Maiden Erlegh Trust

PROTOCOL FOR ACCEPTABLE USE OF DIGITAL TECHNOLOGY FOR STUDENTS

MAIDEN ERLEGH
TRUST

Initial approval:	May 2019
Review frequency:	Every three years
Date(s) reviewed:	August 2010, August 2023, April 2024

Contents

Acceptable use of Digital Technology agreement for students

The use of digital technology and the internet are constantly opening new opportunities for students. They are acquiring new skills and are using technology to an increasing level of sophistication, and this is having a very positive impact on their learning across all subjects. To use digital technology effectively requires students to have an awareness and understanding of the benefits but also of the risks and how to take responsibility for protecting themselves and the equipment they are using.

As part of our Trust's School curriculum, the Trust uses Google Apps for Education. This service is powered by Google with over 8 million other students and teachers around the world using it. The service gives our students and staff access to a set of tools which will support the high levels of collaboration that are required in today's classroom to prepare students with communication and collaboration skills for life. Apps for Education also enhances the delivery of not only our Computing curriculum, but lessons cross curricular. In order to keep you informed and also to comply with data protection legislation and Google's Terms of Service we are required to get parental permission.

We also use a number of other Online Services to support the education of our students. All the suppliers of these services have been checked for their UK General Data Protection Regulations (UK GDPR) and Data Protection Act 2018 (DPA 2018) compliance in line with current legislation.

On the next page of this document are our expectations of students when using digital technology in the Trust's schools. We should be grateful if you and your child would read them through and then sign in the spaces provided to show your agreement.

Ultimately the Trust cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, however, it is understood that the Trust will take every reasonable precaution to keep students safe and to prevent them from accessing inappropriate materials whilst in our care. These steps include an educationally filtered service, restricted access e-mail, the teaching of e-safety skills to students and high-quality teaching practices.

You need to be aware that the Trust can check any files held on any digital device, applications used and the internet sites the students visit, and that if the Trust has concerns about their e-safety or e-behaviour that the Trust will discuss this with parents. High level monitoring of all ICT use takes place, and any misuse is reported.

It is expected that you will support the Trust by promoting safe use of the internet and digital technology at home and will inform the Trust if you have any concerns over your child's e-safety

Such expectations on the acceptable use of Digital Devices are now standard procedure in most schools, but if you are concerned about any aspect of this, please contact the Trust's Strategic and Classroom ICT Advisor.

Rules for acceptable use of Digital Technology

Students are responsible for:

- The care of any Trust equipment they use in the Trust's schools (including printers, copiers, cameras, smart devices etc).
- Not causing any damage to data stored on the network
- The safety of any personal mobile phone or personal device brought into the Trust's schools. The Trust will not take responsibility for personal devices that have been lost, stolen, or damaged.

- Their use of the network, the internet and email and must never seek out or create materials or content which someone else may find offensive, threatening, or which be construed as any form of bullying/harassment or grooming/radicalisation.
- Not bringing into the Trust's schools or create material in any form which could be considered to be offensive to anyone else or be construed as any form of bullying or harassment. This includes paper or electronic copies or social networking sites/profiles/content.

Students should:

- Read and abide by the Trust's E-safety and Acceptable Use Protocol.
- You are responsible for account access on the Trust network. Any unauthorised use of your account should be flagged to the Trust's ICT team immediately.
- Use of the Trust network is regularly monitored by the Trust's ICT team (which includes email access). The Trust will monitor any traffic over the Trust system to prevent threats to the Trust's network.
- You should not write down or share your password with anyone else.
- You are not permitted to share access details to the School's network or Wi-Fi password with anyone else.
- Not use the Trust's schools' printers/copiers for personal material. We reserve the right to charge parents for personal printing in the Trust's schools and/or where it has caused disruption to the work of the Trust's schools, students will be sanctioned.
- Never log on to the Trust's network using someone else's ID or password or attempt to access or alter another student's work in any way. Any unauthorised use of your account should be flagged to the School's ICT team immediately.
- Use "strong" passwords (a mix of upper, lower, and numerical characters) and change them regularly.
- Keep their logon ID's or password's private and change their password if they believe them to be known to another person.
- Always log off when leaving a computer.
- Never download or install program files onto a Trust schools' computer or the network without the express permission by a member of IT Support.
- Only access internet material or software which is age- and task-appropriate.
- Acknowledge sources of information used in work and respect copyright.
- Report any inappropriate or unsuitable sites immediately to a member of staff.
- Only use Trust email accounts for Trust-approved activities and never during lesson time, unless directed by a member of staff.
- Only email people they know or those approved by a member of staff.
- Only use personal headphones in the Trust's schools as directed by a member of staff, and this must never cause a disturbance to anyone else or be in defiance of a member of staff.
- Never take and/or publish images (still or moving) of staff or students without their permission.
- Not access social networking/media or personal publishing sites during the Trust's school day or during a Trust-organised activity without the express permission of the lead member of staff.
- Never use social networking/media or personal publishing sites to bully, harass, impersonate, or bring into disrepute any member of the Trust community or the Trust itself.
- You must be mindful of the information that you post/share/send online and how this may impact others i.e., you should be kind online.
- Never take photographs, videos or audio recordings of other students or staff without permission
- Must not attempt to circumvent security of any host, network or account, or penetrate security measures ("hacking") on or accessed through the School network
- Must not probe, scan or test the vulnerability of the network or other networks.

- Must not try to install any software on School systems without permission from the ICT team. If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.
- Any apps or software that are downloaded onto your personal device whilst using the School's network is done at your own risk and not with the approval of the School.
- Storage media such as USB sticks and hard drives are prohibited at the Trust.

Additional guidance for students in Years 12 and 13

Users of Personal Devices must agree to all terms and conditions in this policy as well as the additional ones listed below to be allowed access to those Maiden Erlegh Trust services:

- When used on the Trust's school sites, the device must only be used for Trust tasks. Irrespective of security precautions mentioned here, you are expected to use your device in an ethical manner and in accordance with Maiden Erlegh Trust IT Acceptable Use Protocol.
- Using your device in ways not designed or intended by the manufacturer is not allowed. This includes, but is not limited to, 'jailbreaking' or 'rooting' your device.
- Some personal devices can be connected to the Maiden Erlegh Trust infrastructure or services, but the user is personally liable for their device and carrier service costs.
- We do not guarantee to be able to add all devices to our student wireless network and we advise students to refer to IT Support to review the device prior to purchase.
- Users of personal devices are not permitted to connect to Maiden Erlegh Trust infrastructure without permission from the School Business Manager and such access will be logged.
- We reserve the right to disable or disconnect some or all services without prior notification.
- We will provide access to the student wireless network only.
- We do not guarantee to be able to retrieve data lost if stored on a personal device and not backed up on the network.
- We reserve the right to inspect the device and monitor its use on the network if the Trust feels inappropriate material is stored on it, or if it has been used in breach of the AUP in any way.
- Students must have signed the school AUP.
- The Strategic and Classroom ICT advisor will help them set up the device in the first instance and provide key running information. He will do this at his convenience, the business of the school taking priority.
- IT Support will in no way support the maintenance of personal devices or any issues caused by using the device on the network.
- We reserve the right to withdraw this privilege at any time where it is in the school's interests.

The Trust reserves the right to change the users password of a student for investigation reasons if malicious or indecent behaviour is suspected.

Computer use is monitored electronically at both a high and low level and staff may request access to any files which a student may have, both on the network or on a personal portable device.

Any student who does not keep to these rules will be dealt with according to the Trust Rewards, Sanctions and Attendance Policy.

Please see Annex 1 for NetSupport DNA Monitoring statement provided by the School Improvement Director: Culture and Safeguarding and Trust IT Network Manager.

Student Agreement

Student Name		
I have read the *Rules for the Acceptable Use of Digital Technology* with my child and agree to these safety restrictions and any subsequent changes. I give my consent for my child to use Online Services and the internet in the Trust's schools. I fully support the Trust and will promote good e-citizenship at home. I understand that my child is responsible for their own ICT use in the Trust's schools.		
Parent/Guardian signature		**Date:**
I have read the *Rules for the Acceptable Use of Digital Technology* and agree to these safety restrictions.		
Student signature		**Date:**

ANNEX 1: NetSupport DNA Monitoring

Online safety and effective monitoring are key features of keeping children safe.

NetSupport DNA is the tool used by Maiden Erlegh Trust to ensure that the internet is used safely in all our schools.

This piece of software is constantly monitoring activity on all PC's as well as internet traffic. All activity is cross referenced against a bank of URLs and a glossary of words and phrases that could be a cause for concern. These are regularly updated and reviewed by NetSupport as well our inhouse network management team.

When an alert is triggered by a pupil/student, an email is sent to the Designated Safeguarding Lead.

All alerts will be assessed for risk and any that are judged to be safeguarding concerns will be followed up.

For online activity that contravenes the Acceptable Use Policy, appropriate staff will follow up with pupils/students. This could lead to sanctions up to and including Permanent Exclusion (for a child). If necessary, the police and local authorities will be informed.

For questions about in-school monitoring, please contact your headteacher; for general questions about safeguarding contact the School Improvement Director: Culture and Safeguarding; and for technical questions contact the Trust IT Network Manager.

ANNEX 2: Artificial Intelligence Policy For Pupils And Parents

Background

Although Data Protection law does not specifically define or discuss the guidelines for Artificial Intelligence ('AI'), the guidance from the Information Commissioner's Office and the UK government defines it as using non-human systems to imitate human intelligence.
In this time of constant development and increased usage, there is a need to provide you with an awareness of how AI will be used by the school and the guidelines for usage by pupils, especially if being used to complete school work.

Staff authorised usage of AI

We permit the informed and responsible use of generative AI applications by staff in carrying out identified business activities. Staff will comply with the terms of the workforce specific policy when using generative AI to carry out business activities.

We permit the informed and responsible use of authorised AI applications by staff, for the following business purposes:

- Drafting internal guidance, training and presentations;
- Lesson planning
-
- Conducting research
- Developing code
- Providing summaries
- Idea generation

Where personal data is used with AI applications, an ICO risk assessment and/or data protection impact assessment ('DPIA') has been carried out to ensure transparency in how AI will be used and what mitigating steps have been taken to reduce any potential risk of harm to pupils, staff and any other data subjects whose data might be shared with the authorised systems.

Authorised AI applications

The school allow access to the AI applications for business purposes.

The listed AI applications may be updated at any time.

Pupil usage of AI

As captured in Appendix A, we will require parents/pupils to sign an Acceptable Use Statement to ensure appropriate usage of AI and they are reminded of the permitted usage along with an outline of what classes as AI misuse.

The school permits pupil usage of AI in the following circumstances:

- As a research tool
- Idea generation for projects
- For use with coursework or homework with the above requirements fulfilled

Data Privacy

The Trust are yet to permit or encourage the usage of AI to process personal data at this time but are aware of the data protection responsibilities to be transparent of such usage and will update the policy as and when needed.

Related Policies

Pupils (and parents) can refer to the following policies that are related to this AI Policy: -
Data Protection Policy
Data Breach Policy
Privacy notice for parents and pupils.
IT and any related communications policies

These are available on the school website.

Breach of this policy

If at any time you feel a data breach has occurred in relation to data used, stored or shared with the AI system, please refer to the schools Data Breach Policy and/ or notify the School Business Manager so that this can be investigated.