Online Policy

Date of Policy: Autumn 2026

Review Date: Autumn 2028

This **Online Safety Policy** has been written by the Headteacher, based on Buckinghamshire Council guidance, the Department for Education's *Keeping Children Safe in Education* guidance, the UK Council for Internet Safety (UKCIS) framework and current national legislation and guidance.

The Online Safety Policy forms part of the school's wider safeguarding arrangements and should be read alongside the Safeguarding and Child Protection Policy, Behaviour Policy, Anti-Bullying Policy, PSHE Policy, Relationships and Sex Education (RSE) Policy, Data Protection Policy and Staff Code of Conduct.

The Governing Body has overall responsibility for ensuring that appropriate online safety arrangements are in place. The Designated Safeguarding Lead (DSL) has strategic oversight of online safety as a safeguarding matter and works alongside the Computing Lead and the school's IT support provider to monitor and review practice.

This policy and its implementation will be reviewed annually or sooner if changes in legislation, technology or safeguarding guidance require it.

How can Internet use enhance learning?

Add the following bullet points:

- Pupils will be taught how to stay safe online through a progressive online safety curriculum.
- Pupils will learn about cyberbullying, online relationships, misinformation and disinformation, online scams, gaming safety and digital footprints.
- Pupils will be taught how emerging technologies, including Artificial Intelligence (AI), can be used safely and responsibly.

How will information systems security be maintained?

Replace the section with:

- Security of the school's systems will be reviewed regularly, including cyber-security measures.
- Anti-virus and security software will be updated regularly.
- Security arrangements will be reviewed with the school's IT support provider (Turn IT On).
- Staff will receive regular cyber-security awareness training, including phishing awareness, password security and data protection.
- Personal data will be processed and stored in accordance with UK GDPR and the Data Protection Act 2018.
- Portable storage devices must only be used where authorised and must undergo appropriate security

checks.

- Unapproved software or applications must not be installed on school devices.
- Files stored on the network will be monitored and protected through appropriate security controls.
- System capacity, resilience and cyber-security arrangements will be reviewed regularly.
- Multi-factor authentication and secure password practices will be used where available and appropriate.

How will social networking and personal publishing be managed?

Replace:

Examples now: TikTok, WhatsApp, Instagram, Snapchat, YouTube, forums, Discord, online gaming platforms, group chats, and livestreaming services.

with:

Examples include, but are not limited to, social media platforms, messaging applications, discussion forums, online gaming platforms, livestreaming services and emerging technologies.

Add:

- Pupils will be taught how to identify online risks, manage privacy settings and report concerns.
- The school will educate pupils about the impact of their digital footprint and online reputation.
- Staff must not use personal social media accounts to communicate with pupils or former pupils.

How will filtering be managed?

Replace the section with:

- All internet access is filtered and monitored.
- The school has appropriate filtering and monitoring systems in place that meet current Department for Education expectations.
- Filtering and monitoring systems are reviewed regularly to ensure they remain effective and age appropriate.
- Staff understand how to report online safety concerns identified through filtering and monitoring systems.
- The Governing Body receives assurance that filtering and monitoring arrangements remain suitable and effective.
- Illegal, extremist or inappropriate content identified through filtering or monitoring systems will be dealt with in line with safeguarding procedures.

- Pupils and staff must report any unsuitable content immediately.

How can emerging technologies be managed?

Replace the section with:

- Emerging technologies will be risk assessed before introduction into the school environment.
- Mobile phones and personal devices will only be used in accordance with the school's Mobile Device Policy.
- The misuse of mobile devices, including recording, messaging, photography or online harassment, is prohibited.
- The school recognises the increasing use of Artificial Intelligence (AI) and generative AI technologies.
- Staff and pupils will be taught to use AI tools safely, responsibly and ethically.
- Personal, confidential or sensitive information must never be entered into public AI platforms.
- Any content produced using AI should be reviewed for accuracy, suitability and bias before use.

How should personal data be protected?

Replace with:

Personal data will be processed in accordance with UK GDPR and the Data Protection Act 2018.

Staff must only use approved school systems and platforms for storing, processing and sharing personal information. Personal data must be handled securely at all times and in accordance with the school's Data Protection, Information Security and Records Management procedures.

Any data breach or suspected breach must be reported immediately in line with school procedures.

How will the policy be introduced to pupils?

Add:

- Online safety education will be delivered through Computing, PSHE and safeguarding activities across the curriculum.
- Pupils will be taught about cyberbullying, misinformation, online scams, inappropriate content, online relationships and emerging technologies, including AI.
- Pupils will be encouraged to report anything online that makes them feel worried, uncomfortable or unsafe.

How will the policy be discussed with staff?

Replace the first paragraph with:

The Online Safety Policy will be shared with all staff and governors and will be available through the school's policy system. Online safety forms part of the school's safeguarding responsibilities and all staff are expected to follow this policy at all times.

Add:

- Online safety and cyber-security training will be provided regularly as part of safeguarding updates and professional development.
- Staff will receive guidance on the safe use of technology, data protection and the use of AI technologies within education.

(Appendix 1)

Online Contacts and References

- **National Online Safety** – correct
- **CEOP** – https://www.ceop.police.uk
- **ThinkUKnow** – https://www.thinkuknow.co.uk
- **Internet Watch Foundation** – https://www.iwf.org.uk
- **NSPCC Online Safety** – https://www.nspcc.org.uk/keeping-children-safe/onlinOnline/
- **Childline** – https://www.childline.org.uk
- **Virtual Global Taskforce** – https://www.virtualglobaltaskforce.org

(Appendix 2)

Computer Resources Policy

Pupil Guidelines

The school has provided computers for use by you. They offer access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all. You are encouraged to use and enjoy these resources, and ensure they remain available to all. You are responsible for good behaviour on the Internet as you are in a classroom or a school corridor. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

Equipment

- Do not install, attempt to install or store programs of any type on the computers without permission.
- Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- Do not open files brought in on removable media (such as, CDs, flash drives, memory sticks etc.) until they have been checked with antivirus software by the ICT lead.
- Do not eat or drink near computer equipment.

Security and Privacy

- Do not disclose your password to others, or use passwords intended for the use of others.
- Never tell anyone you meet on the Internet your home address, your telephone number, your school's name, or send them your picture, unless you are given permission to do so by a teacher.
- Do not use the computers in a way that harasses harms, offends or insults others.
- Do not attempt to bypass, security in place on the computers, or attempt to alter the settings.
- Computer storage areas and memory sticks will be treated like school lockers. Teachers may review files and communications to ensure that users are using the system responsibly.

Internet/World Wide Web

- Do not access the Internet unless for study or for school authorised / supervised activities.
- Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, racist, obscene or abusive.
- Respect the work and ownership rights of people outside the school, as well as other pupils or staff. This includes abiding by copyright laws.
- Do not engage in 'chat' activities over the Internet. This takes up valuable resources which could be used by others to benefit their studies.
- Never arrange to meet anyone unless your parent/guardian or teacher goes with you. People you contact online are not always who they seem.
- Political indoctrination of staff or pupils by self-radicalisation or extremist views is not accepted.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is not allowed,
- Never open attachments to emails unless they come from someone you already know and trust. They could contain viruses or other programs which would destroy all the information and software on your computer.
- The sending or receiving of email containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content. Always report such messages to a member of staff.