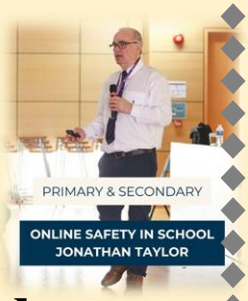
Online Safety for Schools



Online Safety – Key Points & Practical Advice

1. The Online World Has Changed

- Young people face new risks beyond traditional "stranger danger."
- Social internet use includes social media, gaming, messaging and VR.
- 80% of adults believe 13–18 year-olds face significant risk in immersive VR spaces.

2. Key Online Risks

Social Media, Messaging & Gaming

- Cyberflashing and unsolicited explicit content.
- Contact from strangers and grooming.
- Sexting, self-generated content and monetisation.
- Cyberbullying and digital harassment.
- Exposure to misogyny, Incels, extreme views, and porn.
- Data theft, malware, scams and identity fraud.
- Romance fraud and financial extortion.
- Deepfake misuse and AI-generated fake sexual images.
- Reputation damage and cyber-vetting.

3. The Growing Risk of AI

- AI chatbots and companions may:
  - Fail to recognise distress.
  - Reinforce harmful beliefs or suicidal thoughts.
  - Engage in sexualised or abusive conversations.
- Documented cases link chatbot influence to real-world harm and suicide.
- Vulnerable teens are at greatest risk due to developing emotional regulation.

4. VR and Metaverse Risks

- VR combines gaming, messaging and social interaction.
- Risks include:
  - Unwanted contact and harassment.
  - Oversharing personal data.
  - Exposure to harmful content.
  - Spending money unknowingly.

- “Phantom touch” may make harassment feel physically real.
- Offenders use anonymity and avatars to normalise abusive behaviour.

5. Impact on Mental Health

- Social media brings connection but also:
  - Anxiety, low self-esteem and comparison.
  - FOMO and addiction to likes/validation.
  - Pressure to conform, belong and perform online.
- Parental emotional disconnection increases risk.

6. Pornography & Exposure

- Most young people encounter pornography by accident or curiosity.
- Early exposure is linked to reduced self-esteem.
- Age verification tools exist but are easily bypassed.
- Conversations at home remain essential.

7. Cyberflashing

- 80% of girls 12–18 exposed to cyberflashing.
- Airdrop (Apple) / Quick Share (Android) and Bluetooth can be exploited.

Good practice

- Only share with trusted contacts.
- De-personalise phones by changing device name settings.

8. Self-Generated Images (SGI)

- Huge rise in indecent images taken by children themselves (especially girls 11–13).
- Often captured during livestreaming then widely redistributed.
- Material of under-18s is always illegal to create, share or possess.

9. Deepfakes & Undress AI

- 98% of deepfakes are sexual and 99% target women.
- Can:
  - Replace a face onto explicit images.
  - Remove clothing digitally.
  - Generate entirely non-existent “virtual” naked children.
- Still illegal if involving minors, real or artificial.
- Victims can experience trauma, anxiety and loss of self-confidence.

10. Online Scams & Sextortion

- Offenders now aim for rapid financial gain.
- Common approach:
  - Fake profiles/romance approach.
  - Extract images or fake a deepfake.
  - Demand money within minutes.
- Often run by organised criminal gangs overseas.

Advice

- Avoid clicking suspicious messages or files.
- Report threats immediately.
- Parents should review account payments and statements.

11. Online Challenges & "Com Networks"

- Some groups encourage self-harm or sexual acts on camera.
- Harmful groups exist on mainstream platforms used by children.
- Peer pressure and secrecy enable abuse.
- Vigilance and parental awareness are critical.

12. Digital Footprint & Reputation

- What we post may not last forever — but consequences do.
- Screenshots, DMs and group chats can:
  - Be shared.
  - Impact opportunities.
  - Affect future education, careers and sport selection.
- Think before posting, sharing, liking or forwarding.

13. The Parent & Trusted Adult Role

The strongest protection is adult involvement

Conversation + Supervision + Engagement = Safer Online Use

- Children should feel confident to ask permission:
  - "Is it ok if…?"
  - "What should I do if…?"
- Adults should:
  - Be present and involved.
  - Check settings, contacts and device use.
  - Monitor VR and gaming activity.
  - Discuss worries and experiences openly.

14. Key Messages to Give Young People

- If something feels wrong — stop, tell an adult.

- Only communicate with people you genuinely know.
- Don’t rush into decisions online.
- Protect your digital identity and future opportunities.
- Your online world should be safe, respectful and supportive.

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

Online Safety 4 Schools

Online Safety 4 Schools