EATON HOUSE SCHOOLS

ICT ACCEPTABLE USAGE POLICY

Responsibility:	Mrs Roosha Sue (Head, EHTM Nursery) Mrs Claire Fildes (Head, EHTM Girls') Mr David Wingfield (Head, EHTM Prep) Mrs Kirsten Bond (Head, EHTM Pre-Prep) Mr Ross Montague (Head, EHB) Alison Fleming (Principal, Eaton House Schools) Mr Liam Corbett (Bursar, Eaton House Schools) Mr Darren Arnold (IT Manager)
Reviewed:	August 2025
Current version no:	2025v1
Approved by the Governing Body:	
Next review:	August 2026

Contents

Policy Statement 3
Organisation of ICT usage 3
Responsibilities for ICT usage 3
Responsibilities of Staff 3
Use of portable computer systems, USB sticks or any other removable media 5
Use of digital images 5
Use of School Hardware – Laptops, Cameras, Recording Equipment, etc 5
Staff use of the School Network 6
Measurement and Review 6
Education and Training 6
Confidentiality 6
Pupil use of the School Network and Equipment 7
ICT Pupil Code of Practice Agreement 8
ICT Staff Code of Practice Agreement 9

Policy Statement

This policy is designed to make clear the responsibilities of staff in regard to the use of Eaton House Schools computer hardware and facilities.

Organisation of ICT usage

The organisation of ICT usage is the responsibility of the IT Manager.

Responsibilities for ICT usage

In relation to ICT usage, the IT Manager, is responsible for:

- ensuring that this acceptable use of ICT policy is made available to all staff and that appropriate acceptable use guidelines are displayed prominently around the School. The ICT Usage policy is provided to new staff during the staff induction process and is available on the School website.
- putting systems in place to identify staff training needs
- ensuring that any information or data stored on the cloud is protected and personal data is kept secure
- recommending any improvements to ICT systems to ensure the security and safety of the network.

Responsibilities of Staff

Staff have a responsibility, as part of the Eaton House Schools ICT policy, to comply with the following usage policy:

Use of the internet on School premises should principally be for School use, e.g. accessing learning resources, educational websites, researching curriculum topics, use of email on School business.

Staff are allowed to use School equipment, when it is not required by pupils, outside their own individual working hours. This includes laptops provided for the use of one or more members of staff. It also includes the use of e-mail, the broadband link, the School network and the internet.

Equipment provided on short-term or long-term loan to staff remains the property of the School and must be available for inspection at all reasonable times. If a laptop is provided, it is expected that it should be brought to School on a regular basis.

Use of the Schools internet for personal financial gain (including the use of online auction sites), gambling, political purposes or advertising is excluded.

Teachers should not be accessing the internet for personal reasons whilst teaching children. This includes accessing the internet via their mobile phones whilst teaching or supervising children.

In no circumstances should members of staff access websites that are clearly inappropriate (e.g. those that could be considered pornographic, racist, sexist or otherwise offensive). It is possible to access such sites by accident, in which case an individual member of staff should report this to his/her line manager. Evidence of repeated visits to such sites, the downloading of materials from such sites and the use of search criteria (e.g. individual words) that might lead to such sites, will be treated as a disciplinary matter.

There is software in place to monitor all usage by pupils and staff of the School network. Staff should also be aware that computers usually “leave a trail” of documents worked on, websites visited, emails sent/received and so on.

Members of staff should not send or circulate emails which are offensive.

It is imperative that staff protect their password(s) at all times. Staff must log off when they are leaving a computer, even for a short time, since the security of the intranets and internet depend on the staff member locking their computer.

The School recognises that information can be accessed online through the 'streaming' of data, i.e. radio, television, music, etc. Teaching staff should only be accessing streamed information if it is of educational interest to a lesson or to its planning. For example, using BBC iPlayer is acceptable if it is the interest of the class and related lessons. Streaming music for personal use is discouraged. This is due to the streaming process placing demands on the Schools internet bandwidth; as a result the internet can become slow for all users.

Staff are alerted to the fact that they should only download files from reliable sources. If in doubt, do not download and/or respond to emails from unknown sources.

Staff should never knowingly expose the network to risks, such as those from computer viruses or other malicious software or programs.

Staff should remember that any materials downloaded for publication must include an acknowledgement of the source.

All staff who use School ICT resources must do so with reference to UK decency laws, including the Computer Misuse Act 1990, and should report any misuse that they find evidence of to their line manager and the IT Manager.

Use of portable computer systems, USB sticks or any other removable media

All personal data including sensitive data, such as children's personal details and report comments, medical information must not be stored on portable devices.

Please refer to the Data Protection Policy and Privacy Notice Policy regarding to further information on personal data and data processing and protection.

Use of digital images

Any photos or videos taken by teachers, other adults (including parents), and the children themselves during any School activity (including educational visits) should not be put on public display, without express permission. Photos of children should not be published anywhere on the internet (including social networking sites such as Facebook).

The above excludes the publication of photos on the School website and the Schools social media platforms which must go through the marketing department for authorisation and alongside use by School for educational/display uses.

Use of School Hardware – Laptops, Cameras, Recording Equipment, etc.

Use of School laptops, cameras, video cameras and recording equipment is limited to activities directly related to School activity. They can be used during lessons, sporting activities, School visits and residential trips. They are not for personal use.

All data must be transferred to the School network as soon as possible to ensure that data is saved and protected. Once copied to the network the data must be deleted from the recording equipment.

Staff use of the School Network

All members of staff will be given a username and password. Staff must log onto the School network using only their own username and password. Staff are not permitted to use anyone else's details to log onto the School system.

Staff must not download software onto the School network before first liaising with the IT Manager.

Staff must not use personal product keys to install software onto the network. This is a breach of the terms of the software license, and therefore the School will be in breach of licensing laws.

School resources, such as software, etc. are for the use of staff and pupils within the School premises only and should NOT be taken home for personal use.

All external programs/software which are being considered whether online or on the computers must be authorised by the IT Manager before purchase.

Measurement and Review

Eaton House Schools will establish and maintain programmes for the review of ICT usage in School.

The IT Manager and DSLs ensure that appropriate filtering and monitoring systems are in place on School equipment, networks and when accessing internet in the Schools, (as per the DFE filtering and monitoring standards. This is reviewed annually.

Teaching staff ensure pupils are taught about online safety.

Education and Training

It is important that education and training are seen as being part of the productive use of ICT equipment. This training can be formal or informal. Through training, ICT usage can be made more productive.

Confidentiality

The School will have information about ICT usage (including access to the internet) but will not publish it without the written consent of the individual. Employees have a statutory right of access to their own records.

This does not preclude non-confidential records being reported to ensure the School has a basis on which to take remedial measures, safeguards and decisions affecting its employees'

interests.

Pupil use of the School Network and Equipment

Teaching staff will explain the code of practice for IT when using the Schools equipment and network. Year 4 and above pupils must understand and sign the Pupil ICT code of Practice Agreement prior to using the equipment and network.

ICT Pupil Code of Practice Agreement

1. I know that I will be permitted to use the internet if I use it responsibly. I understand that if I do not, I may not be allowed to use the internet at School.
2. I know that being responsible means I should not look for bad language, inappropriate images or violent games, and I know that if I accidentally come across any I should report it to a teacher or parent. I know that my teacher can check the websites I have visited.
3. I will log off when I have finished using the computer.
4. I will NEVER tell anyone I meet on the internet, my home address, my telephone number or my Schools name, or send a picture of myself. I will NEVER arrange to meet anyone in person.
5. If someone says or writes something whilst I am on the internet or gaming, which makes me feel uncomfortable or worried, I will always report it to a teacher or parent.
6. I will never answer unpleasant, suggestive or bullying emails or messages and I will always report them to a teacher or parent. I know not to delete them straight away but show them to the person I have reported it to, as evidence.
7. I will always be myself and not pretend to be anyone or anything I am not. I know that the posting of anonymous messages and the forwarding of chain messages is not allowed.
8. At School, I may not download any software from the internet. I know that information on the internet may not always be reliable and may need checking. I know that some websites may be sponsored by advertisers.
9. If I bring in memory sticks from outside School I will give them to the teacher to check for viruses and content, before opening a file.
10. I will be polite and sensible when I email or communicate with others online and will not send, or encourage material which may offend or annoy others or invade another person's privacy.
11. I know that I am not allowed to access personal e-mail, social networking sites or instant messaging in School.
12. If I bring a mobile phone to School I will take it to the SMT Office as soon as I arrive.
13. I will not change the settings on the desktop or internet browsers or mouse pointers as I know these are not my own personal computer and are School property.

I have read and understand the ICT Code of Practice for Pupils and agree to it.

Name: _____ Form: _____

Date: _____

ICT Staff Code of Practice Agreement

- Use of the internet on School premises should principally be for School use, e.g., accessing learning resources, educational websites, researching curriculum topics, use of email on School business.

- Whilst the School has a robust spam filter in place staff must remain vigilant and to not open any links if unsure whether the email has come from a legitimate source.

- Use of the Schools internet for personal financial gain (including the use of online auction sites), gambling, political purposes or advertising is excluded.

- Staff should only be accessing *streamed* information if it is of educational interest to a lesson or to its planning.

- Teachers should not be accessing the internet for personal reasons whilst teaching children. This includes accessing the internet via their mobile phones whilst teaching or supervising children.

- Use of the internet to access any illegal sites or inappropriate material is a disciplinary offence.

- All staff who use School ICT resources must do so with reference to UK decency laws, including the Computer Misuse Act 1990, and should report any misuse that they find evidence of to their line manager and the IT Manager.

- Staff must recognise that it is not appropriate to discuss issues relating to children or other staff via social networks.

- It is never acceptable to accept a 'friendship request' from pupils at the School, or ex-pupils who are minors. Member of staff should exercise their professional judgment at all times. Please refer to the Staff Behaviour- Safeguarding (Code of Conduct) Policy.

- All personal data including sensitive data, such as children's personal data details and report comments, medical information must not be stored on portable devices. Please refer to the Data Protection Policy and Privacy Notice Policy regarding to further information on personal data and data processing and protection.

- Teaching staff using the iSAMS App on their phone must ensure that they do not allow anyone else to access the App. It is password protected and the password must never be shared with anyone else.

- Memory sticks for Schoolwork should not contain children's personal data or any other sensitive data.

- Staff should NOT use their personal phones for taking photographs of children.

- Mobile phones should not be used when teaching, unless in an emergency.

- Any photos or videos taken by teachers, other adults (including parents), and the children themselves during any School activity (including educational visits) should not be put on public display, without express permission, and must not be published anywhere on the internet (including social networking sites such as Facebook).

- The above excludes the publishing of photos on the School website and the Schools social media platforms which must go through the marketing department for authorisation and alongside use by School for educational/display uses.

- Use of School laptops, cameras, video cameras and recording equipment is limited to activities directly related to School activity. They are not for personal use.

- All data must be transferred to the School network as soon as possible to ensure that data is saved and protected. Photos and videos must be deleted from laptops, cameras, video cameras and recording equipment.

- Staff must log onto the School network using their own username and password only. Staff must not access the School network using the a*dministrator* username and password or any other person's log in details.

- Staff must not download software onto the School network.

- Staff should not be using personal product keys to install software onto the network.

- School resources are for the use of staff and pupils within the School premises only and should NOT therefore be taken home for personal use.

- Staff must always lock computers when leaving the classroom/room. This is to protect personal data and to prevent unauthorised persons accessing the School system and personal data of pupils, parents and staff.

- I understand the importance of training to ensure productive use of ICT equipment and safe practices and confirm that all training will be completed as and when required.

It should be understood by all staff that this Code of Practice is in place to protect staff from potential risk in their use of ICT in their everyday work.

I confirm that I have read and understood the Acceptable Use Policy for ICT and agree to abide by it.

Name:_____ **Signature:**_____

Date:_____