shown to, vary between services. For instance, many social media platforms promote content to wider publics based on user engagement levels with the content. By contrast, the possible reach of any content shared on Nextdoor is limited by the nature of the Nextdoor platform to the community of a neighbourhood and those neighbourhoods in close proximity, which protects against content being amplified to reach much wider audiences, as may sometimes be the case on other platforms. Consequently, illegal or harmful content shared on Nextdoor does not have a broad virality risk, as its circulation is limited to the users of the neighbourhood (and sometimes to users in other neighbourhoods in close proximity) for which the piece of content has initially been shared. In that way, content shared on Nextdoor poses a lower risk than that shared on platforms whose architecture allows for unlimited content amplification. Nextdoor would thus invite Ofcom to consider such system specificities alongside other "challenges and limits" when "directly comparing different datasets and measurement methodologies" (point 3.26 of the consultation) - including "The number of users who are
--	---

	assumed to have encountered illegal content, content that is harmful to children, relevant content or content to which section 15(2) applies by means of the service” (points 3 and 22 of of Part 1 (for Category 1) and 2 (for Category 2B) in Schedule 8) - to create an industry-wide outlook. <u>The proportion of users of the service who are children</u> Under points 11 and 18 in Part 1 (addressed at Category 1 services) as well as point 34 in Part 2 (addressed at Category 2B) of Schedule 8 to the Online Safety Act, Ofcom states that it may require providers to disclose information about the “measures taken or in use by a provider to comply with the duty set out in section 64(1) (user identity verification)” (11) as well as the “measures taken or in use by a provider to provide for a higher standard of protection for children than for adults” (18 & 34). In line with Ofcom’s own guiding principles of “relevance” and “appropriateness”, we think that factor (f) under 2.8 in Annex A - “the proportion of users of the service who are children” - is particularly significant to consider. Indeed the relevance and appropriateness of such information in an online safety context will depend on the user age demographic as well as functionality of the service, as these are crucial elements determining the level of risk. These are particularly significant considerations for providers like Nextdoor, which require users in the United Kingdom to be 13 years old or older to join the platform. Nextdoor estimates that over 99% of its global users are legal adults. Further, less than 10% are under 25 years of age. In contrast, we estimate that more than 40% of Nextdoor users are 55 and over. The reason behind the specificity of Nextdoor’s user age demographic is that the overarching utility offered by the platform does not, by nature, appeal to minors. Our platform is used primarily by legal adults who are looking to connect with other nearby
--	---

	residents in order to give and get help and stay up-to-date on the happenings in their neighbourhood. Nextdoor's average user-age thus has important implications for compliance under point 18 ("Measures taken or in use by a provider to provide for a higher standard of protection for children than for adults"). If Ofcom were to require Nextdoor to collect age data of its users, Nextdoor believes that given the low prevalence of minors of its platform, having users input their age at registration would be most appropriate. Nextdoor believes that any further verification of this information would have detrimental effects on the platform's usage. If date of birth collection and verification were required from prospective users, then Nextdoor would expect a significant number of them to decline to join the platform. If date of birth collection and verification were required from current users, we would expect a significant number of them to be unable or unwilling to provide it in order to continue using the platform. These predictions are based on a volume of negative feedback received from users that Nextdoor has asked to supply identification documentation in the past. With that in mind, we wish to highlight that once the proportion of minors using the platform is considered, the relative risk posed by the lack of mandatory age collection measures becomes much lower.
Is there anything that Ofcom should have regard to (other than the factors discussed in the draft guidance) that may be relevant to the production of provider transparency reports? This might include factors that we should consider when deciding how much time to give providers to publish their transparency reports.	Confidential? – No <u>Existing transparency reporting practices</u> Nextdoor supports Ofcom's decision to add "additional criteria" for consideration to those already decreed by the Online Safety Act, including "whether the service provider has already published the information and how different types of information will enable Ofcom to analyse trends across the industry and over time" (point 3.22 of the consultation). Nextdoor has been producing annual transparency reports since 2022. We believe it would be valuable for Ofcom to recognise the

	proactive steps some services have already taken in publishing transparency data. In the event these platforms are later categorised under OSA thresholds, we recommend the regulator explore ways to take into account providers' existing voluntary initiatives for transparency reporting. This approach could help streamline the process and reduce unnecessary administrative burdens on the services in question. <u>Harmonising international transparency requirements</u> Nextdoor supports Ofcom's openness towards international regulatory engagement in developing their transparency regime. We appreciate that the regulator has "taken note of a variety of legislative frameworks, including the EU's Digital Services Act (2022)" and "the lessons gleaned from their implementation experience" (point 3.39 of the consultation). Nextdoor strongly believes in the importance of engaging with "international experts and regulators" to "seek alignment in processes and approaches where feasible and useful" (3.39). Such streamlining of transparency reporting processes, where relevant, could significantly reduce the burden on service providers, and create clarity for providers operating across multiple jurisdictions. We recognise the need for Ofcom to implement an independent online safety regime, tailored to specific needs and priorities identified in the UK. Nevertheless, we recommend that the regulator consider that many providers categorised under the OSA will also be subject to other regimes, such as the European DSA. Where objectives align, we suggest that British and European regulators explore opportunities for cooperation. Harmonising - or at least, ensuring consistency between - reporting requirements across jurisdictions would ensure that providers do not need to invest substantial extra resources into producing parallel data streams as well as separate reports at different
--	--

	times of the year, which will be particularly significant for smaller providers with more limited capacities.
What are the anticipated dependencies for producing transparency reports including in relation to any internal administrative processes and governance which may affect the timelines for producing reports? What information would be most useful for Ofcom to consider when assessing a provider's "capacity", by which we mean, the financial resources of the provider, and the level of technical expertise which is available to the service provider given its size and financial resources?	Confidential? – No We recognise that in point 2.1 of the draft guidance, Ofcom anticipates that "relevant service providers will have between 2 and 6 months to produce their transparency reports in response to a notice" and that "timings will vary depending on factors such as the scope and nature of the information required by the notice and the capacity of the provider." Nextdoor appreciates the regulator's flexible approach to timings. Below we offer further insights into the timeline dependencies that may affect providers' timelines for producing information reports. <u>Timeline dependencies</u> We expect that many of the services categorised under the OSA will be publicly traded companies, with very specific deadlines for the publication of investor reports. Nextdoor would encourage the regulator to consider providers' existing data reporting commitments and timelines when setting transparency reporting deadlines to facilitate the process for relevant businesses and ensure that they have adequate opportunities for <i>both</i> commercial <i>and</i> regulatory compliance. We welcome Ofcom's approach to open communication and its intention to provide ample notice to providers. We believe that open communication around, and providing flexibility in, timings for transparency reporting would not relax the obligations, but rather allow providers to productively think through business and regulatory requirements. Nextdoor typically publishes its own reporting in Q1 (February). We understand that Ofcom will not be able to adjust its own transparency reporting deadlines to the individual timeline of every relevant provider given the sheer volume of categorised services. As a starting point,

	however, it would be helpful for Ofcom to consider general financial business reporting cycles, when issuing transparency notices. <u>Understanding providers' capacity relative to the risk of harm</u> We note that in A1.14 of the consultation, the regulator expects that their "proposed engagement through the draft notice process may require service providers to obtain additional resources to review, analyse and respond to the draft notices" and that "additional staff or more time from current staff may be needed to deal with this regulatory process on an annual basis." Nextdoor urges the regulator to prioritise the principle of "proportionality" when considering the calibre of additional resources that its transparency notices may require providers to allocate to data reporting. We endorse Ofcom's intention for the online safety regime to create "stronger safety governance in online services" (point 3.5 of the consultation). Nevertheless, we believe it is crucial for the regulator to carefully weigh the potential impact of extensive transparency reporting demands against the risk of diverting resources away from company-driven safety initiatives and innovation that contribute to the overall aim of improved online safety.
Are there any matters within Schedule 8, Parts 1 and 2 of Act that may pose risks relating to confidentiality or commercial sensitivity as regards service providers, services or service users if published?	Confidential? – No <u>Insight into the design and operation of algorithms</u> Nextdoor notes that Ofcom reserves the right to request information about providers' unique algorithms to better understand how illegal or harmful content may be circulated on their services. In particular, points 9 of Part 1 and 27 of Part 2 under Schedule 8 specify that the regulator may request information about "the design and operation of algorithms which affect the display, promotion, restriction or recommendation of illegal content, content

	that is harmful to children, relevant content or content to which section 15(2) applies.” We would welcome further detail on the scope of insight into the functioning of algorithms that Ofcom may require and the way this information may be used. Nextdoor is particularly concerned about the business ramifications of sharing information about the inner workings of algorithms, especially where this information would not be kept confidential. Should Ofcom share information on the intricacies of service providers’ individual algorithms - in its own transparency report, for instance - it would risk compromising business competitiveness. The algorithms used by online service providers are commercially sensitive in nature and we therefore urge the regulator to ensure that should such data need to be shared by a provider, it could be done in a strictly confidential manner, or in ways in which the general design of the algorithm is explained without giving away commercially sensitive information. In addition, if Ofcom were to require services to disclose detailed information regarding the operation of their platforms’ algorithms, it may provide insights to those who wish to evade these algorithms in order to advance illegal or harmful content. As such, detailed public disclosures about the operation of algorithms designed to promote safe and secure online environments risks diminishing the effectiveness of these same algorithms. For this reason as well, we again urge the regulator to ensure that, to the extent any such information must be shared by a service provider, it should be done in a strictly confidential manner, or in ways that do not risk undermining the effectiveness of algorithms that promote online safety.
--	--

Question	Your response
Finally, we are also seeking input into any matter that may be helpful for ensuring Ofcom’s transparency reports are useful and accessible.	

Beyond the requirements of the Act, are there any forms of insight that it would be useful for Ofcom to include in our own transparency reports? Why would that information be useful and how could you or a third party use it?	Confidential? – Y/N
Do you have any comment on the most useful format(s) of services' transparency reports or Ofcom's transparency reports? How can Ofcom ensure that its own transparency reports are accessible? Provide specific evidence, if possible, of which formats are particularly effective for which audiences.	Confidential? – Y/N

Question	Your response
Please provide any other comments you may have.	
General comments	Confidential? – Y/N

Please complete this form in full and return to OS-Transparency@Ofcom.org.uk