

E-Safety Policy

More Than Ed | Independent School

Date: September 2026

Review Date: September 2028

Responsible Person: Jess Temple

Contents

1. Rationale.....	3
2. Aims.....	3
3. E-Safety.....	3
4. Practices and Rules.....	3
5. The School Website.....	4
6. Photos and Images of Children.....	4
7. Email within School.....	5
8. Social Networking and Digital Footprint.....	5
9. Emerging Technology.....	5
10. Data Protection.....	6
11. Related Policies.....	6
12. Legislation and Guidance.....	6

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 students, staff, parents and carers, and the wider community. We aim to give all students the skills they need, now and for the future, to embrace and adapt to an ever-changing digital world.

E-safety is the 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 students, to establish the ground rules for using the internet and electronic communications, educating students about the benefits and risks of digital technology and providing safeguarding protocol and awareness for all users.
- To demonstrate the methods used to protect students from sites containing pornography, racist or politically extreme views, and violence.
- To help students 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 or parents immediately.

3. E-Safety

E-safety is the duty of staff, parents and students. We educate our students so that all users of the internet are respectful, and so that the same standards of safety, equality and acceptable behaviour that apply in our communities are also applied online. As a community, we recognise and guard against bullying, intimidation, discrimination, grooming and the exploitation of vulnerable users.

Parental filters are enabled on all Wi-Fi, and all staff have up-to-date e-safety training. In school, students are taught how to stay safe and behave appropriately online, and parents and carers are guided and strongly encouraged to educate students on what to do if they encounter danger online and how best to deal with it. All staff take appropriate care, awareness and practice in line with the Data Protection Policy when undertaking work that involves online tools. All staff mobile phones and computers listed on the school asset register are password-protected and have appropriate internet security software installed. Access to email and WhatsApp requires a two-step authentication process, and CPOMS and Evidence for Learning (EfL) require password protection for access.

4. Practices and Rules

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

- Any recommended websites given to students are thoroughly checked by the teacher first.
- It is the responsibility of every member of staff to report any e-safety issues they witness or learn of, immediately, to the Headteacher.
- Students' names are not entered into any internet-based software.

- All internet use on the school premises is supervised, including students' access to devices during breaks or lunchtime.
- All students take part in e-safety-focused lessons.
- If staff or students find an unsuitable site accessed in school, the screen is switched off immediately, the device is closed, and the matter is reported to the Headteacher and the E-Safety Co-ordinator.
- Staff and students are aware that all school-based email can be monitored, and that all internet usage is monitored and regulated.
- All staff, parents and students sign an acceptable use agreement before using internet-based software.
- Students are taught that they are responsible for their own 'digital footprint'; all searches and content viewed online are traceable, and filtering and security systems cannot block everything.
- All school laptops (staff and student) are password-protected; passwords for student laptops are not shared with students.
- Any school work created by students is stored on an encrypted memory stick assigned to each student; memory-stick use is supervised and monitored, sticks remain at school, and no school work is stored on laptops. All devices are stored securely at school when not in use.
- All staff mobile phones are password-protected with other security features enabled, including the logging and secure storing of phone IMEI numbers as part of the asset-register security arrangements.
- Staff keep their passwords secure and do not share them with anyone.

Staff ensure that all their social media profiles are sufficiently secure and set to private, and no social media account is held under a member of staff's official name. Staff are not permitted to accept any request from a student to connect on social media; if this happens, it must be reported to the Headteacher immediately. Any form of online connection with students who attend the school is strictly prohibited and may lead to disciplinary action. The school does not encourage online connections with parents; where staff have friends or family who are parents, they must uphold their professional responsibility to ensure school information and data are not compromised.

5. The School Website

- The contact details on the website are the school address, email and telephone number; staff or students' personal information is not published.
- The Headteacher is responsible for the content and editorial choices.
- Students' full names are not used anywhere on the website.
- Written permission from parents or carers is obtained before photographs of students are published on the website.

6. Photos and 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 held by the Headteacher.

- All photographs of students for use on Evidence for Learning (EfL) are taken using staff mobile phones registered on the MTE asset register, and are used to upload to the EfL cloud-based recording system.
- Any image taken is uploaded, then deleted and removed from the device's recycle bin in close succession. If images are taken off-site, this is done at the earliest opportunity when connecting to the internet, and then deleted.
- Images of students may be shared internally via WhatsApp only for the specific purpose of good practice and upload to EfL, and are then immediately deleted and removed from the phone's recycle folder.
- Because modern devices automatically link to other owned devices, this setting is turned off so that school-based images are not stored online via any phone cloud-backup system.
- Students may not upload images of themselves or other students.

7. Email within School

Email is an essential means of communication for both staff and students. In the context of school, email should not be considered private. The national curriculum states that students should learn to use technology safely and respectfully, keeping personal information private, and to identify where to go for help and support when they have concerns about content or contact online. We recognise that students need to understand how to style an email appropriately for their age. 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 student's private address or any unfamiliar source.

8. Social Networking and Digital Footprint

- All access to social networking sites is blocked within school for students.
- Students and parents are advised that the use of social network spaces outside school is inappropriate for our students.
- Students are educated on the safe use of social networking and the implications of their digital footprint, to prepare them for the future.

9. Emerging Technology

Emerging technologies are examined for educational benefit and then risk-assessed before use in school is permitted.

Artificial intelligence (AI): the implications of AI for children's privacy, safety and security range from benefits, such as identifying threats to children with greater accuracy, to risks, such as unintended privacy infringements, and these change constantly as the technology develops. Students do not use AI in school, and AI is not part of the curriculum. Staff use approved AI tools for professional purposes only, in line with our Artificial Intelligence (AI) Policy. For further detail on AI and the risks to children and young people, please see our Safeguarding and Child Protection Policy.

10. Data Protection

The school processes personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Anyone who handles personal information must comply with the data protection principles when processing personal data relating to any living individual. Further information and guidance is available from the Information Commissioner's Office (ICO) at ico.org.uk. Full detail of how the school collects, uses and protects personal data is set out in our Data Protection Policy and privacy notices.

11. Related Policies

This policy should be read alongside the school's other policies, including:

- Acceptable Use Policy
- Safeguarding and Child Protection Policy
- Data Protection Policy and Privacy Notices
- Cyber Security Policy
- Anti-Bullying Policy
- Artificial Intelligence (AI) Policy

12. Legislation and Guidance

In drawing up this policy, the school has had regard to the following:

- Keeping Children Safe in Education (DfE, current edition), including the filtering and monitoring standards
- Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR)
- Education for a Connected World framework (UK Council for Internet Safety)
- Equality Act 2010