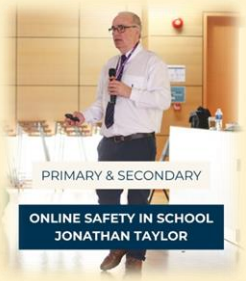
Online Safety for Schools



Online Safety: Preventing Online Risks & Dangers for Children & Young Adults

This document provides **10 practical prevention tips** for each major online risk area. It is designed for use by **schools, parents, carers, safeguarding leads, and youth professionals**.

1. Cyberflashing & Exposure to Unsolicited Content

1. Enable device-level content and message filtering by default.
2. Teach young people how to block and report users immediately.
3. Disable AirDrop / Quick Share Bluetooth sharing except when needed.
4. Encourage private social media accounts with limited messaging.
5. Explain that unsolicited content is never the child's fault.
6. Use age-appropriate platform settings and parental controls.
7. Discuss safe use of group chats and public forums.
8. Promote trusted adult reporting routes at home and school.
9. Regularly review app permissions and message settings.
10. Reinforce that images received should not be forwarded.

2. Online Stranger Danger & Grooming

1. Reinforce that not everyone online is who they claim to be.
2. Discourage private messaging with unknown contacts.
3. Teach children to avoid sharing personal information.
4. Encourage keeping conversations within moderated platforms.
5. Explain grooming warning signs clearly and calmly.
6. Promote the use of nicknames instead of real names.
7. Review friend and follower lists together.
8. Encourage reporting of uncomfortable conversations early.
9. Ensure devices are used in shared family spaces when possible.
10. Reinforce that secrets online are a red flag.

3. Exploitation in Online Gaming

1. Disable voice and private chat where not essential.
2. Use age-appropriate games and PEGI ratings.
3. Teach children never to share login details.
4. Warn against in-game gifts or rewards from strangers.
5. Encourage playing with known friends only.
6. Monitor friend requests within games.
7. Discuss manipulation tactics used by exploiters.
8. Enable spending limits on accounts.

9. Promote regular breaks from gaming environments.
10. Reinforce reporting and muting features.

4. Self-Generated Images (Sexting & Monetisation)

1. Teach that once shared, images can never be fully controlled.
2. Reinforce that no one has the right to request images.
3. Explain the legal and emotional consequences clearly.
4. Promote body respect and self-worth discussions.
5. Encourage immediate reporting if pressured.
6. Teach how images can be manipulated or reused.
7. Discourage storing intimate images on devices.
8. Reinforce consent and coercion education.
9. Provide reassurance that support is available.
10. Promote safer digital decision-making skills.

5. Cyberbullying & Digital Harassment

1. Encourage blocking and reporting rather than engaging.
2. Teach how screenshots can preserve evidence safely.
3. Reinforce kindness and respectful online behaviour.
4. Monitor changes in mood or behaviour.
5. Promote positive peer support strategies.
6. Ensure children know where to seek help.
7. Reinforce platform reporting tools.
8. Encourage time away from harmful spaces.
9. Address bystander responsibilities.
10. Reinforce that bullying is never acceptable.

6. Online Misogyny, Incel Culture & Pornography

1. Teach critical thinking around online narratives.
2. Discuss healthy relationships and respect.
3. Explain how algorithms can reinforce harmful content.
4. Encourage open conversations without shame.
5. Use filters to limit explicit material.
6. Challenge stereotypes and harmful ideologies.
7. Promote positive male and female role models.
8. Teach consent and equality education.
9. Encourage questioning extreme viewpoints.
10. Reinforce that online content is often unrealistic.

7. Personal Data Theft, Scams & Viruses

1. Teach strong, unique password habits.
2. Enable two-factor authentication.
3. Warn against clicking unknown links.

4. Teach how to spot phishing messages.
5. Keep devices and software updated.
6. Avoid public Wi-Fi for sensitive activity.
7. Limit oversharing on social media.
8. Encourage antivirus protection.
9. Reinforce logging out of shared devices.
10. Promote checking privacy settings regularly.

8. Sexual, Psychological & Financial Grooming

1. Teach manipulation and flattery warning signs.
2. Reinforce that pressure is a red flag.
3. Discourage sharing financial information.
4. Promote transparency with trusted adults.
5. Encourage questioning requests for help or money.
6. Teach how trust can be slowly exploited.
7. Monitor sudden behavioural changes.
8. Reinforce reporting without fear of blame.
9. Encourage critical evaluation of relationships.
10. Reinforce personal boundaries education.

9. Scamming, Fake IDs, Romance Fraud & Extortion

1. Teach scepticism of online relationships.
2. Discourage sharing images or money.
3. Explain common scam techniques.
4. Encourage verification through trusted adults.
5. Warn against urgency-based pressure tactics.
6. Teach how fake profiles are created.
7. Encourage reporting suspicious behaviour.
8. Reinforce that threats should not be complied with.
9. Promote privacy-first social media use.
10. Reinforce seeking help immediately.

10. Sextortion & Deepfake Threats

1. Teach that threats rely on fear and silence.
2. Encourage immediate reporting.
3. Discourage paying or complying with demands.
4. Explain deepfake technology in simple terms.
5. Limit image sharing online.
6. Secure social media accounts.
7. Promote evidence preservation safely.
8. Reinforce legal protections available.
9. Encourage trusted adult involvement.
10. Reinforce that victims are not at fault.

11. VPN App Misuse

1. Explain what VPNs do and why misuse is risky.
2. Restrict VPN installation on devices.
3. Monitor app downloads.
4. Teach how VPNs bypass safety filters.
5. Reinforce school and home rules.
6. Encourage transparency about app use.
7. Use device-level restrictions.
8. Reinforce age-appropriate access.
9. Discuss consequences of misuse.
10. Promote responsible digital choices.

12. Virtual Reality & Metaverse Safety Issues

1. Use age-appropriate VR platforms only. (eg VR Chat)
2. Set clear time limits.
3. Disable public interactions where possible.
4. Teach personal space boundaries.
5. Encourage supervised use.
6. Reinforce avatar privacy.
7. Discuss immersive manipulation risks.
8. Teach reporting tools in VR spaces.
9. Monitor emotional impact of VR.
10. Reinforce real-world grounding.

13. AI Misuse (Face Swaps, Deepfakes, Undress Apps)

1. Teach what AI-generated content is.
2. Explain consent and misuse risks.
3. Discourage uploading personal images.
4. Teach how images can be altered and created.
5. Reinforce legal and ethical consequences.
6. Encourage privacy-first behaviour.
7. Promote critical evaluation of media.
8. Encourage reporting AI abuse.
9. Limit app permissions.
10. Reinforce digital responsibility.

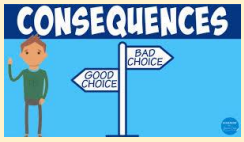
14. Digital Footprint, Reputation & Cyber Vetting

1. Teach that online posts are permanent.
2. Encourage thinking before posting.
3. Review privacy settings regularly.
4. Explain employer and school vetting.
5. Encourage positive digital identities.
6. Discourage impulsive sharing.

7. Teach how content can resurface.
8. Promote respectful online presence.
9. Encourage regular profile clean-ups.
10. Reinforce long-term impact awareness.

15. Understanding Consequences of Online Behaviour

1. Teach legal consequences clearly.
2. Explain emotional harm caused to others.
3. Reinforce accountability online.
4. Encourage empathy and reflection.
5. Discuss real-life safeguarding cases.
6. Reinforce school behaviour policies.
7. Encourage positive role modelling.
8. Promote digital citizenship education.
9. Encourage pause-and-think habits.
10. Reinforce responsible online choices.



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

Online Safety 4 Schools

Online Safety 4 Schools