**Grindr: Responses to Ofcom's consultation "New priority offences - serious self-harm and cyberflashing"**

**Question 3: Do you agree with the risk factors proposed for the Risk Profiles for cyberflashing?**

We agree that cyberflashing should be included in the Risk Profiles and that platforms should assess their risk. We do not agree that the risk factors, as currently framed, will produce accurate risk assessments across the full range of regulated services.

The government has framed increased regulatory action on cyberflashing as existing, first and foremost, to protect women and girls. The YouGov survey cited by the government found that one in three teenage girls had received unsolicited genital images, overwhelmingly from men. That is the harm these provisions are designed to address, and rightly so. Yet, as the proposed risk factors focus primarily on whether a service enables direct messaging with image-sharing functionality, Grindr (and many other services) would be assessed as high risk for cyberflashing. That assessment would be misleading, because it conflates sharing of images, including intimate images, with sharing of images without consent.

Grindr is a platform specifically designed for gay and bi men to identify potential partners and assess romantic suitability. The harm that the cyberflashing offense is designed to prevent does not occur on Grindr. Instead, it subjects gay and bi men's lawful private communications to a level of regulatory scrutiny that lacks an equivalent for comparable heterosexual services, and it does so on the basis of a lack of understanding of how gay and bi men relate to one another and what they expect from online spaces like Grindr.

Intimate images on Grindr are shared between consenting adults who are mutually engaged in sexual conversation, on a platform they have chosen precisely because it facilitates that exchange. All profiles on Grindr can set whether and how they would like to receive "NSFW" pictures (users can select "Yes", "Not at first" or "Never") and can access and change this setting at any time. Classifying this as at high-risk of cyberflashing does not reflect the reality of the offence or the service. It reflects an assumption that intimate image exchange is automatically unsafe, which is an assumption rooted in a mainstream, heterosexual framing of digital sexual interaction that does not apply to the community Grindr serves.

Indeed, the need for this nuance is already explicitly recognised by Ofcom in Paragraph 1.93 of the draft ICJG. That guidance correctly states that intent or recklessness should not be inferred where there is 'evidence of consent' or where the exchange is a 'commonly accepted part of the culture' of the service.

The risk profile should distinguish between platforms where unsolicited sexual images are an intrusion into a non-sexual context and platforms where intimate image exchange between adults is a routine feature of interaction. Failing to draw that distinction omits an understanding of how gay and bi men relate to one another on a platform built for and by that community. We recommend that the risk factors include:

- Whether the service is restricted to adults and has age assurance in place. An adults-only, age-assured service presents a fundamentally different risk profile from a service accessible to children.
- Whether intimate image exchange between consenting adults is a likely feature of the service. On platforms where users have opted into a context that includes sexual expression, the baseline probability that any given intimate image constitutes an offence is lower than on platforms where such content is unexpected.
- Whether the service is designed for and predominantly used by a community with distinct cultural norms around intimate image exchange. A risk framework that does not account for cultural reality does not produce accurate risk assessments. It produces assessments that treat the ordinary sexual culture of gay and bi men as a liability, which is neither just nor proportionate under the Equality Act 2010.
- The availability and effectiveness of user controls - blocking, reporting, content management tools - that enable users to manage their experience.
- The rate of user reports of unwanted or non-consensual images, relative to the volume of image sharing. This is a more reliable indicator of actual cyberflashing risk than the total volume of intimate images.

A risk profile that focuses on whether a service enables intimate image sharing via direct messaging, without accounting for user context and the consent dynamics of the platform, would over-state the cyberflashing risk on services like Grindr and produce a risk assessment that does not correspond to the actual prevalence of the offence.

Indeed, the need for this nuance is already explicitly recognised by Ofcom in Paragraph 1.93 of the draft ICJG. That guidance correctly states that intent or recklessness should not be inferred where there is 'evidence of consent' or where the exchange is a 'commonly accepted part of the culture' of the service.

**Question 5: Do you have any views on our proposed changes to the cyberflashing section of the Register of Risks?**

The Register of Risks should reflect the full range of contexts in which intimate images are shared online, including contexts where such sharing is consensual (whether explicitly or implicitly) and an established part of the cultural norms of the community the platform serves.

The current evidence base for cyberflashing - including the YouGov survey cited by the government, which focused on teenage girls aged 12–18 - describes the experience of unsolicited images on general platforms or through services like AirDrop. Notably, this survey also showed that only 5% of boys in the same age group reported similar experiences, reinforcing that cyberflashing is fundamentally a gendered issue disproportionately affecting women and girls. It does not describe the experience of adult users on sex-positive platforms, including those for adult gay and bi men, where image exchange is a routine feature.

We would welcome the Register acknowledging that different platform types carry different levels of cyberflashing risk, and that the factors that drive risk vary by context. On a general social media platform accessible to children, any direct message containing genital imagery

is likely to be unwelcome and may well constitute the offence. On an adults-only, age-assured dating platform designed for gay and bi men, the picture is fundamentally different: intimate image exchange is a common part of interaction. Treating these two contexts as equivalent produces a framework that disproportionately burdens the gay and bi community, whose sexual culture falls outside the heterosexual mainstream that this regulation was designed to address.

**Question 7: Do you have any views on our proposed updates to the cyberflashing section of the ICJG?**

The Illegal Content Judgements Guidance is critical for platforms like Grindr, and we believe it requires more detailed treatment of how platforms should assess the s.66A offence in the context of private messaging between adults.

The cyberflashing offence is unusual among the priority offences in that it is not defined by the content of the image alone. A photograph of genitals sent in a private chat may be perfectly lawful (between consenting adults engaged in a mutual exchange) or criminal (sent with intent to cause alarm or for sexual gratification with recklessness as to distress). The image itself is identical in both cases. The distinction lies entirely in the sender's mental state and the context of the exchange.

Platforms cannot assess intent and consent directly. What platforms can assess are contextual signals: whether the conversation was mutual and ongoing before the image was sent; whether the recipient had communicated willingness to receive such content; whether the recipient reported the image; whether the sender's behaviour suggests a pattern of unsolicited contact.

On Grindr, the contextual baseline is that image exchange is expected and indeed desired. Users have downloaded an adults-only app for sexual and romantic connection, completed age assurance, and entered into private messaging with another user to assess if they are a romantic and sexual match. In this context, the sending of an intimate image does not, without more, carry the same inference of harmful intent that it would on a professional networking platform or a general messaging service. This is a factual observation about the cultural norms of the community Grindr serves.

We recommend that the ICJG:

- Acknowledge explicitly that the presence of a genital image in a private message is not, on its own, sufficient to constitute illegal content under s.66A. The mental element must also be present. While we welcome Paragraph 1.2 and Paragraph 1.92, which require both a conduct and a state-of-mind element, this principle must be applied consistently across all regulatory documents. Provide guidance on the contextual factors platforms should consider when assessing whether content is likely to meet the threshold - including the nature of the service, whether the exchange appears mutual, and whether the recipient has reported the content.
- Recognise that on services where intimate image exchange is expected and commonplace, user reports are the most reliable indicator that a specific exchange was non-consensual, and that the absence of a report is a reasonable (though not conclusive) contextual factor.

Without this guidance, platforms like Grindr face an impossible operational choice: treat every genital image as potentially illegal content (requiring intervention in millions of consensual private exchanges) or rely on user reports (which may be characterised as insufficiently proactive). Clear, context-sensitive guidance resolves this.

**Question 9: Do you have any comments on our proposed approach to updating the Codes, in light of the creation of the two new priority offences?**

We support the principle that existing code measures should apply to cyberflashing where relevant. Our concern is with how "where relevant" is interpreted for adult platforms where consensual intimate image exchange is a core function. Specifically, whether that interpretation will reflect any meaningful understanding of how gay and bi men use platforms like Grindr or whether it will default to a general-platform standard that was not designed with this community in mind.

The proposal that the blocking and muting measure (ICU J1) should apply to services at risk of cyberflashing is reasonable and proportionate. Grindr already provides users with the ability to block any other user instantly and to report content or behaviour. We support the application of this measure to cyberflashing.

However, the extension of other code measures - particularly content moderation measures - to cyberflashing should be approached with care when applied to adult platforms. We address this in detail in our response to Q11. The key principle is that the same measure may be proportionate on one type of platform and disproportionate on another, depending on user context, and the Codes should allow for this distinction in their application.

**Question 11: Do you have any views on the proposed changes to the application of the Content and Search Moderation measures or the impacts we have identified?**

If the extension of content moderation measures to cyberflashing is interpreted to require proactive automated scanning of private messages for nudity on adult platforms, this would be disproportionate.

Private chat is where adults communicate in ways that include sexual expression. Intimate images - including images of nudity - are exchanged as a routine part of this interaction. If Grindr were required to deploy automated nudity detection across all private messages, every such image would be flagged. The system would be intervening in consensual exchanges between adults, at enormous scale, to identify the tiny proportion that may be non-consensual.

The proportionate approach for adult platforms is to ensure that users have effective tools to manage unwanted content. Grindr provides:

- **Blocking:** users can block any other user instantly, preventing all further contact.
- **Reporting:** users can report unwanted content easily, with reports actioned by the moderation team.
- **Community guidelines:** Grindr's guidelines communicate clearly that consent matters in private exchanges.

- **Age assured:** all UK users are age-assured, ensuring the platform serves adults only.

These measures target the actual harm - the non-consensual receipt of unwanted images - through the mechanism best placed to identify it: the recipient. They do not require the platform to make judgements about sender intent in millions of private exchanges where both participants are willing. They are proportionate to the risk, operationally feasible, and more likely to reduce the actual incidence of cyberflashing than blanket automated scanning that would generate overwhelming volumes of false positives on a platform like Grindr.

Section 18(4) of the Act requires that measures recommended in codes of practice are proportionate to the risk of harm. On a platform where the vast majority of intimate image exchange is consensual, the risk of harm from cyberflashing - while not zero - is materially lower per-image than on a general platform, and the cost of proactive scanning (in terms of interference with lawful expression) is materially higher. The balance of proportionality favours user-empowerment measures.

**Question 15: Do you have any views on the proposed changes to the application of the User Controls measures or the impacts we have identified?**

We support the application of user controls measures to cyberflashing. User controls - including blocking, reporting, and the ability to manage interactions - are the most proportionate and effective approach for reducing cyberflashing on adult platforms.

We would welcome Ofcom recognising, in its guidance, that user controls can serve as the primary compliance mechanism for adult, age-verified platforms where intimate image exchange is expected. On such services, giving users effective tools to control what they receive and to report unwanted content is both more proportionate and more effective than requiring the platform to pre-screen all private messages for nudity.

The effectiveness of user controls depends on their accessibility, visibility, and the speed with which the platform acts on reports. Grindr is committed to ensuring that its reporting and blocking tools are easy to use, prominently available, and that reports are actioned swiftly.

**Question 17: Do you agree with our assessment of the combined impacts of our proposals set out in the Combined Impact Assessment?**

The impact assessment should explicitly address the effect of the proposals on adult LGBTQ+ platforms.

The government has framed cyberflashing principally as part of its commitment to halve violence against women and girls. That framing reflects a real and serious problem: YouGov data indicates that one in three teenage girls has received unsolicited images of male genitalia. We do not dispute this evidence or the policy priority behind it.

However, the regulatory framework applies to all regulated services, including those serving communities where the dynamics of intimate image sharing are qualitatively different. On Grindr, the user base is adult gay and bi men using a platform designed for sexual and romantic connection with other men. Image exchange is not an intrusion; it is an expected

feature. A regulatory approach designed solely for the paradigm of unsolicited images sent to women on general social media may not produce sensible outcomes when applied, without calibration, to a platform like Grindr.

Sexual orientation is a protected characteristic under the Equality Act 2010. Grindr serves a community for whom the platform is, for many, the primary means of meeting sexual and romantic partners. Regulatory measures that disproportionately restrict how adult LGBTQ+ users interact on a platform designed for their community should be subject to careful proportionality analysis. We ask Ofcom to ensure that the combined impact assessment considers this dimension explicitly.