Illegal Harms Updates – New Priority Offences (Self-harm & Cyberflashing)

Submitted by:
Independent civic stakeholder (Romania / EU)- NGO ,,[redacted] ‘
Focus: user safety, vulnerable users, and systemic risk in digital environments

---

1. General Position

I welcome Ofcom’s proposed updates to reflect the inclusion of **encouraging or assisting serious self-harm** and **cyberflashing** as priority offences under the Online Safety Act.

The alignment of regulatory documents (Risk Assessment Guidance, Register of Risks, Codes of Practice, and ICJG) demonstrates a **coherent system-level approach**, which is essential for addressing modern online harms.

In particular, I support:

- The integration of **self-harm into a broader “suicide and self-harm” risk category** for assessment purposes;
- The recognition of **cyberflashing as a distinct illegal harm requiring separate risk evaluation**;
- The emphasis on **risk-based obligations** rather than purely reactive content moderation.

---

2. Key Observations and Recommendations

2.1. Risk Must Be Treated as Systemic, Not Merely Content-Based

The consultation correctly highlights that harms are driven not only by content, but by:

- platform design,
- functionalities,
- user interaction patterns,
- and algorithmic systems.

However, this principle should be **more explicitly operationalised**.

Evidence within the Register of Risks shows that high-risk functionalities include:

- recommender systems,
- private and encrypted messaging,
- anonymity/pseudonymity,
- livestreaming features.

👉 Recommendation:
Ofcom should require **explicit mapping between each high-risk functionality and mandatory mitigation measures**, rather than leaving this primarily to provider discretion.

2.2. Distinction Between Suicide and Self-Harm Should Be Preserved Operationally

While combining suicide and self-harm into a single risk category may simplify risk assessment:

👉 In practice, these phenomena differ significantly in:

- intent,
- vulnerability patterns,
- intervention pathways.

There is a risk that:

- operational responses become too generic,
- or that critical signals are diluted.

👉 Recommendation:
Maintain **a unified risk category**, but require:

- **separate internal detection models**,
- and **distinct intervention protocols** for:
    - suicidal intent content,
    - non-suicidal self-harm content.

2.3. Early Intervention Obligations Should Be Strengthened

The framework relies heavily on:

- risk assessments,
- governance structures,
- and content moderation systems.

However, the **actual moment of harm** often occurs:
👉 before content reaches clear illegality thresholds.

Given that providers operate under a “reasonable grounds to infer” standard

👉 Recommendation:
Introduce stronger expectations for:

- **early-stage detection signals**,
- **preventive friction (e.g., prompts, delays, warnings)**,
- and **real-time user support mechanisms**.

This is especially relevant for:

- self-harm escalation,
- repeated targeting (cyberflashing),
- and vulnerable user journeys.

2.4. User Controls Must Be Default, Not Optional

The Codes propose measures such as:

- blocking,
- muting,
- disabling comments,
- reporting tools.

However, their effectiveness depends entirely on:
👉 usability and default configuration.

👉 Recommendation:
Ofcom should require that:

- key safety controls are **enabled by default for high-risk contexts**,
- not buried in settings or dependent on user awareness.

Particularly important for:

- minors,
- new users,
- and victims of repeated abuse.

2.5. Protection of Vulnerable Users Requires Stronger Focus

The Register of Risks confirms:

- harms disproportionately affect **children and vulnerable individuals**,
- and risk increases with cumulative vulnerabilities.

Yet the current proposals remain largely **platform-centric**, rather than **user-centric**.

👉 Recommendation:
Require providers to:

- explicitly identify **vulnerable user segments**,
- and implement **targeted safeguards**, including:
    - adaptive risk thresholds,
    - enhanced moderation,
    - contextual support interventions.

---

3. Governance and Accountability

The Codes of Practice appropriately emphasise:

- governance,
- accountability structures,
- and internal monitoring systems.

👉 Recommendation:
Strengthen this further by requiring:

- **clear internal ownership of user safety outcomes (not just compliance)**,
- and **periodic external validation or audit** for high-risk services.

---

4. Final Remarks

Ofcom's approach represents a **major step forward** in regulating online harms through:

- systemic risk analysis,
- cross-document coherence,
- and adaptive regulatory design.

However, to ensure real-world effectiveness, the framework should:

- move further from **formal compliance → to functional safety outcomes**,
- and from **content moderation → to system design accountability**.