Online Safety 4 Schools

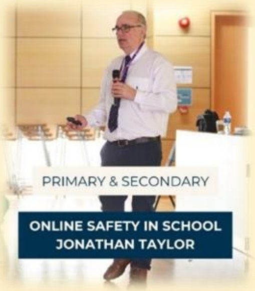
Online Safety 4 Schools

Online Safety for Schools - Staff

Author: Jonathan Taylor MSc – Schools Online Safety Consultant
Purpose: Staff CPD (Continued Professional Development) workshop on safeguarding against online risks

Introduction: Online Risks in a Digital World

- Emerging threats through Artificial Intelligence (AI) and Virtual Reality (VR)
- Shift from traditional 'stranger danger' to complex, tech-enabled risks
- Purpose: equip staff to recognize, respond to, and prevent digital harm



The Online Safety Act 2024 (UK)

- Applies to: Social Media, Search, Pornographic Content Services
- New duties: age enforcement, illegal content removal, harm prevention
- Sanctions: fines up to £18M / 10% of turnover, criminal actions
- Platform responses (Meta, TikTok, Snapchat): varying policies & enforcement

Evolution of Online Engagement

- From pre-Internet to immersive VR
- Common platforms: social media, messaging, gaming
- 80% of public concerned about child sexual abuse risks in VR

Online Threats Breakdown

- Categories: Cyberflashing, Grooming, Gaming exploitation, Sextortion, Self-harm trends
- Tech misuse: AI deepfakes, Fake IDs, VPN apps
- Psychological, sexual, and financial grooming via online channels

Behavioural Frameworks

- Online Safety Spectrum: Acceptable → Illegal
- Victimology & Confidence: Hyper-confident ↔ Hyper-cautious
- Empowering students: choices + critical thinking

Predators & Self-Generated Content

- Online predators bypass rapport by exploiting pre-shared content
- Apps used: WhatsApp, Kik, Messenger, etc.
- Massive rise in self-generated indecent content – 92% of flagged material by IWF in 2023

Dangerous Online Challenges

- Examples: Blue Whale, Momo, Skull Breaker, Benadryl Challenge
- Nature: peer pressure + viral validation
- Categorization: Motivational / Neutral / Dangerous

Cyberflashing & Sextortion

- Non-consensual image sharing through Bluetooth/AirDrop
- Sextortion on the rise, mainly targeting boys aged 14–18
- Criminal exploitation for money via AI-generated or hacked content

AI-Driven Exploitation

- Deepfakes (face swaps, undress AI, virtual image generation)
- 98% of deepfakes = explicit, women are 99% of targets
- Emotional and mental toll: PTSD, anxiety, depression
- Legal: UK law criminalizes non-consensual fake explicit images

Respectful Online Behaviour

- 'It's only banter' → not consequence-free
- Impact: bullying, sexism, objectification, toxic chats
- Consequences: mental health decline, social exclusion, suicide cases (e.g., Mia Janin)

Influencer-Driven Misogyny

- Influencers like Andrew Tate, Sneako, Fresh & Fit normalize misogyny
- School impact: sexist jokes, girls silenced, classroom disruption
- Staff role: promote digital literacy, empathy, respectful masculinity

Digital Identity & Staff Responsibilities

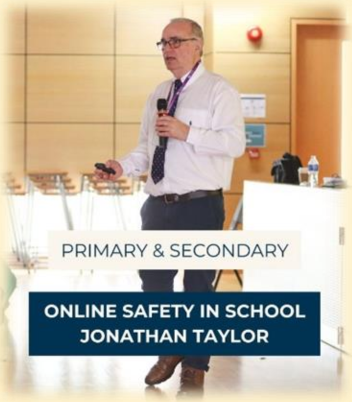
- "Digital Tattoo": every online action leaves a trace
- Staff risks: public content scrutiny, job loss (case law: Faraz v Core Educational Trust 2018)
- Example cases: Vahey (2014), Coleman (2022) show boundary issues & cultural silencing

Key Messages for Parents & Staff

- Online safety isn't just about strangers
- Real risks: peer abuse, closed group bullying, exploitation
- Advice: ask about apps, privacy settings, digital boundaries
- Reporting barriers: fear, shame, confusion, lack of trust

Final Takeaways

- Foster safe, empathetic digital communities
- Understand students' online environments
- Maintain professional digital boundaries
- Push for early intervention and digital competence



🌐 Presented by: Jonathan Taylor MSc
www.onlinesafety4schools.co.uk
✉ onlinesafety4schools@ymail.com