Model National Framework for Addressing Non-Consensual Intimate Images (NCII)

A Preliminary Blueprint for Global Standards for Preventing and Responding to Adult Image-Based Sexual Abuse

The threat or sharing of non-consensual intimate images (NCII) is a type of cybercrime and growing form of technology-facilitated gender-based violence (TFGBV) that is worsening with the rise of generative artificial intelligence (AI). Given its borderless nature, setting international norms to address NCII is imperative, through efforts such as the United Nations Convention against Cybercrime. While the growth in legal frameworks addressing NCII and other forms of TFGBV is welcome progress, the existing patchwork of national, regional and global standards offers mixed levels of protection for victims, weak or inconsistent accountability for offenders, and insufficient requirements for a duty of care across industry. The UK Government, as co-chair of the Global Partnership for Action on Gender-Based Online Harassment and Abuse, together with UN Women, the United Nations Office for Drugs and Crime (UNODC), and SWGfL, home to the UK Revenge Porn Helpline and StopNCII.org, have coordinated a preliminary blueprint for a Model National Framework for Addressing NCII. Drawing on lessons-learned from the WeProtect Global Alliance Model National Response to end Child Sexual Exploitation and Abuse Online, the Model National Framework aims to:

- Identify core elements, suggested and promising practices for a whole-of-society approach to preventing and addressing authentic, synthetic, or manipulated intimate imagery involving identifiable adults that is created, shared, or threatened without consent;
- Support effective implementation of the UN Convention on Cybercrime and promote policies, laws and regulations on adult image-based sexual abuse that are rights-based and survivor-centred, based on the best available evidence, and shaped through multistakeholder engagement;
- Build on and align common efforts to enhance global coordination on TFGBV and related cybercrimes.

Disclaimer: This preliminary blueprint for a Model National Framework is an **aspirational guide** for effective, multi-sectoral approaches to preventing and responding to NCII. While acknowledging the diverse political, economic, and cultural contexts across countries and regions, this blueprint for a Model National Framework—rooted in universal human rights obligations—outlines core elements for building capabilities across six components and offers suggested, promising practices along a continuum of options for national, regional and local decisionmakers, practitioners and industry to consider in implementation. It is not meant to be prescriptive, nor is it intended to create any legally binding obligations under domestic or international law and will not be deemed to constitute or create any legally binding obligations or enforceable obligations, express or implied.

Cross-Cutting Principles

- **Rights-based.** Firmly rooted in international human rights frameworks upholding the right to privacy, freedom of expression, and the rights of women - and all people - to live free from violence and discrimination, the framework recognises national efforts to prevent and respond to NCII will only succeed when states uphold their duty to protect human rights, and the private sector exercises its obligation to respect them, as articulated in the UN Guiding Principles on Business and Human Rights.
- **Survivor-centred.** Efforts to address NCII must be truly survivor-centred and trauma-informed, meaning individuals with lived experience are invited to meaningfully engage from the outset, are routinely consulted, offered care and support and fairly compensated, with their participation grounded in an intersectional approach that recognises how experiences, help seeking, and interactions with the criminal legal system vary across survivor communities, identities, and backgrounds.
- **Evidence-informed.** Effective, survivor-centred NCII policies and regulations must be evidence-informed and shaped by diverse multisectoral expertise, extending to ethical, rights-based approaches to data governance across both government and industry, encompassing the responsible collection, management, storage, and sharing of data.
- **Integrated approach.** NCII must be understood as a both a cybercrime, and form of TFGBV that frequently intersects with other gendered online and offline abuses, requiring laws, policies, research, and interventions to be integrated into—rather than siloed from — broader cybercrime and GBV/VAWG frameworks. Like other forms of GBV, NCII affects everyone, including men, but disproportionately impacts women and LGBTQI+ individuals in all their diversity.
- **Universal standards with adaptable application.** The framework aims to advance universal, survivor-centred standards for NCII laws and policies, anchored in international human-rights principles while adaptable to diverse country and cultural contexts. Because approaches that succeed in one setting may be ineffective—or even harmful—in another, it is essential to sustain and empower civil society and survivor-led NGOs, particularly those operating in low-resource settings and under governments with fragile institutions, so that responses to NCII are grounded in local realities.
- **Multistakeholder, whole-of-society lens.** While laws and regulations are essential, they are not sufficient on their own to prevent and address NCII; lasting change also requires a robust civil society, strong coordination with industry, and active efforts to shift cultural norms away from the objectification of women and girls and the uncritical embrace of digital innovation without safety guardrails.

	Core Elements	Suggested and Promising Practices
Policy, Legislation and Governance *Principles for survivor-centred legal protection and justice for offenders, regulations to promote industry accountability, and coordinated national structures to prevent, deter and respond to NCII.*	**Establish and maintain a clear national policy and legal framework on NCII, aligned to international human rights standards**, recognising its link to cybercrime and existing national GBV/VAWG mechanisms and centred on the harms experienced by victim-survivors. This should explicitly cover the creation, sharing and facilitation of NCII, including synthetic or manipulated content, such as AI-generated material. Legislation should move away from intent-based approaches and promote consent as a central element, or risk being insufficiently effective. **→Principle in Practice:** ● Criminal and civil laws to hold individual perpetrators accountable, without requiring an intent to harm, instead defining the offense based on lack of consent by the person(s) depicted in the image(s). ● Where applicable, civil remedies should allow for victims to recover legal fees and damages, including cost of image removal, along with other services to support victims such as counselling costs and financial losses. ● Criminal and civil penalties apply to both real and synthetic or manipulated intimate images/ video of identifiable adults. **Regulatory frameworks to hold industry accountable** through effective reporting mechanisms, timely and transparent removal processes, and meaningful consequences for platforms that fail to take reasonable steps to address verified NCII. **→Principle in Practice:** Where governments have regulatory bodies in place (or belong to a regional regulatory authority) to monitor private sector compliance with national/regional law, consider enacting regulations that: ● Balance the need for sector-wide user safety standards as well as product or service-specific requirements based on their use or misuse in the creation, dissemination, or monetisation of NCII. ● Require covered platforms to have easily accessible, dedicated reporting channels and strong content moderation policies that facilitate swift removal of verified NCII, with safeguards against false or malicious reports, including efforts to censure individuals or particular forms of content by falsely labelling them NCII. ● Incentivise compliance through fines or penalties, based on expectations platforms make reasonable attempts to remove illegal content in a timely manner. ● Clarify that industry does not have a liability shield with immunity from civil claims when they profit directly from hosting or facilitating NCII, or fail to take reasonable steps to curb illegal, non-consensual content.	**Legal frameworks on NCII include criminal and civil penalties for *threats* to share or create**—in addition to the actual creation or distribution of NCII. Governments will find value in integrating the following survivor-centred protections: ● Integrating protections from and penalties for NCII into existing cybercrime, GBV/VAWG legal frameworks, including laws concerning the right to be free from violence and discrimination in the workplace and education. ● Enacting legal protections for victims of NCII who have been coerced into sex work or trafficking. ● Clarifying legal protections for NCII apply to individuals engaged in consensual sex work or adult content creation. ● As applicable, updating or clarifying copyright laws to grant victims legal rights over images they have taken of themselves, enabling them to exercise ownership over self-generated intimate images or videos shared or manipulated without their consent and providing another tool for relief, with consideration for reasonable defenses, such as public interest. ● Refraining from imposing statutes of limitations for criminal or civil complaints, recognising late discovery inherent in cases of image-based sexual abuse (e.g. victims may be delayed between initial offense/creation or public distribution of NCII and becoming aware of its existence/spread). ● Establishing deepfake/AI-generated NCII of persons running for public office as a prohibited practice in electoral laws and regulations, as well as requiring disclosures of AI-generated material by political parties and campaigns. **Ensuring sustainability and future-proofing national policies and legal frameworks to address NCII**. Governments may also consider the following strategies for sustaining an enduring, evergreen national agenda to prevent and respond to NCII: ● Wherever possible, laws addressing NCII are paired with resilient funding models for specialised helplines and victim services, enabling survivors free, confidential access to support. ● Where regulatory frameworks exist, explore redistribution schemes to allocate fines and penalties for platform non-compliance towards government-funded helplines and other organisations supporting victims of cybercrime. ● Laws are purposefully developed to be future- proofed and are regularly reviewed and updated as needed to cover emerging harms and technologies. ● Engage survivors as lived experience experts through formal structures that facilitate their active participation in shaping, informing, and updating laws and policies on NCII.

Demonstrate political leadership signalling NCII prevention and response as a government-wide priority.

→Principle in Practice:

- Show visible, sustained political leadership on NCII, including clear statements that NCII is a cybercrime and serious form of GBV, not a private or low-level harm.
- Building on/integrating within existing structures to address cybercrime and GBV/VAWG, assign clear senior ownership within government, for example through a designated ministerial lead and a senior official or unit responsible for coordinating national action on NCII across departments and agencies (e.g. ministries of justice, health, education, social welfare, ICT, foreign affairs).
- Where feasible, allocate sufficient and sustained resources to prevention, enforcement and victim-survivor support. This includes funding for law enforcement capability, regulators, victim support services, public awareness campaigns and specialist expertise on NCII and other forms of cybercrime and TFGBV.
- Ensure coordination with national efforts to address online child sexual exploitation and abuse where such efforts exist.

Monitoring, accountability and continuous improvement.

→Principle in Practice:

- National governments have mechanisms to monitor and evaluate the effectiveness of laws, policies, and interventions, using both quantitative data and qualitative feedback from survivors and practitioners.
- Where such mechanisms exist, track trends in prevalence and emerging risks, including changes in technology, offending patterns and impacts on different populations and communities, to promote relevant and effective responses.
- Publish aggregate, population-level, anonymised data and key findings/learnings, promoting transparency and accountability to the public and contributing to international understanding of what works to tackle NCII.
- Based on monitoring prevalence, trends and risks, periodically review and consider reforms to legal definitions of NCII to avoid systematic exclusion of minority populations whose cultural concepts of nudity, intimacy and privacy may differ from the general population, thereby chilling reporting and access to justice for vulnerable groups.

Strengthening industry accountability by pairing regulations with implementation guidelines for transparency and safety-and-privacy-by-design measures, and other strategies to prevent and address the creation, distribution and monetisation of NCII. Governments or regional bodies implementing regulations may consider enhancing industry accountability by:

- Incentivising or encouraging the adoption of privacy-protecting, robust image-hashing tools, like StopNCII.org.
- Banning nudify apps and websites that are designed to facilitate the creation, sale or dissemination of NCII.
- Incentivising platforms to establish trusted flagger programs that fast-track reports of NCII, encouraging responsiveness to civil society requests for removal of illegal content, and exploring funding mechanisms to compensate civil society organisations operating as trusted flaggers.
- Complementing requirements for good faith, timely removal of NCII with independent, third-party audits to evaluate platforms' response times, takedown rates, and the frequency, volume and incidence of verified reports of NCII, recognising reasonable attempts for removing identical or near-identical copies, particularly through the use of perceptual hashing, may take longer.
- Striving to harmonise laws and policies wherever feasible, encouraging industry to apply protections universally and avoiding geofencing so that survivors receive the same level of responsiveness regardless of geography.

Incentivising "good actor" platforms, including small and mid-size tech companies in emerging markets. Governments, regional bodies and regulatory authorities can help advance a safer internet through policy frameworks that:

- Recognise innovative small and mid-size tech enterprises—particularly in emerging markets—that are demonstrating safer rights-respecting practices and contributing to a more trustworthy digital ecosystem.
- Foster market competition through fair data-access rules, enhanced advertising transparency, interoperability requirements for key services, and mechanisms that allow users to easily opt out of platform default settings.

Contributing to international coordination, knowledge exchange and multistakeholder coalitions to counter cybercrime and TFGBV and promote online safety for all. National agendas to prevent and respond to NCII are strengthened by active engagement in international and multilateral efforts, including:

- Global coalitions for exchanging knowledge, sharing best and promising practices, and advancing international, rights-based norms and practices to combat cybercrime and end TFGBV, such as the Global Partnership for Action on Gender- Based Online Harassment and Abuse.
- Linking national participation in global and regional forums for AI governance with country priorities for countering

NCII and child sexual abuse material.
- As applicable, participating in international forums to promote harmonised approaches to regulating industry, like the Global Online Safety Regulators Network.

Society and Culture/Prevention

Principles for action to shift social and gender norms that reduce the risk of NCII perpetration and victimisation, foster healthy and responsible technology use, and promote a culture in which survivors and victims are believed and supported, and offenders are held appropriately accountable.

Targeted prevention strategies that teach privacy, consent, and healthy relationships translated to the digital context.

→Principle in Practice:

- Prevention efforts include both population-specific education and training, and general audience awareness campaigns.
- Targeted prevention strategies start early in the life course, teaching developmentally- appropriate lessons that build core values around privacy, bodily autonomy, consent, and gender equality and healthy relationships, translated to the online environment.
- Prevention education engages parents, caregivers, and community and faith leaders, using adult learning methods, and adopting a “train the trainer” approach that teaches core concepts while empowering adults to serve as instructors.
- Lessons are culturally-sensitive, available across schools, faith communities, and workplaces.
- Prevention strategies meaningfully involve men and boys through affirming, evidence-based curricula that model positive, respectful interactions with women, girls, and peers of all genders—both online and offline—drawing on proven approaches from what works to counter GBV/VAWG.

National awareness campaigns that convey NCII as illegal and harmful, and signpost services and helplines in a variety of languages and accessible formats.

→Principle in Practice:

- General-audience prevention campaigns that raise awareness about NCII and related forms of intimate image abuse as harmful—and in certain cases illegal—while consistently directing the public to dedicated support resources like helplines.
- Universal messages communicating laws and penalties around NCII, and advertising victim support services, are customisable for culturally-specific settings and available in multiple languages, ensuring accessibility for individuals who are blind, deaf, or hard-of-hearing.
- Awareness campaigns include lessons on responsible bystander engagement and activation, and promote collective responsibility for digital safety, such as discouraging the circulation of NCII, refraining from victim blaming, and understanding the permanence of online content.

Media guidance for responsible reporting and storytelling about NCII. Comprehensive media guidance and sensitisation on NCII should aim to reduce stigma, recognise survivor agency, and signal resources for support.

Integrating lessons on consent, online safety and image-based sexual abuse as core to digital citizenship and individual cybersecurity training–rather than siloed topics. It is further recommended that digital literacy curricula and personal cybersecurity training:

- Incorporate themes of consent, privacy, and online safety, including lessons on image-based sexual abuse, as a core component of overall learning, rather than limited to stand-alone modules.
- Are included as part of teacher credentialing and continued professional education, with information on where to refer people seeking help for NCII and image-based abuse.
- Aim to enhance knowledge of effective cybersecurity practices and privacy-preserving strategies for safe use of social media platforms and AI tools.
- De-normalise the use of AI apps and tools to generate violent, misogynistic content, in addition to instilling lessons on refraining from altering or using another person’s likeness to create content without their consent.

Tech sector pilots innovative safety-and-privacy -by-design approaches to signal violations of community guidelines/ acceptable terms of use and norm-set what actions are illegal or harmful. Industry can complement community-based prevention and national awareness campaigns by:

- Piloting in-product behavioural nudges such as pop-up warnings to signal to users when actions—like uploading violent or sexually explicit images or videos or prompting AI tools to generate sexually explicit content—may be illegal or a violation of platform/community guidelines.
- Supporting prevention messaging and awareness campaigns through ad credits and as featured content.
- Inviting survivors, frontline practitioners and civil society organisations, including youth, to inform product development and promote safer user experiences.

→Principle in Practice:

- Media (including journalists, newsrooms, film, radio, and television producers, podcasters, content creators and social media influencers) is equipped with knowledge and tools to promote legally accurate, trauma-informed and victim-centred reporting and storytelling about image-based sexual abuse.
- Responsible reporting on NCII avoids re-traumatising victims and facilitates survivor agency/ownership over their stories.
- News articles, investigative reports, interviews, and creative storytelling featuring NCII incorporates information about relevant helplines and support services.

Criminal Legal System Response

Principles for building a trauma-informed, well-resourced criminal legal system that effectively investigates and prosecutes offenders and provides victims of NCII with safe, stigma-free pathways to justice.

Clearly defined laws and policies, with sentencing guidelines and considerations for minors alleged, accused, or convicted of a crime.

→Principle in Practice:

- Comprehensive laws and policies that clearly define NCII offenses, including synthetic or manipulated images and videos, such as AI-generated material.
- Sentencing guidelines that take into consideration the harm and risks posed to victims, with criminal sanctions including appropriate orders that meaningfully protect victims from further harm, such as a requirement to destroy existing NCII, and remove NCII from shared spaces.
- Appropriate measures for children who are alleged, accused or convicted of creating or sharing NCII, aligned with international child rights law and the UN Convention against Cybercrime.
- Specifications that victims are not required to engage in the criminal legal system or formally report NCII to legal authorities as a pre-condition for access to support services.
- Policies governing data access and records requests from law enforcement to online platforms, incorporating data-minimisation, use-limitations, and auditability requirements to safeguard survivor data, prevent secondary victimisation and investigative overreach.
- Clear and accessible avenues for victims to file complaints regarding how their case was handled, including human rights complaints related to sexist or discriminatory decision-making by law enforcement.
- NCII perpetrated by an intimate partner should be considered a form of family violence and protection orders in family law should include protections from NCII.

Training and trauma-informed capacity-building for justice sector professionals on NCII.

→Principle in Practice:

- Police, judges, forensic experts and prosecutors are trained on foundational concepts for trauma-informed and evidence-based understanding of cybercrime and GBV/VAWG, including

Trauma-informed court procedures that preserve privacy of victims and the accused. Governments may also consider implementing guidelines for court proceedings and judicial processes in NCII cases such as:

- Closed hearings and ability for remote court appearances for victims to reduce trauma and preserve privacy.
- Anonymity and publication bans on the victim's name or any identifying information—including details that could be used to locate the NCII—should be the default. However, these protections should be easy to lift if the victim chooses to be identified in court documents.
- Timely victim notification of offender charging and sentencing updates.
- Enabling victims to petition for digital protective orders or injunctions, including granting court-ordered, emergency image-removal by platforms, offender abstention from sharing/threatening to share the image further, image destruction, or platform de-indexing orders (recognising limitations for content removal from encrypted services).
- Services for these types of emergency orders should be available in a reasonable timeframe. Ideally, judicial authorities should be on call 24 hours a day, 7 days a week to assess urgent applications for protective orders of this kind.

Trauma-informed law enforcement practices, paired with technologies that safeguard victims' privacy. Law enforcement agencies may also consider adopting the following practices for trauma-informed, survivor-centred case handling, investigations, and management of digital evidence:

- Establishing consistent points-of-contact and timely, periodic updates to victims on case status, risk assessments and protective measures taken, throughout all stages of the criminal legal process, and by request.
- Use of robust image-hashing, alongside methods for image categorisation that describe and code relevant digital evidence without further distributing non-consensual content to preserve victim privacy and dignity.
- Training that further combines digital forensic skills with an understanding of

victim encounter skills that reduce stigma, avoid victim-blaming and prevent the need for victims to repeatedly recount traumatic experiences.
- Justice sector training on cybercrime and GBV/VAWG integrates lessons on NCII, including its co-occurrence with other forms of GBV as a form of digital coercive control, and incorporating NCII into domestic abuse and stalking risk assessments.
- Police training on NCII strengthens digital competency and deepens understanding of the technology-driven risks and harms associated with intimate image abuse, emphasising the need for timely case handling and investigations given the rapid pace of digital dissemination.
- Law enforcement training on NCII clarifies the legal and procedural distinctions between adult NCII and child sexual abuse material (CSAM), while acknowledging practical gaps and complexities, particularly in cases involving adolescents, so that responses are age-appropriate and better aligned with the realities young people face.
- Training for the justice sector is cyclical and updated to account for developments in digital forensics, and changes to laws and policies related to NCII.
- Where specialised helplines and victim services for NCII exist, first responders routinely refer victims to resources upon initial intake.

Law enforcement is equipped with skills, knowledge and resources for effective, timely digital forensics, investigations and responsible evidence-handling.

→Principle in Practice:

- Law enforcement agencies are appropriately resourced with or have access to technical tools, software, and devices needed for effective digital forensics and cyber investigations.
- Local, frontline police and law enforcement officials have established protocols for triage and safeguarding evidence at first contact upon receiving initial reports of NCII, victim-centred evidence preservation to minimise re-traumatisation, and thresholds for escalation to specialist units, regional or national law enforcement agencies.
- Law enforcement agencies are well-versed on the acceptability of different types of digital evidence, enabling officers to understand what evidence is admissible without compromising digital evidence quality or victim safety or wellbeing.
- Law enforcement agencies have established chain-of-custody protocols restricting access to a limited set of authorised personnel, preserving victim privacy and reducing unnecessary exposure of NCII material.
- Law enforcement agencies have clear and consistent guidance and training on appropriate engagement with online platforms, including preservation and removal requests, the use of subpoenas and warrants, and where cross-border legal constraints may limit access.

how digital abuse operates in contexts of GBV/VAWG and coercive control, supporting earlier identification of NCII and recognition of evidence such as escalating communications, phone-use patterns, false profiles, and in-home surveillance.

International law enforcement coordination to strengthen cross-border investigations grounded in survivor-centred, trauma-informed and rights-based principles. Governments actively contribute towards international efforts to better coordinate law enforcement agencies through:

- Assisting partner countries' law-enforcement agencies by sharing technical expertise, delivering training, and providing access to critical databases and digital-forensics capabilities for NCII.
- Cooperating with international law-enforcement agencies to investigate NCII cases involving victims and perpetrators in different jurisdictions.
- Supporting the development of rights-based, trauma-informed, and survivor-centred investigative standards for NCII, grounded in internationally agreed-upon digital-forensics principles such as selective extraction, limiting collection to only what is necessary for the investigation and balancing victim privacy.

Exploring alternative justice practices—including restorative justice models, Indigenous and culturally-grounded approaches—to offer survivors of NCII additional pathways to healing and accountability outside the criminal legal system.

- Promising restorative and alternative justice models used in other GBV/VAWG contexts may offer insights for NCII cases, provided robust safeguards are in place to protect survivors, determine whether the severity of the harm is appropriate for addressing outside formal legal systems, and considering the readiness and ability of the person who has engaged in harm to constructively participate.

- Law enforcement agencies observe and enforce strict misconduct and accountability policies that address officer misuse or mishandling of digital evidence that could itself constitute the non-consensual sharing of intimate images.

Victim Support and Empowerment

Principles for free, accessible, specialised, and sustainably funded services that empower victims of NCII through safety planning, legal and psychosocial support, clear reporting pathways, and provider referrals and cross-training.

Dedicated, specialised helplines and victim services for NCII, freely available.

→Principle in Practice:

- Survivors have access to specialised helplines that provide safety planning, assistance with platform takedown requests, warm referrals to law enforcement and independent, authoritative information about their legal rights.
- Specialised providers are equipped with skills and knowledge to assess immediate safety risks—including self-harm, doxxing, stalking, and threats of violence.
- Helplines offer accessible, plain-language, multilingual support in a variety of formats, such as chat, text, phone, and in-person options, where available.
- Services are widely promoted and advertised as welcoming, inclusive, and accessible to survivors of all backgrounds and identities, including men, and survivors with children.
- Where resources allow, helplines work towards 24/7 operational capability.

Organisations providing services for other forms of GBV/VAWG possess baseline knowledge of tech- facilitated abuse and awareness of specialised helplines/resources for NCII.

→Principle in Practice:

- Domestic violence, sexual assault, stalking and trafficking organisations possess a baseline awareness of tech-enabled abuse and NCII, including basic cybersecurity measures to protect victim privacy and preserve digital evidence.
- These organisations develop and maintain strong referral pathways to specialised helplines and other NCII-specific resources.
- Where available, non-specialised GBV organisations offering holistic, wraparound support for survivors (e.g. psychosocial support and counselling, housing and financial assistance, legal advice and referrals) are accessible to victims of NCII.

Coordination between adult-serving and child-focused image-based sexual abuse organisations to facilitate victim referral, joint advocacy and training.

→Principle in Practice:

- Organisations serving adult and child survivors of image-based sexual abuse have established referral pathways and active working relationships to enable survivors of all ages to receive seamless, developmentally appropriate support– (e.g. 16- and 17-year-olds who may be creating and sharing images within legal age of consent frameworks

National budgets for cybercrime and GBV/VAWG include funding for specialised helplines and victim services for NCII. Governments with dedicated financing for cybercrime, GBV/VAWG are encouraged to also:

- Identify funding for specialised helplines and victim services for NCII, including express support for organisations led by and for racial minority and other marginalised communities offering culturally-competent, trusted and accessible support.
- Enable support for peer-to-peer advocacy, safely connecting survivors who wish to be in community with others with similar lived experiences, facilitated by victim-serving organisations.
- Differentiate funding streams for victim-serving organisations to address both operational needs and training and provide mental-health resources and time off for first responders to reduce burnout and address vicarious trauma.

Partnerships between NCII-focused organisations and industry to escalate takedown requests and scale adoption of robust image-hashing tools, like StopNCII.org.

- Specialised helplines, hotlines, and victim-serving organisations function as trusted flaggers or otherwise have established contacts with online platforms to facilitate faster image-takedown responses and escalate high-risk cases.
- Specialised helplines, hotlines, and victim-serving organisations also have access to robust image-hashing tools, such as StopNCII.org, to help prevent the circulation of victims' images.

Collaboration among NCII-focused organisations, legal aid programs, pro-bono lawyers and prosecution services to enhance survivors' access to justice and quality legal representation.

- By partnering with NCII-focused organisations, legal aid programs, pro-bono lawyers and prosecution services supporting survivors of domestic violence, sexual assault, stalking, and trafficking can deepen their expertise in digital abuse and expand their ability to assist victims of NCII.

Sustained, diversified funding models for specialised services and helplines, including those operating in high-risk, under-resourced and fragile settings. Sustainable victim empowerment and support for NCII requires funding from diverse sources, with consideration for:

- Long-term government investment in national specialised services and helplines, in addition to resourcing capacity-building and training for organisations tackling other forms of

in some jurisdictions, but whose images would constitute CSAM in others).
- Partnerships between adult and child-focused organisations conduct joint training and engage in coordinated advocacy and coalition-building to strengthen policy and legislation, and advance effective industry responses to shared online safety goals.

GBV/VAWG to understand NCII.
- Flexible, non-government funding from philanthropy and the private sector that preserves independent victim advocacy.
- Philanthropic funding, multilateral and bilateral international assistance for NCII and TFGBV organisations serving victims in high-risk, under-resourced, or fragile settings, particularly where civil society is under threat.

Industry

Principles to enable industry to strengthen prevention, detection, and timely removal of known NCII through survivor-centred practices, responsible design across diverse platforms and services, and ongoing, transparent collaboration with civil society and government in a manner that respects international human rights standards.

Industry follows a core set of standards for user safety, removal of verified NCII, and reporting abuse, while operationalising practices based on the use or misuse of their products and services in the creation, dissemination, or monetisation of NCII within the broader tech ecosystem.

→Principle in Practice:

- Industry adopts baseline standards for user safety, timely and transparent responses to takedown requests, and dedicated channels for reporting NCII. Where regulations, laws and policies are in place, industry practices align with legal requirements.
- Industry continuously develops and refines distinct prevention and response capabilities tailored to product and service type (e.g. search engine, social media platform, cloud provider, payment processor, generative AI developer or deployer, adult content platform).

Industry develops, implements and refines technology-enabled tools, paired with platform policies and practices that reduce risk of NCII generation, distribution and monetisation.

→Principle in Practice:

- Industry widely adopts perceptual image-hashing, hash and signal-sharing for NCII.
- Image-hashing tools and user reporting flows balance friction with ease of flagging potentially harmful content to reduce volume of false reports and avoid suppressing non-abusive user activities.
- Social media platforms, app stores and search engines ban and actively enforce policies against advertisements for, as well as de-list or de-index, sites, tools, tutorials and communities/forums with the primary purpose of generating, sharing, and/or monetising NCII.
- Platforms that allow users to upload, share and/or generate image/video content made available publicly (excluding encrypted services) require users to make a good faith assertion that they have obtained the consent of individuals whose likenesses are depicted, and place restrictions/create friction for re-uploading image or video content.

Platforms operationalise consent across policies and product design, appropriately differentiating adult NCII from child safety protocols.

→Principle in Practice:

- Platform policies recognise survivor

Industry adopts a universal, invisible watermarking standard for AI-generated content.

- Through the adoption of a universal, invisible watermark for all AI-generated content, industry supports downstream identification of AI-created NCII by providing metadata—such as when, where, and by whom the content was produced—to strengthen accountability.

AI developers consistently resource and maintain robust red-teaming units to conduct human-led reviews for detecting NCII and other forms of image-based sexual abuse.

- Complementing SOPs for testing and safeguarding models against NCII generation, AI developers prioritise staffing and resourcing for specialised, human-led red-teaming units skilled in identifying NCII and other forms of image-based sexual abuse.
- Red-teaming units are appropriately staffed and thoroughly vetted (including background checks and screening of externally contracted red-teamers) and given access to psychosocial support for human moderators exposed to violent material and at risk for vicarious trauma and burnout.

Industry helps address systemic bias embedded in technology development, design and governance.

- Industry actively pursues strategies to recruit, retain and advance a diverse workforce– particularly women and individuals from marginalised groups– whose typical underrepresentation in leadership and core product, engineering, and design roles can perpetuate gender bias and limit the integration of lived experience into safer, more inclusive technologies.
- Industry models responsible use of technology by embedding guidance on NCII awareness within workplace sexual harassment training and broader HR structures, to support employees affected at work.

Industry engages with Global Majority civil society organisations to shape culturally-relevant, inclusive content moderation policies and AI design.

- Social media platforms regularly engage and fairly compensate civil society groups from Global Majority countries so that their cultural and local expertise informs content-moderation policies that reflect women's diverse, lived realities rather than predominantly Western notions of harm, intimacy and consent.
- AI developers likewise partner with and compensate community-based experts

autonomy by seeking consent for image removal through privacy-preserving approaches like good faith assertions that are based on a statement declaring the depiction is non-consensual.
- Policies refrain from automatic referral of adult victims into law-enforcement pathways—unlike mandated CSAM protocols.
- Adult-content platforms take additional care to provide multiple ways for users to evidence consent and enable clear, accessible mechanisms to withdraw it.

Platform policies minimise the burden on survivors to report and request removal of NCII.

→Principle in Practice:

- Platforms adopt and adhere to transparent, accessible reporting systems based on safety-and-privacy-by-design principles.
- Platform policies prioritise survivors' removal requests over content-owner status.
- Platforms operate timely image removal processes, bolstered by privacy-preserving, perceptual hashing tools like StopNCII.org and special reporting channels.
- Special reporting channels for NCII prompt users to provide information sufficient to identify the harmful content (such as URLs) and enable platforms to contact users in the event additional follow-up is needed to locate the content.
- Platforms signpost resources for victim support services and specialised helplines, and pair backend safety measures with front-end reporting systems that are easy to find, simple to navigate, transparent in outcome, and responsive to the realities of how survivors experience harm—even where technical constraints, such as encrypted services, limit full removal.
- Platforms enact processes to facilitate timely notification to victims on outcomes of content removal requests and confirm takedown of verified NCII.

AI model developers and data providers follow standard operating procedures (SOPs) for model training, testing, and deployment to reduce the risk of NCII creation.

→Principle in Practice:

- AI model developers help prevent the misuse of models to create non-consensual content through feedback loops and iterative stress-testing strategies in their development processes.
- AI model developers employ semantic guardrails that prohibit the creation of NCII via user prompts/inputs as well as outputs.
- AI model developers and data providers responsibly source training data including through ongoing detection and removal of known/verified NCII.
- Multi-modal models that store user-generated images/videos and are retrained on outputs employ robust image-hashing tools to identify verified NCII and apply a "no train" label on

from low and middle-income countries to ensure that AI model training and evaluation incorporate diverse experiences and languages, leading to systems that better represent survivors' lived experiences worldwide.

Industry partners with civil society and academia to support research on NCII, while protecting user privacy and safeguarding sensitive data.

- Industry collaborates with academics, grassroots organisations, and research institutions to enable meaningful researcher access to relevant platform data, in accordance with legal requirements and best practices for protecting individual privacy and safeguarding sensitive data.
- Industry supports independent research through mechanisms such as public data, greater transparency into algorithmic systems, and API access, enabling the study of perpetration patterns, deterrence strategies, and effectiveness of interventions to help address NCII, and other forms of TFGBV and cybercrime.
- Industry can also support research through grants and access to compute to facilitate large-scale, data-intensive projects.

Industry partners with civil society to develop voluntary safety frameworks and best practices that strengthen survivor protection while upholding fundamental rights, including privacy and free expression.

- Industry actively engages with civil society organisations, survivors, government, law enforcement, and multilateral institutions as part of multistakeholder coalitions to establish shared norms and rights-based standards for platform conduct and AI governance that explicitly address NCII, CSAM, and gendered forms of online harm.
- Survivor-centred, civil society oversight bodies help to inform and strengthen platforms' trust and safety policies.
- Industry participates in public-private partnerships that provide meaningful support to civil society through direct funding, in-kind contributions and ad credits, and harness industry expertise and resources to address root causes of NCII as a form of GBV/VAWG.

non-consensual content.
- Where feasible and depending on the purpose of the model, AI developers opt for closed, v. open-source, open-weight models, which can be more easily exploited to build image/video generators fine-tuned specifically to create image-based sexual abuse.
- AI developers ensure safety protocols that limit the misuse of models to generate NCII are consistently robust across both free and subscription APIs.

Research and Data

Principles for building, resourcing, and sustaining an ethical, survivor-centred evidence base to inform programs, policies, laws and regulations and technological innovations to prevent and address NCII through an intersectional lens.

Standardised definitions and metrics to assess and compare national, regional and global prevalence of NCII.

→Principle in Practice: As countries develop and update existing cybercrime and GBV/VAWG surveillance systems, it is recommended that they pursue:

- Common measures for NCII, consistent with national laws and policies, integrated into public health surveys, law enforcement reporting, and crime victimisation surveys.
- Anonymous surveys measuring population-level prevalence of NCII disaggregated by sex, age, race/ethnicity, disability, and other relevant factors to understand disparities across groups.
- National cybercrime reporting systems tracking law enforcement data that are updated to include NCII, with uniform standards and guidance for crime recording and classification provided to local, regional and national law enforcement agencies.

Ethical, methodologically-sound research based on informed consent that protects survivor/subject confidentiality, privacy and data.

→Principle in Practice: Government bodies and other funders require research proposals to demonstrate:

- Adherence to established ethical and methodological standards for informed consent, protecting survivor/subject confidentiality, privacy and data, drawing on tested approaches to survey and study design from the GBV/VAWG field.
- The use of additional protections and considerations regarding the use of technology to gather and publish information and securely store survivor data, including efforts to minimise data collection, limit retention, and abide by a “do no harm” principle.
- Protocols for safeguarding researchers conducting research in fragile or high-risk settings, or with populations that place them at elevated risk for online harassment, threats, and targeting.

Research on the characteristics, costs, and consequences of NCII to capture direct and indirect impacts on individuals, communities and society, through an intersectional approach.

→Principle in Practice:

- Research to explore varied manifestations and experiences of NCII across diverse populations and

Multi-method, interdisciplinary, participatory and representative research on NCII. Government bodies and other funders may consider enhancing national research agendas on NCII and other forms of GBV/VAWG through:

- Support for research that employs a variety of methods and approaches, such as rapid evidence and rapid reviews, including civil-society-led documentation of emerging issues, longer-term studies, and qualitative and quantitative evaluations.
- Elevating practice-based approaches, survivor and culturally-specific knowledge, recognising varied forms of expertise, understanding and evidence.
- Investing in participatory research that actively engages youth through advisory councils, particularly to inform prevention strategies that work to address risks for image-based sexual abuse across the life course.
- Encouraging and enabling research that is open-access and open-source, with safeguards in place to protect survivor and subject privacy and anonymity.

Expanding Global Majority representation in the evidence base for NCII. Donor governments, multilateral institutions, the private sector, philanthropic institutions and academia from high-income countries can improve global understanding, inclusion and representation in NCII research by:

- Funding research led by and for grassroots, civil society organisations working at the intersection of women’s rights and digital rights, and survivor groups in low and middle-income countries.
- Supporting partnerships, fellowships and visiting scholars programs with researchers from low and middle-income countries studying NCII.
- Sponsoring grants to address gaps in research on NCII in low and middle-income countries.

Deeper research into primary prevention, perpetrator ideologies, and how digital technologies shape, influence and accelerate social and gender norms that increase risk for NCII.

- Investigating perpetrator motivations, ideologies and causal pathways across diverse contexts, including sextortion frauds and scams, the weaponisation of NCII to undermine women in public life, and links with violent extremist networks.
- Research through a Science, Technology and Society lens that examines how social, political, and cultural values

communities to capture disparities across race, ethnicity, gender, sexual orientation and identity, religion, disability, age, type of work, and other factors.
- Research into the effects of experiencing NCII on education, employment, and physical and mental health, including risk for offline violence and intersections with other forms of GBV/VAWG, such as intimate partner violence.

Prevention-focused research examining risk and protective factors for NCII victimisation and perpetration and what works to prevent it.

→Principle in Practice:

- Research to identify risk and protective factors for NCII using the social-ecological model, examining how factors at the individual, relationship, community, and societal level influence behaviour and informing the development of interventions.
- Program evaluation to understand effectiveness of interventions across different audiences and settings, including bystander intervention strategies.

Research on effective responses to NCII through policies, laws, and regulations, including assessment of unintended consequences.

→Principle in Practice:

- Research to assess deterrent effects, outcomes, and unintended consequences of NCII-related laws, policies, and regulations.
- Qualitative and quantitative research into survivor-defined measures of justice and wellbeing beyond takedowns or convictions.
- Research to periodically examine accessibility and uptake of criminal and civil remedies to identify potential barriers faced by victims in exercising their rights, such as systematic response failures or bottlenecks when engaging with law enforcement, and institutional actions resulting in secondary harm, re-traumatisation and victim disengagement.

Research that translates evidence into practice.

→Principle in Practice: Governments, civil society, academic institutions, industry and multilateral organisations work together to enable:

- Research translation efforts to break down key findings into accessible, actionable applications for policy and program development to prevent and address NCII.
- Research dissemination strategies to promote widespread access and sharing of knowledge, early learnings and promising practices for NCII prevention and response.

shape the design, use, and impact of technology on individual attitudes, behaviours and beliefs, considering men and boys' exposure to AI tools (e.g. nudify apps) and algorithms accelerating harmful gender norms, stereotypes, and misogyny.