E-Safety Policy

Date: September 2024
Reviewed: September 2025
Review Date: September 2026
Responsible person: Jess Temple

Rationale

We believe that every child and adult is equally respected and accepted, and that all aspects of school life are safe and fair for children, staff, parents, carers, and the wider community. We aim to give all children the skills they need, now and for the future, to embrace and adapt to an ever-changing digital world.

E-Safety is that area of Safeguarding that deals with the acceptable behaviour needed to achieve a safe and harmonious online community. It teaches users of the internet, social media, connected devices, and emerging technologies such as artificial intelligence what to do should they encounter difficulties or distressing experiences.

Aims

This policy aims to:

- Establish, through consultation with pupils, the ground rules we set for using the internet, social media, and emerging digital technologies including artificial intelligence
- Educate pupils about the benefits and risks of using digital technology and provide safeguarding protocols and awareness for all users
- Demonstrate the methods used to protect children from sites containing pornography, racist or politically extreme views, and violence
- Ensure understanding that accessing inappropriate sites accidentally or being subject to distressing content is not something to feel guilty about, and that any such incident should be reported to staff or parents immediately
- Establish clear protocols for the safe and appropriate use of emerging technologies, including artificial intelligence tools, by staff and students

This policy works in conjunction with our AI Policy 2025, which provides specific guidance on the use of artificial intelligence tools by staff.

E-Safety Principles

E-Safety is the duty of staff, parents, and the children. We educate our children to practise that all users of the internet should be respectful, and that the same standards of safety, equality, and acceptable behaviour that apply in our communities are also applied online and in digital interactions.

As a community we aim to recognise and guard against bullying, intimidation, discrimination, grooming, and exploitation of vulnerable users. E-Safety is an important part of keeping children safe at school and home. Filtering and monitoring is enabled on the school Wi-Fi network, and all staff have up-to-date E-Safety training that includes awareness of emerging technologies and artificial intelligence.

In school, children are taught how to stay safe and behave appropriately online. Parents and carers are reminded, guided, and strongly encouraged to educate children on what to do if and when they encounter danger and how best to deal with it.

All staff demonstrate and take the appropriate care, awareness, and practice as per school GDPR Policy when undertaking work-based practice that involves the use of digital technologies, including internet-based tools and artificial intelligence systems.

Device and System Security

All staff mobile phones and computers as per the School Asset Register are:

- Password protected with secure passwords
- Equipped with appropriate internet security software and protocols
- Registered on the school asset management system with IMEI numbers logged

Access to key systems requires enhanced security:

- Email and WhatsApp require two-step authentication for access
- CPOMs requires two-step authentication for full access and password protection for basic access
- EFL requires password protection to gain access

Staff must:

- Keep their passwords secure and not share them with any other person
- Ensure all laptops (staff and students) are password protected
- Not share student laptop passwords with students

All staff mobile phones must have password protection and other security features enabled as part of asset register security policy.

Practices and Rules

In order to keep children safe online, the following are in place:

- All staff are aware that any recommended websites given to children should be thoroughly checked by the teacher first
- It is the responsibility of every member of staff within the school to report any E-Safety issues they have witnessed or had knowledge of
- Any E-Safety issues should be reported immediately to the Headteacher
- Children's names, personal information, or identifiable data must not be entered into any internet-based software or artificial intelligence systems
- All internet use on the school premises is supervised, including children's access to devices during breaks or lunchtime
- All children will take part in E-Safety focused lessons that include awareness of emerging technologies
- If staff or students find an unsuitable site accessed in school, the screen must be switched off immediately, the device must be closed, and the matter must be reported to the Headteacher and E-Safety coordinator
- Staff and students are aware that all school-based email can be monitored
- Children are aware that all internet usage is monitored and regulated
- All staff, parents, and students must have signed an acceptable use agreement prior to using internet-based software or school digital resources
- Children are taught to recognise that they are responsible for their own digital footprint and understand that all searches and content viewed online is traceable
- School systems cannot block everything - children and parents cannot rely only upon filtering and school security systems to keep children safe online

Staff use of artificial intelligence tools must comply with our AI Policy 2025, which prohibits the entry of any student personal data into AI systems.

Staff Professional Conduct and Social Media

Staff are required to ensure that all social media profiles are sufficiently secure and set to private to protect their own privacy and professional integrity. No social media account should be held under the member of staff's official name.

With this in mind, staff are not permitted to accept any request by a child to connect on social media. In the event that this should happen, staff must report this immediately to the Headteacher. Any form of online connection with children who attend the school is strictly prohibited and may lead to disciplinary action.

Furthermore, school does not encourage online connections with parents, although there may be exceptions whereby staff have friends or family who are parents. In this case, staff must uphold their professional responsibility to ensure that school information and data are not compromised.

Staff must maintain professional boundaries when using any digital platform, including artificial intelligence tools, ensuring no personal or identifiable student information is shared. Refer to our AI Policy 2025 for specific guidance on AI tool usage.

The School Website

The school website maintains high standards of data protection:

- Contact details on the website should be the school address, email, and telephone number only
- Staff or pupils' personal information will not be published
- The Headteacher is responsible for the content and editorial choices
- Pupils' full names are not used anywhere on the website
- Written permission from parents or carers must be obtained before photographs of pupils are published on the school website

Photos and Images of Children

The school maintains strict protocols for photographing and storing images of children:

- When joining school, parents are asked to give consent for images of their child to be published digitally or around the school environment
- A list of children who do not have this consent is available from the Headteacher
- All photos for use on the EFL recording system are taken using staff mobile phones registered on the school asset register
- Images should be uploaded to EFL, then deleted from the device and removed from the recycle bin in close succession
- If images are taken whilst offsite preventing direct upload, this must be done at earliest convenience when connecting to the internet, then deleted and removed from the device's recycle bin
- No images of children should be shared via any platform including WhatsApp
- The person taking the image must upload onto EFL and follow deletion procedures as above
- Automatic linking of mobile devices to other owned devices must be turned off to prevent school-based images from being stored online in phone cloud-based backup systems
- Children may not upload images of themselves or other children

Staff must never upload images of children to artificial intelligence systems or any internet-based image processing tools. This aligns with our AI Policy prohibition on entering any student personal data or identifiable information into AI systems.

Email within School

The use of email within school is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email

can offer significant benefits including direct written contact between schools on different projects, whether staff-based or pupil-based, within school or externally.

We recognise that pupils need to understand how to style an email in relation to their age. As part of our school curriculum, students learn to use technology safely and respectfully, keeping personal information private, and identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Staff must only use their school email to communicate on a professional basis and never respond to any email that may have originated from a pupil's private address or any unfamiliar source.

Social Networking and Digital Footprint

The school maintains clear guidelines on social networking:

- All access to social networking sites is blocked within school for pupils
- Pupils and parents are advised that the use of social network spaces outside school is inappropriate for primary-aged pupils
- Pupils are educated on safe use of social networking and the implications of their digital footprint to prepare them for future use

This education includes awareness of emerging technologies and the importance of protecting personal information when interacting with digital systems, including artificial intelligence.

Emerging Technology and Artificial Intelligence

Emerging technologies will be examined for educational benefit and risk assessed before use in school is permitted. This includes artificial intelligence tools, virtual reality systems, and other innovative technologies that may enhance learning.

Artificial Intelligence

Artificial intelligence tools represent both significant opportunities and risks in educational settings. Our approach to AI is governed by our dedicated AI Policy 2025, which provides comprehensive guidance on acceptable use by staff.

Key principles for AI use:

- No student names, personal information, or identifiable data may ever be entered into any AI system
- AI tools may only be used by trained staff for appropriate purposes such as lesson planning templates and generic resource creation
- All AI-generated content must be thoroughly reviewed for accuracy, appropriateness, and suitability before use with students
- Safeguarding matters must never involve AI systems
- Any breach of AI usage protocols must be reported to the Compliance Manager and Headteacher within two hours

Students are not permitted to use AI tools independently within school. Any educational use of AI with students must be supervised and form part of a planned lesson on digital literacy or emerging technology awareness.

For comprehensive guidance on staff use of artificial intelligence tools, refer to our AI Policy 2025.

The UK General Data Protection Regulation

The UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 govern how we handle personal information. These regulations are designed to harmonise data privacy laws, protect and empower individual data privacy, and reshape how organisations approach data privacy.

The UK GDPR requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. This includes:

- Processing personal data lawfully, fairly, and transparently
- Collecting data only for specified, explicit, and legitimate purposes
- Ensuring data is adequate, relevant, and limited to what is necessary
- Keeping accurate data and updating it when necessary
- Retaining data only for as long as necessary
- Processing data securely and protecting against unauthorised access

Our policies on E-Safety and AI use are designed to ensure full compliance with UK GDPR requirements, particularly regarding the protection of student personal data. For more information on UK GDPR, visit the Information Commissioner's Office website at https://ico.org.uk/for-organisations/

Monitoring, Review, and Compliance

The Senior Leadership Team monitors E-Safety practices across the school, including emerging technology use and compliance with data protection requirements. This monitoring encompasses traditional internet safety, social media usage, and the appropriate use of artificial intelligence tools.

This policy will be reviewed annually or sooner if significant changes in technology, legislation, or school practice occur. The E-Safety Policy will be reviewed in parallel with the AI Policy 2025 to ensure continued alignment and consistency.

Staff will be notified of any updates and required to confirm their understanding of changes. All staff receive annual E-Safety training that includes awareness of emerging technologies and data protection requirements.

Related Policies:

- AI Policy 2025
- Data Protection and GDPR Policy
- Safeguarding Policy
- Acceptable Use Policy
- Being Safe Online Policy