ETONBURY ACADEMY

POLICY TITLE: E-Safety & The Acceptable Use of ICT Facilities Policy

---

STATUS:	Non-Statutory
REVIEWED BY:	Local governing body/ Principal
DATE OF APPROVAL:	May 2023
FREQUENCY OF REVIEW:	Annually
DATE OF REVIEW:	May 2024
AUTHOR:	SLT

Rationale and Aim

The purpose of this policy is to establish safe working practices in school for using IT resources, so that we get the best possible outcomes for our young people.

IT resources are a very important part of school life and provide many helpful ways to improve the outcomes for children and young people and they are a useful tool for staff to make them more effective in their work. We recognise that there are a number of risks associated with using IT resources which we need to help our young people understand and protect them from. We also need to protect staff from the dangers associated with IT resources.

Policy

This policy applies to all members of the school community (including all employees, students, volunteers, parents/carers, governors and visitors) who have access to and are users of school IT systems, both in and out of school.

The Principal and the SLT are responsible for ensuring:

- The establishment and review of the school e-safety policies and documents.
- That there is one member of the SLT team who has strategic oversight of IT.
- That adequate training is provided, including informing all users of the relevant procedure in the event of an e-safety allegation.
- That effective monitoring systems are set up.

The IT Network Manager is responsible for ensuring that:

- The school's IT infrastructure is secure and meets e-safety technical requirements.
- The school's password policy is adhered to.
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- They keep up to date with e-safety technical information.
- The use of the school's IT infrastructure is regularly monitored in order that any misuse or attempted misuse can be reported to the appropriate persons.

Currently Etonbury Academy engages the services of Partnership Education for day-to-day support of the school's PCs, laptops, printers and servers with BEST IT Support Team providing authority infrastructure. The IT Manager therefore has an additional responsibility to ensure that the support team adhere to the above e-safety measures during the course of their activities and are aware of the E-Safety & The Acceptable Use of ICT Facilities Policy.

Teachers and Support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They have read, understood the ETA Practical Information and BEST Staff Code of conduct
- E-safety issues are embedded in the curriculum and other school activities.
- Students understand and follow the school's E-Safety & The Acceptable Use of ICT Facilities Policy.
- They monitor IT activity in lessons, extracurricular and extended school activities, including the appropriateness of websites for research etc.
- Reporting abuse, misuse or notifying of access to inappropriate materials.

Students are responsible for:

- Using the school IT systems in accordance with the Home School Agreement – Student Internet Use (appendix 1), which will also be shared with parents/carers.
- Reporting abuse, misuse or notifying of access to inappropriate materials.
- Adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy also covers their actions out of school, if related to their membership of the school.
- They have read and understood the Home School Agreement – Student Internet Use (appendix 1)

Procedure

Email

All digital communications with students should be on a professional level and only carried out using official school systems. Under no circumstances should staff contact pupils, parents/carers or conduct any school business using personal email addresses. School email is not to be used for personal use. Staff should be mindful of the need to protect other users', such as parents', personal email addresses when sending emails to more than one address by using the school communications software or, if necessary Blind Carbon Copy (Bcc) option in an email client.

Mobile Devices and digital images.

Staff should avoid, wherever possible, using their own personal devices to record digital images (photos or videos) of students, rather they should be using school owned mobile devices. Where this is not practical, the images should be transferred to the school network shared drives, including Etonbury cloud storage (Google Drive), or to an official school social media account (such as a department twitter/facebook account) and then the original photos should be removed from the private phone, and any personal backups deleted. Staff should not store images or videos of students on their own personal devices.

Staff will not post images of children from other schools on ETA social media (for example in sports fixtures).

Data Security: Files and Cloud storage

Staff are expected to use Google Drive for storage of all files and folders. Shared drives for departments and multiuser use are created to enable sharing and collaboration of data.

The use of USB storage devices is discouraged as this can lead to the unintentional threat of malware and other IT security issues. When accessing and storing folders staff should also follow the BEST Data Protection (GDPR) Policy.

Security: Virus and other Malware

Staff should be always conscious when accessing emails and files that could be a security threat. Considering the following:

- Do you know who sent the email?

- Is the email structure correct when you look at the properties of the address?
- Is the content relevant?
- Delete junk emails without opening
- Do not open suspicious hyperlinks in emails
- Do not open suspicious attachments.

Use of Own Equipment

Students are encouraged to bring their own devices to school (BYOD), but must follow the instructions of teachers in relation to their use in school. All private equipment is brought in to school at the owners' risk and the school takes no responsibility for loss or damage to that equipment whilst it is on site.

Use of School Equipment

All users should ensure any screens are locked before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

Responding to incidents of misuse

Any e-safety incidents must immediately be reported to the SLT member with strategic oversight of IT who will investigate further. Staff investigating an incident should immediately impound the equipment if needed. It is important that any incidents are dealt with as soon as possible in a proportionate manner, this will be done in line with Hr and safeguarding policies.

Links with other Policies

This policy must also be read in conjunction with the

- Behaviour Policy
- Home School Agreement
- Relationships and Sex Education Policy
- Safeguarding Policy
- Anti-Bullying Policy
- Child-on-Child Abuse Policy
- Keeping Children Safe in Education
- Working Together to Safeguard Children
- Data Protection (GDPR) Policy & Privacy Notices
- Visitors Policy (include use of mobile phones)
- ETA Practical Information and BEST Staff Code of conduct

Monitoring and Evaluation

All incidents of IT misuse are logged. Trends are analysed and appropriate action taken by senior staff.

Implementation and Review

This policy will be made known to all staff, parents/carers and governors, and published on the Academy website. Copies are also available upon request from the Academy office. This policy will be reviewed annually or as required.

Appendix 1 – Home School Agreement – Student Internet Use

As a school user of the internet, I agree to comply with the school rules on its use. I will use the network in a responsible way and observe all the restrictions explained to me by the school.

Student Internet Use

- I will only use ICT systems in school, including the internet, email, digital video, mobile technologies etc for school purposes
- I will neither download nor install software on school technologies
- I will only log on to the school network/learning platform using my own username and password
- I will follow the school's internet security system and not reveal my password to others
- I will make sure that all my ICT communication is responsible and sensible
- I am responsible for my behaviour when using the internet. This includes the resources I use and the language I use
- I will not browse for, download, upload or forward any material that may be offensive or illegal. I will report any such material to my teacher or ICT manager immediately
- I will not give out any personal information such as my name, phone number, address or photograph. Neither will I give out any personal information about others
- Images of students/staff will only be taken, (when prior consent has been given by the school) stored and used for school purposes in line with school policy and they will not be distributed outside the school network
- I promise that my on-line activity, both within school and elsewhere, will not cause distress to anyone or bring my school into disrepute
- I will respect the privacy and ownership of others work on-line at all times
- I will not copy material from the internet and present it as my own
- I will not attempt to bypass the internet filtering system
- I understand that all my use of the internet and other related technologies can be monitored, logged and made available to the ICT manager
- I understand that this code is to keep me safe and to highlight the responsibility I have towards others. If I choose to break this code the school will apply sanctions and will contact my parents/carers