Iris

Response to Ofcom Consultation: New Priority Offences - Serious Self-Harm and Cyberflashing

Respondent: Iris Anticipa Ltd

Submitted by: [redacted] Founder and CEO

Contact: [redacted]

Date: 24 April 2026

Consultation reference: Consultation on Updates for New Priority Offences, published 24 March 2026

Summary

Iris Anticipa Ltd supports Ofcom's proposal to treat suicide and self-harm as a single kind of illegal harm for risk assessment, and to add cyberflashing as a separately risk-assessed priority illegal harm. We write to offer one substantive observation, drawn from building detection technology for this space.

Both offences, as Ofcom itself acknowledges for cyberflashing at paragraph 2.25, are expressions of behaviour that unfolds across conversations and over time. The continuum of abuse online and offline - a framing the Domestic Abuse Commissioner placed before the Online Safety Bill Public Bill Committee, and which Parliament has subsequently reinforced through the Victims and Prisoners Act 2024 and SI 2025/1352 - is exactly the continuum these updates now need to operationalise. The proposed updates to the Risk Profiles, the Register of Risks and the Illegal Content Judgements Guidance will be stronger if they explicitly recognise a behavioural-pattern signal layer alongside content. A pattern layer, operating on the trajectory of interactions rather than individual messages, is a structural complement to content-level detection. Ofcom can anchor it in the Risk Profiles and the ICJG now, without reopening scope.

1. Who we are

Iris Anticipa Ltd is a UK SME developing technology that detects coercive, fraudulent, exploitative and manipulative patterns across digital conversations. Our portfolio comprises seven patent families, forty-four specifications and more than 865 claims filed in the UK, covering the signal-processing architecture for pattern detection across messaging, voice and multi-agency intelligence. We are not a content-moderation vendor. Our technology operates on the trajectory of interactions, not on their content.

We submit this response in our own capacity and name as a UK provider of relevant technology. We would welcome the opportunity to share our technical evidence base with Ofcom in future consultation cycles and working groups.

2. Q1: Combining suicide and self-harm as a single kind of illegal harm

We agree with the proposal. In practice, the behavioural patterns associated with the two offences overlap materially inside private messaging, inside closed community spaces, and along the trajectory by which users are drawn into progressively more harmful content. Treating them as a single risk-assessed category is proportionate, matches the evidence from survivor-led and clinical research, and follows the legislative logic

of The Online Safety Act 2023 (Priority Offences) (Amendment) Regulations 2025 (SI 2025/1352), under which Parliament designated both offences on the same statutory footing.

3. Q2 and Q3: Risk factors for the proposed Risk Profiles

We support the risk factors Ofcom has proposed for both Profiles. We suggest one addition for each.

Suicide and self-harm (Q2). Explicitly include **behavioural-trajectory risk factors inside private messaging and persistent groups**, in addition to the recommender-system and discovery-surface factors already in scope. Recommender-driven filter bubbles are a real harm-vector (paragraph 3.80). They are not the only one. A significant share of self-harm escalation happens inside direct-message threads and small closed groups, where the harm trajectory is not a content classification problem but a pattern-across-conversations problem. Risk factors that belong in the Profile include: repeat engagement with the same at-risk user by the same sender over time; acceleration in message cadence; escalation in the severity of material shared; and persistent attempts to route a conversation off-platform. These are measurable signals that do not require content classification to operate.

Cyberflashing (Q3). Explicitly include **repeat-sender targeting patterns** as a risk factor. Ofcom already acknowledges at paragraph 2.25 that cyberflashing *"is a manifestation of existing patterns of sexual violence and abuse... can form part of a pattern of harmful behaviour that includes stalking, harassment and coercive or controlling behaviour."* That framing belongs in the Risk Profile itself, not only in the narrative section. The operational signal is not the single image - by the time an image is sent, the perimeter has been crossed. The signal is the pattern: multiple unsolicited sends from the same actor across sessions, targeting selection, escalation from messaging to media request to unsolicited media, and coordinated behaviour across adjacent accounts. Refuge research cited to the Online Safety Bill Public Bill Committee in 2022 already indicated that 59% of survivors had experienced coercive control through social media. Including pattern-level risk factors in the Profile gives providers clear direction on what to risk-assess against.

4. Q4 and Q5: Register of Risks

We welcome the proposed changes. In the cyberflashing section (Q5), we suggest adding a short note that the harm is, in a meaningful share of cases, repeat-sender and pattern-driven rather than one-off. Mirroring paragraph 2.25 in the Register itself ensures the pattern framing is carried through to the operational content that providers actually engineer against.

In the suicide and self-harm section (Q4), we suggest explicit recognition that private-messaging and closed-group trajectories are in scope alongside recommender-driven surfaces. The Register of Risks is the right document in which to make that split visible.

5. Q6 and Q7: Illegal Content Judgements Guidance

We support the proposed updates. In both sections of the ICJG we suggest that judgement criteria recognise cumulative and pattern-level evidence as relevant to a provider's assessment of illegality, not just single-message content signals.

This is consistent with a clear UK statutory progression that Parliament has endorsed over the past decade:

- **Section 76 of the Serious Crime Act 2015** criminalised controlling or coercive behaviour in an intimate or family relationship as a pattern-level offence.

- **Section 1(3)(c) of the Domestic Abuse Act 2021** codified controlling or coercive behaviour as a recognised form of domestic abuse in statute.
- **The Victims and Prisoners Act 2024,** in force from 3 February 2025, now places controlling or coercive behaviour on a par with other domestic abuse offences under MAPPA (Multi-Agency Public Protection Arrangements).

Cumulative, pattern-level evidence is therefore how UK law now frames the most analogous offline harm. The ICJG should reflect the same evidential logic for the online expressions of these behaviours. No change to the statutory thresholds in the Online Safety Act is required for Ofcom to make that reflection explicit in the Guidance.

6. Q13: Recommender Systems

We broadly support the proposed approach to recommender systems for suicide and self-harm. We would, respectfully, flag paragraph 3.83 - *"We are not aware of evidence suggesting that content recommender systems are a risk factor for cyberflashing"* - as an area where the Risk Profile should nonetheless remain open to pattern-level evidence. The primary cyberflashing risk-vector is messaging and profile-discovery behaviour, not discovery-feed recommendation. The Risk Profile and the ICJG together should therefore place greater weight on messaging-trajectory and repeat-sender signals for cyberflashing than on recommender-system signals. We would welcome the opportunity to share our technical evidence base on this point.

7. Q20: Cross-cutting observation - proactive technology

Proactive-technology measures as currently scoped (ICU C11 and C12) sit principally at the content layer. Both offences are expressions of patterns of behaviour that precede and surround the detectable content. We encourage Ofcom, when the proactive-technology criteria are next revised, to recognise behavioural-pattern detection as a technically feasible and privacy-compatible complement to content-level proactive technology.

Pattern-level detection does not require content exposure, does not depend on cross-platform data sharing, and can operate on metadata-level features alone. These properties matter for survivors and for children, because they allow anticipatory risk-identification without recreating the privacy concerns associated with legacy content-monitoring approaches.

This posture is aligned with the direction of cross-government practice: the National Cyber Security Centre has, with Police Cyber PROTECT, independent domestic violence advisors and charity partners, published practitioner guidance recognising technology-facilitated domestic abuse as a distinct category of harm. Pattern-level detection is the technical counterpart to that front-line recognition.

We are prepared to engage with Ofcom, survivor-led organisations and child-safety charities on how pattern-level detection is specified, evidenced and held accountable.

[redacted]
Founder and CEO, Iris Anticipa Ltd
[redacted]

Sources cited

Ofcom, Consultation on New Priority Offences: Updates in Light of the New Priority Offences of Cyberflashing and Encouraging or Assisting Serious Self-Harm, 24 March 2026.

The Online Safety Act 2023 (Priority Offences) (Amendment) Regulations 2025, SI 2025/1352.

Serious Crime Act 2015, s.76 (controlling or coercive behaviour in an intimate or family relationship).

Domestic Abuse Act 2021, s.1 (definition of domestic abuse).

Victims and Prisoners Act 2024 (MAPPA extension to controlling or coercive behaviour, in force 3 February 2025).

Domestic Abuse Commissioner, written evidence to the Online Safety Bill Public Bill Committee, 2022.

National Cyber Security Centre, Guidance for practitioners supporting victims of technology-facilitated domestic abuse, 2024.

Simon Moseley, Automating Deception: AI's Evolving Role in Romance Fraud, CETaS Briefing Papers (Centre for Emerging Technology and Security, Alan Turing Institute), April 2025.