AI AND CHILDREN'S SOCIAL CARE

Where's the Harm?

Protecting children from online sexual abuse and risk in the age of artificial intelligence

Child Safeguarding in the Digital Age

THE LANDSCAPE

AI and Children's Online World

97%

of children aged 3-17 use the internet at home

1 in 3

internet users globally is a child

300%

increase in AI-generated CSAM reports since 2020

£1.6bn

UK investment in AI safety & regulation (2023)

HOW AI CHANGES THE RISK

New Technologies, New Threats

Deepfakes & Synthetic CSAM

AI-generated child sexual abuse material that creates no 'victim' in traditional sense — yet causes real harm through normalisation and demand.

AI-Powered Grooming

Large language models enable sophisticated, personalised grooming scripts at scale — lowering barriers for offenders.

Facial Recognition Misuse

AI tools can identify children from public photos, enabling targeted exploitation and stalking.

Algorithmic Amplification

Recommendation systems can funnel vulnerable children toward harmful content and predatory communities.

Current Protections and Their Limits

Existing UK Frameworks

- Online Safety Act 2023 — platform duties to protect children
- Protection of Children Act 1978 — criminalises CSAM
- Sexual Offences Act 2003 — grooming and exploitation offences
- GDPR / UK GDPR — Age Appropriate Design Code
- Investigatory Powers Act — surveillance powers
- Children Act 1989/2004 — duty to safeguard

Critical Gaps

- AI-generated CSAM not clearly covered under existing law
- Jurisdictional complexity — AI platforms often overseas
- Reactive legislation vs. rapidly evolving AI capabilities
- No mandatory AI impact assessments for children
- Underresourced enforcement — NCMEC, IWF overwhelmed
- Definitional challenges around 'harm' in synthetic content

SOCIAL CARE RESPONSE

What Children's Services Must Do Differently

Identification

- Recognise AI-facilitated abuse indicators
- Update assessment frameworks for digital harm
- Train practitioners in online exploitation patterns
- Use consistent screening tools across agencies

Intervention

- Trauma-informed responses to technology-facilitated abuse
- Specialist VAWG and CSE pathways for AI harms
- Coordinate with police digital forensics units
- Support children in evidence preservation

Prevention

- Educate children on AI risks in PSHE
- Engage parents/carers on monitoring tools
- Work with schools on digital literacy
- Advocate for safer design by platforms

ETHICAL TENSIONS

Navigating Rights, Privacy and Protection

Child protection requires surveillance	VS	Children's right to privacy
AI detection tools reduce abuse	VS	Client-side scanning threatens encryption
Removing harmful content protects children	VS	Over-removal can silence survivors

WHAT GOOD LOOKS LIKE

Principles for a Child-Safe AI Future

01

Child Rights by Design

AI products affecting children must embed UNCRC principles from conception — not as an afterthought.

02

Transparency & Accountability

Algorithmic systems used in safeguarding must be explainable, auditable and contestable.

03

Survivor-Centred Approaches

Detection and intervention tools must centre the needs, dignity and agency of affected children.

04

Workforce Capability

Social workers, police and prosecutors need specialist digital harm training embedded in professional standards.

05

Cross-Sector Intelligence

Platforms, government, NCMEC/IWF, law enforcement and social care must share data with appropriate safeguards.

06

Proportionate Regulation

Risk-based AI regulation that moves at pace with technology — not years behind it.

KEY RECOMMENDATIONS

Actions for Government, Platforms and Practitioners

Government

- Legislate specifically on AI-generated CSAM
- Fund specialist digital CSE units nationally
- Mandate child rights impact assessments for AI systems

Tech Platforms

- Implement proactive detection of AI-generated CSAM
- Report fully to NCMEC and IWF with no carve-outs
- Share hash databases across platforms and borders

Social Care

- Embed digital harm in all CSE assessment frameworks
- Create specialist online exploitation pathways
- Co-locate digital leads within MASH/safeguarding hubs

EU LEGISLATIVE LANDSCAPE

Current Law and What's in the Pipeline

✓ IN FORCE

EU AI Act (2024/1689)

Bans AI systems exploiting age vulnerabilities. Mandates risk assessments, deepfake watermarking and disclosure when children interact with AI.

Digital Services Act (DSA)

July 2025 Commission guidelines require platforms to protect minors from grooming, addictive design, and harmful AI chatbots.

GDPR / Age Design Code

Grants children specific data protection rights. Underpins all EU digital child safety obligations.

ePrivacy Derogation (to Apr 2026)

Allows voluntary CSAM scanning by platforms. Extended as a stopgap — a gap here caused a 60% drop in NCMEC reports previously.

⟳ IN PROGRESS

Child Sexual Abuse Regulation (CSAR)

Proposed mandatory CSAM detection & reporting. Trilogue underway in 2026 — stalled over encryption vs. child safety debate ('Chat Control').

Revised CSA Directive

Parliament adopted June 2025. Would explicitly criminalise AI systems designed for child sexual abuse and live-streaming of CSAM.

AI Act — Nudification Ban

May 2026: EU agreed to ban AI nudification apps outright under simplified AI rules.

EU Centre on Child Sexual Abuse

Proposed new EU agency to coordinate CSAM detection, reporting and cross-border enforcement across member states.

IWF 2025: 260× increase in AI-generated CSAM videos year-on-year — making 2025 the worst year for online child abuse in the IWF's 30-year history

THE HARM IS REAL.

THE RESPONSE MUST BE URGENT.

AI is not a future threat — it is reshaping child sexual exploitation right now.
Children's services, government, and platforms must act together with the urgency this demands.

Key Contacts & Resources

Internet Watch Foundation: iwf.org.uk | NCMEC: missingkids.org | NSPCC: nspcc.org.uk/onlinesafety