

Student-Friendly E-Safety Leaflet- Updated 2025

Cybersecurity

- Use strong passwords (12+ characters, mix of letters, numbers, symbols).
- Turn on two-factor authentication wherever possible.
- Watch out for phishing emails – don't click suspicious links.
- Keep your software and apps up to date.

Digital Footprint

- Everything you post, like, or share leaves a trail.
- Think before you post – would you be happy for a teacher, family member or future employer to see it?
- Check your privacy settings on social media and apps- ask an adult at home to help with this or there are many youtube tutorial videos.

Algorithms

- Actively use features like "Not Interested" or "Don't Recommend" to shape what algorithms show you.
- Work with a trusted adult to set up privacy and safety settings, such as time limits and content filters, so you understand their purpose.
- Use the report and block buttons on platforms to remove harmful or unwanted content, and encourage platforms to act on these reports.

Misinformation/Disinformation

- Not everything online is true – check the source.
- Be aware of deepfakes and edited content using AI.
- Use fact-checking websites like Full Fact or Snopes.
- Don't re-share anything that has the intention to cause harm

Online Behaviour

- Be respectful – cyberbullying is never okay.
- Don't share personal info (full name, address, school, phone number) publicly.

- Report anything that makes you feel uncomfortable to a trusted adult or teacher.

Scams

- If it sounds too good to be true, it probably is.
- Don't enter card details on websites you don't trust or that are not verified.
- Watch out for in-app purchases and loot boxes – they can cost real money.

Social Media Safety

- Set profiles to private.
- Avoid accepting unknown friend requests.
- Be mindful of what you share and turn off your location sharing with anyone but family.
- Turn off the setting which enables you to be added to groups automatically

Sharing of indecent images

- It is illegal (under the age of 18) to make, possess, share or distribute any images which contain partial or full nudity
- Do not convert any inappropriate images into stickers, this still counts as possession of an inappropriate image
- Report any sharing of indecent images to the police
- Be aware that AI can be used to edit images online

Gaming Chatrooms

- Never use your full name. Choose a username that doesn't include any personally identifying information, and avoid suggestive or revealing nicknames.
- Never post photos of yourself or your location in a chat room.
- Be careful about downloading mods or cheats from unofficial sources, as they can contain malware.
- Understand that you could be talking to people of any age, including adults who might not have good intentions. Never agree to meet up with someone you've only met online.
- Use the block and report functions for anyone who says or does something creepy, inappropriate, or makes you feel uncomfortable. Sign out.