

Written evidence submitted by South West Grid for Learning (SWGfL) and UK Safer Internet Centre (UKSIC) (VAWG0084)

SWGfL is a 25-year-old UK-based charity, dedicated to ensuring that *everyone should benefit from technology, free from harm*. As a recognised leader in online safety, SWGfL has driven policy, technology, and victim support efforts to tackle NCII and wider digital harms.

Beyond national efforts, SWGfL is recognised for its global influence, working with major intergovernmental organisations such as the United Nations International Telecommunication Union (ITU), the Council of Europe, and the World Economic Forum to advance online safety policy and digital harm prevention worldwide.

SWGfL's direct action to tackle NCII and TFVAWG includes the operation of the UK's Revenge Porn Helpline and the creation of StopNCII.org, an innovative, global solution designed to prevent the spread of intimate images online.

The Revenge Porn Helpline (UK) (<https://revengepornhelpline.org.uk/>)

The Revenge Porn Helpline, part of SWGfL, is the UK's specialist service providing practical support, primarily focused on content reporting and takedown to UK victims who are adults affected by NCII. Since its launch in 2015, it has handled a dramatic increase in cases, rising from 1,600 in 2019 to over 22,000 in 2024, offering victims specialist guidance and intervention services.

Key statistics:

In 2023, the helpline experienced a 12-fold increase in cases compared to 4 years earlier.

90% of victims are women, often where there is a previous relationship involved, highlighting the gendered nature of NCII.

Services provided:

Image removal: Works directly with technology companies to report and request removal of images, with 94% of reported content successfully taken down.

Policy engagement: Influences UK and international legislation, shaping key NCII-related provisions within the Online Safety Act and beyond.

StopNCII.org: A Global, Tech-Enabled Solution (<https://stopncii.org/>)

StopNCII.org is a world-first, survivor-centred initiative developed by SWGfL in collaboration with leading technology companies to prevent the spread of NCII. The platform provides a free, secure, and privacy-preserving solution that empowers individuals to take proactive action against the unauthorised sharing of their intimate images.

How it works:

Users create a unique digital fingerprint (hash) of their image securely on their own device.

These hashes are shared with participating platforms (Facebook, Instagram, TikTok, Microsoft Bing, OnlyFans, Reddit, Snap, Aylo, Threads, Niantic, Redgifs, Playhouse and Bit.ly (currently)).

If an image matching a stored hash is uploaded, it is automatically blocked, restoring power to the victim before it can be made public.

Key impact:

More than 1 million hashes have been created, demonstrating high global engagement.

Written evidence submitted by South West Grid for Learning (SWGfL) and UK Safer Internet Centre (UKSIC) (VAWG0084)

Integrated into leading platforms (Facebook, Instagram, TikTok, Microsoft Bing, OnlyFans, Reddit, Snap, Aylo, Threads, Niantic, Redgifs, Playhouse and Bit.ly), setting a new industry standard for proactive NCII prevention.

Recognised by regulators, policymakers, and survivor networks as a best-practice intervention.

StopNCII.org also collaborates with 107 NGOs worldwide, extending its reach to victim support organisations that provide direct assistance to those affected by NCII.

We have also drawn on the key findings and recommendations from the **Women and Equalities Committee Report on Tackling Non-Consensual Intimate Image (NCII) Abuse**, published in 2025, to highlight gaps in current policies and propose urgent reforms to **strengthen protections, hold online platforms accountable, and improve victim support**.

Our evidence focuses on:

- The prevalence of NCII abuse and its impact on victims.
- Shortcomings in the current legal and regulatory framework.
- Necessary policy changes to strengthen protections for women and girls online.
- The role of online platforms in mitigating NCII abuse.
- Improvements in victim support mechanisms.
- The Women and Equalities Committee (WEC) Report on Tackling NCII Abuse

1. The Current Landscape of NCII Abuse

- a. While the Revenge Porn Helpline has over a 90% success rate in removing over 350,000 images, approximately 30,000 images remain online and accessible due to jurisdictional limitations and legal barriers.
- b. The websites hosting this NCII content often operate outside UK jurisdiction, deliberately choosing locations that enable them to host NCII content with impunity.

2. Key Challenges and Policy Gaps

- a. NCII possession is not criminalised: While the sharing of intimate images without consent is an offence, mere possession remains legal, allowing perpetrators to store and redistribute content.
- b. Deepfake abuse is not fully covered: The current legal framework does not explicitly criminalise the creation of sexually explicit deepfake images.
- c. Insufficient platform accountability
- d. Lack of mandatory hash-matching technology: While StopNCII.org provides a tool to prevent the re-uploading of known NCII content, many platforms have not integrated it.
- e. Lack of training and resources: Many victims report re-traumatisation due to police mishandling of NCII cases. Officers often do not understand the issue or urgency of removing content.

3. Recommendations for Policy and Legislative Reform

Written evidence submitted by South West Grid for Learning (SWGfL) and UK Safer Internet Centre (UKSIC) (VAWG0084)

- a. Criminalise possession of NCII content: Amending legislation to prohibit possession of non-consensual intimate images, ensuring perpetrators cannot retain harmful content.
- b. Expand the definition of NCII abuse: Updating the legal framework to include deepfake pornography and AI-generated explicit content.
- c. Mandate an NCII takedown service: Establishing a legal obligation for platforms to remove known NCII content within 24 hours of a verified report from the Revenge Porn Helpline.

4. Enforcing Stronger Platform Responsibilities

- a. Ofcom should mandate that StopNCII.org be integrated into all regulated services, preventing re-uploading of known NCII content.
- b. Empower the blocking of non-compliant websites: Websites that consistently refuse to remove NCII content should face ISP blocking and financial disruption.
- c. We propose the creation of a legally mandated NCII Register to classify illegal NCII content, enabling Internet Service Providers (ISPs) to block access and prevent further distribution.
- d. Prevention Over Reactive Removal: Current regulatory and industry responses focus primarily on the removal of NCII content after it has been reported. Hashing technology enables pre-emptive prevention, stopping harmful content from being re-uploaded and reducing the risk of repeated victimisation.

5. Improving Law Enforcement and Victim Support

- a. Expand funding for victim support services: Government funding should be increased to the only specialised NCII helpline - Revenge Porn Helpline.
- b. Develop training programs for law enforcement: Police officers should receive mandatory digital safety training on NCII abuse to assist victims effectively.

6. Public Awareness and Education

- a. Integrate NCII awareness into school, further and higher education curricula: Educating young people about consent, digital safety, and the legal consequences of image-based abuse.
- b. National campaigns on online abuse: Government-funded campaigns should raise awareness of NCII reporting mechanisms and support services.

7. The Women and Equalities Committee (WEC) Report on Tackling NCII Abuse identified several key concerns and recommended:

Legislative & Regulatory Changes

- Criminalisation of NCII & Deepfakes: The Government should ensure that laws criminalising sexually explicit deepfakes (synthetic NCII) are based on lack of consent rather than requiring proof of the perpetrator's intent.
- Possession of NCII as an Offence: The Government should amend the Crime and Policing Bill to make possession of NCII an offence, not just its creation.

Written evidence submitted by South West Grid for Learning (SWGfL) and UK Safer Internet Centre (UKSIC) (VAWG0084)

- Statutory Civil Process: A fast-track, inexpensive statutory civil process should be introduced to allow victims to quickly remove NCII content and claim compensation.
- Extended Time Limits for Prosecution: The statutory time limit for prosecuting intimate image abuse should start only once the victim becomes aware of the abuse.

Support for Victims

- Increase Funding for the Revenge Porn Helpline (RPH): Funding should be increased and made multi-year to ensure sustainability, as demand for RPH services has increased sevenfold since 2020.
- Inclusion in the Criminal Injuries Compensation Scheme: Online sexual offences, such as NCII abuse, should be explicitly included in the Criminal Injuries Compensation Scheme.
- Deprivation of Perpetrators' Devices: Courts should ensure perpetrators do not retain devices containing NCII images, and the Crown Prosecution Service must outline actions to enforce this.

Technology & Online Platforms

- Mandatory Hashing Technology: Platforms should be required to use hash-matching technology (such as StopNCII.org) to prevent reuploads of NCII content.
- Google Should Accept NCII Hashes: Google and other major platforms must integrate StopNCII.org's technology without delay.
- Regulatory Powers for Internet Infrastructure Providers (IIPs): Internet infrastructure providers should have clearer guidance on blocking NCII sites, similar to child sexual abuse material (CSAM) regulation.

Law Enforcement & Governance

- Improving Police Response: The College of Policing, Ofcom, and the RPH should collaborate to produce new police guidance on handling NCII cases.
- Online Safety Commission: A dedicated Online Safety Commission should be established to support victims and oversee a registry of NCII content. Provide authoritative powers to Revenge Porn Helpline to take down content, through the established NCII register
- Culturally Intimate Images Protection: The legal definition of NCII should include cultural violations, such as images of individuals without their religious attire, which could cause significant harm.

Synthetic NCII & AI Concerns

- Ban on Nudification Apps: The use and promotion of "nudification" apps should be criminalised, and Ofcom should investigate platforms that distribute them.
- AI Industry Responsibility: Tech companies involved in AI should cleanse datasets of NCII content and commit to responsible data sourcing, and adequate guardrails, to prevent AI-generated abuse.

Next Steps

Written evidence submitted by South West Grid for Learning (SWGfL) and UK Safer Internet Centre (UKSIC) (VAWG0084)

- Amend legislation (Crime and Policing Bill, Data (Use and Access) Bill) to incorporate these recommendations.
- Ensure proper funding and support mechanisms for law enforcement and victim services.
- Enforce platform accountability through regulatory mandates, requiring adoption of prevention technologies.
- These recommendations aim to strengthen protections for victims, increase enforcement against perpetrators, and hold tech companies accountable for enabling NCII abuse.

8. Conclusion

- a. The Women and Equalities Committee Report on Tackling NCII Abuse has highlighted urgent gaps in law enforcement, legal protections, and platform accountability. Addressing these issues requires bold policy reforms, stronger regulatory enforcement, and enhanced victim support services.
- b. SWGfL and UK Safer Internet Centre urge the Public Accounts Committee to support these policy recommendations and legislative changes to make the online world safer for women and girls.

9. References

- a. Women and Equalities Committee Report on Tackling NCII Abuse: committees.parliament.uk

March 2025