E-Safety Policy

Date: September 2024
Review Date: August 2026
Responsible Person: Jonathan Mundin

Content

1. Rationale

We believe that every child and adult is equally respected and accepted, and that all aspects of school life are “fair” and “safe” 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 everchanging 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 and connected devices what to do should they encounter difficulties or distressing experiences.

2. Aims

- Through consultation with pupils; establish the ground rules we set for using the Internet and electronic communications. It highlights the need to educate pupils about the benefits and risks of using digital technology and provides safeguarding protocol and awareness for all users to enable them to use the internet safely and respectfully.
- Demonstrate the methods used to protect children from sites containing pornography, racist or politically extreme views and violence.
- To understand 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/parents immediately.

3. E-Safety

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, is also applied online.

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. Parental filters will be enabled on all Wi-Fi, and all staff have up-to-date E-Safety training.

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 E-Safety.

All staff mobile phones and computers as per the School Asset Register are password protected and have the appropriate internet security software and protocols installed.

Access to Email and WhatsApp require 2 step protocol systems for access required. CPOMs requires the 2-step protocol for full access to the system. CPOMs requires password protection for basic required access. EFL requires password to gain access.

4. Practices and Rules (see also our 'Being safe online' Policy)

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 should not be entered into any internet-based software.
- All internet use on the school premises is supervised, this includes children's access to devices during breaks or lunchtime.
- All children will take part in E-safety focused lessons.
- If staff/students were to find an unsuitable site accessed in school, then 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.
- Children are taught to recognise that they are responsible for their own 'digital footprint'. All searches and content viewed online is traceable; school systems cannot block everything - children and parents cannot rely only upon the filtering and school security systems to keep children safe online.
- All school laptops (staff and students) are password protected.
- Laptops that are used by students, passwords are not shared with students.
- Any school work created by students will be stored on an encrypted memory stick assigned to each student. All memory stick use is supervised and monitored, remain at school and are not taken home by a student. All devices are stored securely at school when not in use. No school work is stored on laptops.
- All staff mobile phones are password protected as well as other security features enabled. This includes logging and secure storing of phone IMEI numbers as part of asset register security policy.
- Staff are aware they must keep their passwords secure and not share them with any other person or persons.

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 'friend' a member of staff and 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.

5. The School Website

- The contact details on the website should be the school address, email and telephone number. 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.

6. Photos and Images of children

- When joining school, parents are asked to give consent for images of their child/children 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 EFL recording system of children, are taken using staff mobile phones that are registered on the MTE Assets register and are used to upload onto the EFL pupil school work cloud-based recording system.
- Any image that is taken, should be uploaded, then deleted, then removed from the recycle bin from the staff's device in close succession when using the EFL recording system. If any images are taken whilst offsite preventing direct upload, this must be done at earliest convenience when connecting to the internet and then deleted and removed from the device's recycle bin.
- Images of children can be shared internally via WhatsApp for the specific purpose of good practice and upload to EFL. All images should then be immediately deleted and also removed from the phone's recycle folder.
- Due to modern day mobile devices automatically linking to other owned devices; this setting must be turned off in order to not store school-based images online from any phone cloud-based backup system.
- Children may not upload images of themselves or other children.

7. 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, be they 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. The National Curriculum states that children should learn to use technology safely and respectfully, keeping personal information private; 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 in order to communicate on a professional basis and never to respond to any email that may have originated from a pupil's private address or any unfamiliar source.

8. Social networking and Digital Footprint

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

9. Emerging Technology

Emerging technologies will be examined for educational benefit and then risk assessed before use in school is permitted. Emerging technologies include: -

- **Artificial Intelligence (AI)** The implications AI has for children's privacy, safety, and security fall across a wide spectrum, from benefits related to the ability to understand threats facing children with greater specificity and accuracy than ever before (and respond accordingly), to risks around unintended privacy infringements. The positive and negative implications for children's privacy, safety, and security in an AI age are constantly changing as technology and understanding develops. As a school, we do not utilise AI, and AI is not included in our curriculum. For further details on AI and the risks to children and young people, please see our School Safeguarding and Child Protection Policy.

10. The EU General Data Protection Regulation (GDPR)

For organisations | ICO (https://ico.org.uk/for-organisations/)

This website is a resource to educate the public about the main elements of the General Data Protection Regulation (GDPR).
After four years of preparation and debate the GDPR was finally approved by the EU Parliament on 14 April 2016. Enforcement date: 25 May 2018 - at which time those organisations in noncompliance may face heavy fines.
The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy.
The key articles of the GDPR, as well as information on its business impact, can be found throughout this site.
The GDPR requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual.