



Online Safety for Schools (Years 1-2)



What's Covered in 2026 and Beyond



Celebrate Offline Habits

- Salute & congratulate students who don't use devices yet

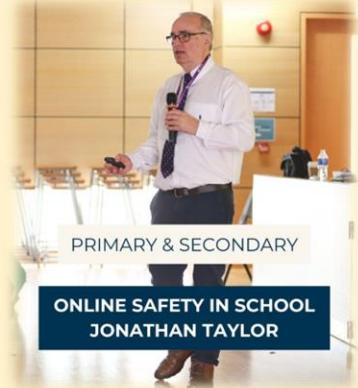


- Smartphones
- Nintendo Switch
- PlayStation
- Xbox



Key Online Safety Messages

- Ask Permission before going online
- Take regular breaks from screens
- Play online with parents – not alone
- Limit screen use to 30 minutes max
- Use the 4 Q's (custom framework for decision-making)



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

The workshop is an age-appropriate and is delivered and designed to create a pupil response type presentation to ascertain internet understanding, device, and social internet usage. This allows schools to be aware of any possible disengagement with education and/or friendship groups.

Online Safety 4 Schools

Online Safety 4 Schools



Online Safety for Schools (Years 3-4)

What's Covered in 2026 and Beyond



Welcome to
Key Stage 2



Celebrate Offline Habits

- Salute & congratulate students who don't use devices yet

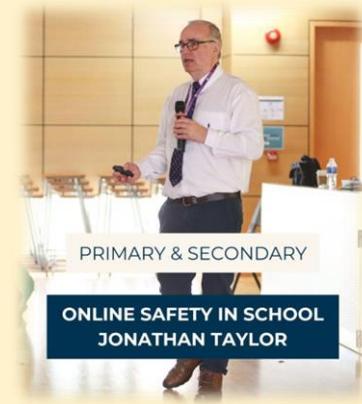
🔍 Know What Devices Students Use

- Know Your Devices: Nintendo Switch, PlayStation, Xbox, etc.
- Understanding Accidental Bullying
- Make the Right Choices – Friends Matter
- Think Before You Share a Selfie
- Try the ICON Test
- Celebrate Students Who Don't Use Devices Yet!
- Workshops include student participation and Q&A



Key Online Safety Messages

- Ask Permission
- Take Breaks
- Get Parents to Play
- Use for 30 Mins Max
- Use the 4 Q's (Think before you click!)



Presented by: Jonathan Taylor MSc
www.onlinesafety4schools.co.uk



onlinesafety4schools@ymail.com

The workshop is an age-appropriate and is delivered and designed to create a pupil response type presentation to ascertain internet understanding, device, and social internet usage. This allows schools to be aware of any possible disengagement with education and/or friendship groups.

Workshop can be delivered with pupils in discussion pods to discuss topics

Online Safety 4 Schools

Online Safety 4 Schools



🛡️ Online Safety for Schools (Years 5-6)

2026

What's Covered in 2026 and Beyond



📱 Key Habits

- Ask Permission / Take Regular Breaks
- Play Online with Parents / Limit Online Time to 30 Minutes
- Use the 4 Q's
- Think before you Like, Post, Share, or Send



🎮 Know the Devices

- Smartphones, Nintendo Switch, PlayStation, Xbox, etc.
- Social Media & Respectful Online Behaviour



⚠️ Digital Dangers

- Accidental Bullying / It's Not Banter / Online Stranger Danger
- Selfies & ICON Test / Passcodes & Online Payments / Being kind Online

🎁 Positive Reinforcement

- Celebrate students who don't use devices yet
- Always Speak to an Adult / Grown Up if anyone hurts you online.
- Why it is important to respect others use of social media and games.
- Don't talk to strangers or accept unknown friend requests.
- Only play online games with true friends you know in real life.
- Set boundaries, take breaks, and include others.
- Use block and report tools when needed.
- Tell a trusted adult if something makes you uncomfortable.
- Real friends won't pressure you to do or share things online.
- Always ask permission — and get parents involved.
- Together for a Better Internet — 'Your Internet, Your Choice'.



🌐 Presented by: Jonathan Taylor MSc

www.onlinesafety4schools.co.uk

✉️ onlinesafety4schools@ymail.com

Online Safety 4 Schools

Online Safety 4 Schools



2026

What's Covered in 2026 and Beyond



🔍 Understand Devices

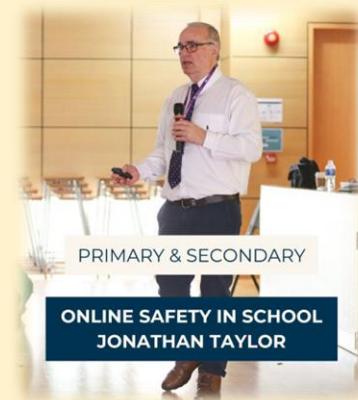
- Smartphones, Oculus, Horizon World, 18+ Games, VR & AI
- Social media is powerful — Think before you Like, Post, Share, or Send.

🌐 Key Concepts

- Digital Permanence, Screen Time, Stranger Danger
- Your Digital Tattoo lasts forever — build a positive one
- Be kind online — 'It's only banter' doesn't mean it's okay — there are consequences.
- Sexism, objectification, and bullying hurt — online and offline.
- Respect protected characteristics — it's the law.
- Technology vulnerabilities (GPS, servers, depersonalisation)
- Together for a Better Internet — 'Your Internet, Your Choice'

⚠ Risks & Realities

- Private chats and DMs can become toxic fast.
- Misogyny, InCel Culture, Online Pornography
- Understand the emotional impact of online actions.
- Challenge harmful stereotypes and promote kindness.



⚠ Tips

- Don't talk to strangers or accept unknown friend requests.
- Only play online games with true friends you know in real life.
- Set boundaries, take breaks, and include others.
- Use block and report tools when needed.
- Tell a trusted adult if something makes you uncomfortable.
- Real friends won't pressure you to do or share things online.
- Always ask permission — and get parents involved.

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



🛡️ Online Safety for Schools (Years 9-10)



What's Covered in 2026 and Beyond

🔍 Understand Devices



- Smartphones, Oculus, Horizon World, 18+ Games, VR & AI
- Your Digital Tattoo and online identity affect your future.
-

SCHOOL YEAR
9 to 11



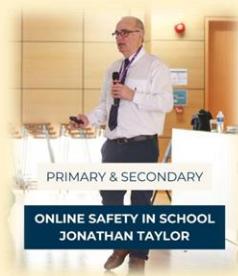
🌐 Key Concepts

- Digital Permanence, Screen Time, Stranger Danger
- GPS & Images, Online Identity, Digital Tattoo
- Managed vs. Unmanaged Devices
- Digital Tattoo: Your Online History Matters
- Digital Permanence & Identity: You Can't Undo Everything
- Build Clean Online Profiles for Future Success
-

Meta

⚠️ Risks & Realities

- Cyber Flashing, Sextortion
- Student-on-Student Bullying
- Understand InCel culture, misogyny, and online radicalization, Online Pornography
- Technology vulnerabilities (GPS, servers)
- Depersonalisation: What Happens With Apple Devices?
- Recognise and report sextortion, scams, and deepfakes.
- Radicalisation, Influencers, and Cancel Culture
- Emerging Tech: VR, AI, Horizon Worlds 18+
- Influencers aren't always positive role models — think critically.
- Healthy masculinity = empathy, vulnerability, and respect.
- Watch for manipulation in group chats and DMs.
- Don't overshare — scammers and predators use personal data.
- Foster a positive online presence for universities and employers.
- Make the Right Choice to Stay Safe — Be Proud of Your Online Brand.



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



11-13
years

🛡️ Online Safety for Schools (Years 11-13)

2026

What's Covered in 2026 and Beyond

🔍 Know the Online World of Students

- Create a positive 'Digital Tattoo' that reflects your values.
- Explore platforms like Oculus, Twitter (X), LinkedIn, Blogging tools
- Be aware of 18+ games and virtual spaces (e.g., Horizon Worlds)



⚠️ Online Dangers Still Exist



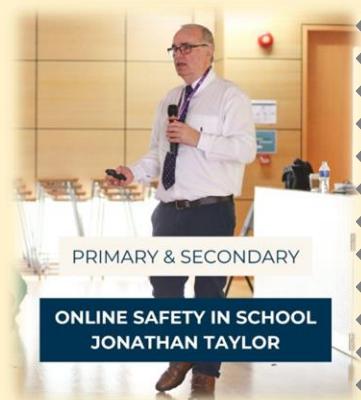
- AI & VR misuse/ Sextortion threats / Online fakeness
- Streaming risks / Face Check ID & Passcode breaches
- InCel culture, Misogyny, Online Pornography

💡 Encourage Positive Use of Technology

- Publish EPQs / Extended Essays online
- Follow universities and companies on LinkedIn & Twitter
- Promote positive blogging
- Stay updated with SGi's & legislation

🤝 Build a Strong Support Network

- Connect with True Friends, Family, Professionals
- Call out sexism, bullying, and harmful content — in real time.
- Surround yourself with respectful, positive role models.
- Healthy masculinity includes vulnerability and empathy.



🔒 Personal Security Matters

- Check online profiles – Physically & Electronically
- Learn about online payments and acknowledgments
- Your future employers, universities & partners are watching.
- Stay safe, be proud — build a legacy you can stand by.

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



Online Safety for Schools - Staff

Author: Jonathan Taylor MSc – Schools Online Safety Consultant

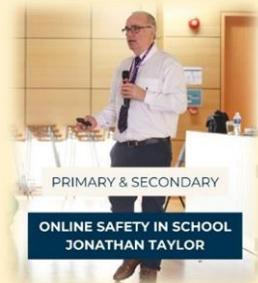
Purpose: Staff CPD (Continued Professional Development) workshop on safeguarding against online risks

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

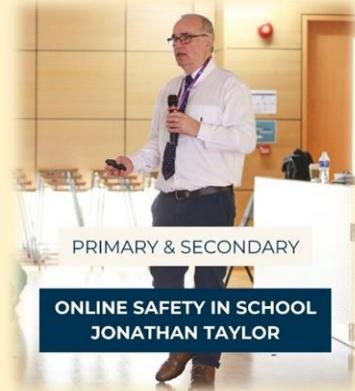
- "Digital Tattoo": every online action leaves a trace
- Staff risks: public content scrutiny, job loss (case law: Faraz v Core Educational Trust 2018)
- Example cases: Vahey (2014), Coleman (2022) show boundary issues & cultural silencing

Key Messages for Parents & Staff

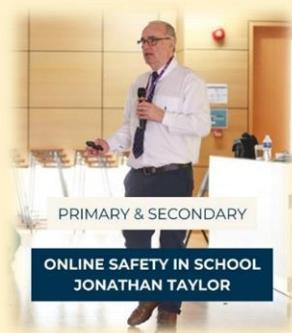
- Online safety isn't just about strangers
- Real risks: peer abuse, closed group bullying, exploitation
- Advice: ask about apps, privacy settings, digital boundaries
- Reporting barriers: fear, shame, confusion, lack of trust

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



Online Safety Awareness Parents & Carers - 2026

Author: Jonathan Taylor MSc - Social Media & Online Safety Consultant

Purpose: To provide parents and carers with essential insights and guidance on digital risks, responsible technology use, and safeguarding strategies.

1. New Risks in the Digital Age

Focus on threats from AI, Virtual Reality, and self-generated content (SGIs). Shift from traditional dangers to modern digital exploitation.

2. Common Online Dangers

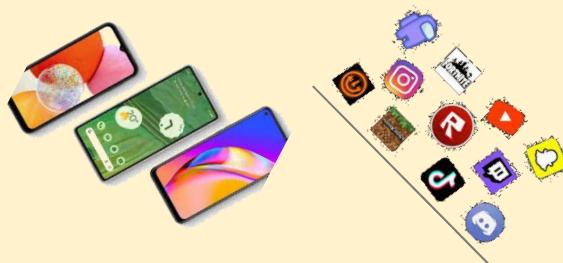
Cyberflashing, grooming, sextortion, incel culture, scams, deepfakes, online gaming risks, and AI misuse.

3. Online Safety Act 2024

Regulates platforms like Meta, TikTok, and Snapchat. Enforces age restrictions, content removal, and accountability. Sanctions include heavy fines and legal action.

4. Online Usage & Devices

Discussion of pre-internet to immersive VR world. Emphasis on social media, messaging, gaming, and devices as access points to risk.



5. Mobile Phones by Age

Age-appropriate phone use:

0–10: no phone unless for care/safety

11–13: brick phones

13–14: limited smartphone access

14–16: supervised full access

6. Safety Spectrum & Online Competence

Behaviour types from Acceptable to Illegal. Online competence means using tech responsibly and with understanding—not just access.

7. Role of Parental Involvement

Online resilience is built through trusted adult involvement, modelling, support, and honest conversations.

8. Grooming & App Awareness

Predators exploit platforms with chat/video features. Parents should know app features: messaging, live streaming, GPS, and age limits.



9. Self-Generated Content & Sexting

Sharp rise in underage content shared via webcam or livestream. Mostly involves girls aged 11–13. Digital Footprint is permanent.



10. Online Challenges & Peer Pressure

Examples: Blue Whale, Momo, Skull Breaker. These prey on vulnerable children seeking social validation online.

11. Respectful Behaviour & Digital Permanence

Digital actions leave permanent marks. Unkind group chats, bullying, and inappropriate content sharing can have lasting effects. **Joint Enterprise and being Guilty by Association**

12. Misogyny, InCel Culture & Influencers

Online misogyny driven by figures like Andrew Tate. Harmful ideologies are spreading in youth spaces, influencing identity and respect.

13. Technology as a Double-Edged Sword

Algorithms can promote harmful content. Students must be taught media literacy and how to evaluate what they see online.

14. Sextortion, Deepfakes & AI Abuse

Blackmail using explicit real/fake images. Offenders use apps and bots to exploit kids quickly. Most victims are boys aged 14–18.



15. Trusted Adults & Safety Advice

Teach kids to recognize abuse, ask for help, understand pressure, and use reporting tools. Support them without fear or shame.

16. Positive Digital Identity

Encourage children to build a healthy online presence. Every post, like, and comment contributes to their digital 'tattoo'.

17. Parental Takeaways

Stay involved, ask questions, supervise screen time, model safe behaviour, and foster open dialogue.