# Acceptable Use of IT Policy - Pupils

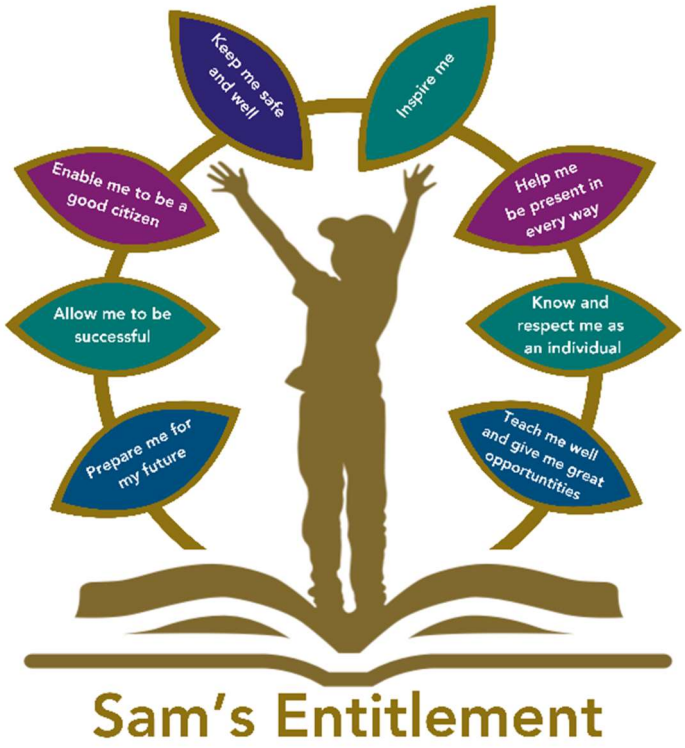
| | | | |
|---|---|---|---|
| Reviewed on | Sept 2025 | Review frequency | Annually |
| Next review due | Aug 2026 | Template Yes / No | Yes |
| Owner | J Solanki | Approved by | Executive |

## 1. History of Policy Changes

| Date | Page | Change | Origin of Change |
|---|---|---|---|
| | | | |

## 2. Contents

1. History of Policy Changes ..... 2
2. Contents ..... 2
3. Introduction ..... 3
4. Scope ..... 4
5. Definitions (delete as appropriate) ..... 4
6. Terms of use ..... 4
7. School Specific Systems ..... 6
8. Passwords ..... 7
9. Software ..... 8
10. Artificial Intelligence (AI) ..... 8
11. Network Access and Data Security ..... 8
12. Unacceptable Use ..... 8
13. Breaches of Policy ..... 9
14. Monitoring & Review ..... 10




## 3. Introduction

"Hamwic Education Trust (HET) believe that all pupils should receive a high quality, enriching, learning experience in a safe and inclusive environment, which promotes excellence through a broad curriculum that prepares them for their future and opens doors to a diverse array of opportunities as well as that all pupils and adults within HET flourish as individuals and together." Digital technologies have become integral to the lives of children, young people and adults, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. People should have an entitlement to safe access at all times.

This Acceptable Use of IT Policy is intended to ensure:

- That people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that everyone has good access to digital technologies to enhance their learning and will, in return, expect them to agree to be responsible users.

This policy aims to ensure a safe, secure, and productive IT environment for all pupils, promoting responsible digital citizenship.

## 4. Scope

This policy applies to all use of IT hardware, software, devices, networks and communications by anyone who has access to any of the school's IT resources, or to non-school owned IT resources, for anything that may impact on the school or members of the school community.
All pupils/parents are responsible for reading, understanding and complying with this procedure if they have access to IT. All leaders are responsible for supervising and supporting their team to read, understand and comply with this procedure if they have access to IT.
The Data Compliance Officer (DCO) provides assistance and further guidance on the use of IT in line with DP legislation, with guidance from the HET Data Protection Officer (DPO).

## 5. Definitions

- HR' in this policy, means Hamwic Education Trust HR.
- 'Local Governing Committee' in this policy, where reference is made to the Governing Committee, this means the Local Governing Committee of the school, or the Trust in the case of a school where no Local Governing Committee is present. Where a Governing Committee is not present in a school, or numbers are low, Governors from other schools/partnerships may be used.

## 6. Terms of use

Pupils are permitted to use IT resources solely for educational purposes, research, and academic-related activities. Unauthorized access, use, or distribution of any inappropriate, illegal, or offensive content is strictly prohibited.

- **Responsibility**: School IT systems must be used in a responsible way, to ensure that there is no risk to your safety or to the safety and security of the IT systems and other users.
- **Monitoring**: The school will monitor use of the systems, devices and digital communications.
- **Vandalism**: Please report any cases of vandalism to the IT support team/school/Trust, and appropriate action will be taken by the school to recover any costs for loss or damage.
- **Personal use:** The school systems and devices are primarily intended for educational use and you cannot use them for personal or recreational use unless you have permission.
- **Concerns**: If you have any concerns about the IT, data or content, please inform the IT support team immediately.
- **Data security & retention**: Data is backed up daily**.** If you should accidentally delete/lose files in your folder or shared area, please inform your teacher immediately so that they can check with the IT Team if it can be recovered.
- **Protect school IT resources** by careful and considerate use of equipment and networks, reporting faults and minimising the risk of introducing computer viruses or similar to the system.
- **Protect Pupils** from harmful or inappropriate material accessible via the Internet or transportable on computer media. Network will be filtered and devices will be monitored to assist with this.
- **Protect the Confidentiality** of individuals and of school matters, including complying with the Data Protection Policy and supporting documents, and not sharing sensitive or private information without authorisation, either intentionally or unintentionally.
- **Monitoring & Logging:** All device activities may be monitored and logged and kept for an appropriate amount of time. Logs are taken for reasons of security, diagnostic and account/audit reasons. Logs are available only to authorised systems personnel and kept for no longer than necessary and in line with current data protection guidelines.
- **Equipment Disposal:** Hamwic will dispose of all redundant ICT equipment in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and the Data Protection Act 2018 (DPA). Any equipment that is to be resold must have a demonstrable audit trail to prove that is has been disposed of in line with ESFA requirements and authorisation has been sought by the same,

where appropriate. We will ensure that all data is wiped prior to disposal, which could potentially mean personal data being lost

| DO'S | DON'TS |
|---|---|
| • Keep usernames and passwords safe and secure | • Do not share them, or use any other person's username and password<br>• Do not write down or store a password where it is possible that someone will steal it |
| • Be aware of "stranger danger", when communicating on-line | • Do not disclose or share personal information about yourself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc) |
| • Report any unpleasant or inappropriate material, messages, or anything that makes you feel uncomfortable when you see it online | • Do not make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work |
| • Respect others' work and property | • Do not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission |
| • Report any damage or faults involving equipment or software, however this may have happened | • Do not take or distribute images of anyone without their permission |
| • Ensure that you use any remote access systems from safe locations where you cannot compromise any sensitive information that you may need to access | • Do not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others |
| • Lock screen if away from desk | • Do not use any programmes or software that might bypass the filtering/security systems in place to prevent access to inappropriate content |
| • Use secure systems for file transfers and/or sharing. Where possible keep all files stored on the school network and provide the location to the person so they can access it from there, rather than emailing the document | • Do not open any hyperlinks in emails or any attachments to emails, unless from a trusted person/organisation who sent the email |
| | • Do not send emails with personal details that could identify a data subject |
| | • Do not forward emails to home computers or personal email addresses |
| | • Do not leave documents in vehicles |
| | • When using social media, do not share information that can identify a data subject without permission |

## 7. School Specific Systems

### School IT Resources

The school will provide various IT resources within the school, including but not limited to:

- Curriculum Delivery devices (pupils use devices e.g. laptops, tablets, etc.)
- IT Suites

All these resources have to be used appropriately according to the terms of use laid out in this policy, the data protection policy and the equipment loan agreement.

### Email

You will be provided with an email address by the school, and the expectation is that you will use this facility for legitimate educational and research activity. You are expected to use email in a responsible manner. No messages should be sent or received if they contain any material that is sexist, racist, unethical, illegal, or likely to cause offence.

Remember when sending an email to:

- Be polite - never send or encourage others to send abusive messages
- Use appropriate language - remember that you are a representative of the school on a global public system. What you say and do can be viewed by others. Never swear, use vulgarities or any other inappropriate language
- Do not reveal any personal information about yourself or anyone else, especially home addresses, personal telephone numbers, usernames or passwords. Remember that electronic mail is not guaranteed to be private
- Consider the file size of an attachment, files exceeding 1MByte in size are generally considered to be excessively large and you should consider using other methods to transfer such files
- Do not download or open file attachments unless you are certain of both their content and origin. File attachments may contain viruses that may cause loss of data or damage to the School network
- Not engage in mass transmission of unsolicited emails (SPAM)
- Be vigilant to scam targeting communications especially phishing emails and know how to spot and report suspicious emails
- If you receive an email that is inappropriate or abusive, you must report it to your teacher immediately, who will take the appropriate action. If the sender is known to you, inform them that they should cease sending the material.

### General Email Guidance

- Emails should only be kept in your inbox for a limited time as recommended in the retention schedule. Any emails that you need to keep beyond this period should be moved to appropriate file storage.
- You must only use School provided email systems to send and receive School information.
- You must not use the email system in any way that is insulting or offensive. Any authorised personal data sent externally by email e.g. to solicitors, Inland Revenue etc. must be sent in compliance with the Secure Email Policy.
- You must not use anonymous mailing services to conceal your identity when mailing through the Internet, or falsify (spoof) emails to make them appear as if they have been sent from someone else.
- All emails are automatically tagged with the classification ‘controlled’. You should consider whether you need to change the classification to ‘public’ or ‘restricted’.

- If you receive an email that is inappropriate or abusive, you must report it to your line manager immediately, who will take the appropriate action. If the sender is known to you, inform them that they should cease sending the material.
- Email Disclaimer: A disclaimer is automatically attached to all emails sent from the School informing the recipient that the email is intended solely for them, is confidential, may be legally privileged and may contain personal views that are not those of the School.

**Copyright**

You may be in violation of copyright laws if you simply cut and paste material from one source to another. Most websites contain a copyright notice detailing how material may be used. If you are in any doubt about downloading and using material for official purposes, speak to your teacher.

**Remote Studying/Access**

We recognise that remote or mobile studying is required in certain situations, but this brings with it a number of potential risks, to data protection, confidentiality and privacy. The school offers remote access to pupils, and appropriate use of this technology is important.
The remote access system will enable users to access their documents and some school programs from anywhere they have internet access. Pupils are expected to use the remote systems in a safe and secure manner ensuring all data is kept secure and on the school storage systems for backup and compliance. School data must not be stored on any system other than issued equipment.

- Devices and documents must be kept secure when offsite, not left unattended on the screen or if printed, not left lying around for anyone to view.
- Data should never be sent to a personal email address, all electronic data must be worked on through the school's network
- Do not download any data off the school systems onto personal devices
- Use of Memory Sticks is NOT permitted.

will be encrypted and the IT support team will be able to track the device when it is off the school premises.
Any breach or misuse of this technology will lead to disciplinary procedures.

**Printers and Consumables**

Printers are provided across the school for use by pupils. Pupils are provided with a code/badge that they must keep private and use it to release the print jobs. You must use the printers sparingly and for school purposes only.

All printer use is recorded and monitored and therefore if you deliberately use the printer for non-education or offensive material you will be subject to the behaviour management measures of the school.

A printer security and accounting system is in operation across the school. This facility is used to monitor pupil use. Where pupils are unable to act responsibly when using the printing services, their use of these facilities will be removed.

**8. Passwords**

Access to applications and information is controlled to protect you and our organisation. It's important that the passwords you use are strong and safe enough to keep our data secure.
Choosing a secure password
When choosing your passwords:

- keep all account log in and system passwords private
- never write down your passwords or share them with anyone
- use a strong password - at least 10 characters with upper and lower case letters, numbers and special characters like asterisks or currency symbols
- Don't choose a password based on any personal data such as your name, age, or your address. Avoid using words (English or otherwise) as well as any proper names, names of television shows, keyboard sequence or anything else that can be easily guessed or identified.
- Putting punctuation marks or other symbols at the beginning or end of words is not advised either.

**9. Software**

- Users should use software in accordance with applicable licence agreements. It is a criminal offence to copy software or any supporting documentation protected by copyright.
- The use, or possession of unlicensed copies or "pirated" versions of software is illegal and is expressly prohibited by the school.

**10. Artificial Intelligence (AI)**

HET does not intend to prohibit the use of AI for pupils, however, there are protocols that would need to be followed when using AI. Please refer to the AI guidance policy and ensure that you follow this guidance for the use of AI.

**11. Network Access and Data Security**

- Pupils must only access information held on the School's computer systems if authorised to do so and the information is needed to carry out their work. Under no circumstances should personal or other confidential information held on the school network or IT equipment be disclosed to unauthorised persons.
- If you accidentally access information which you are not entitled to view report this immediately to the teacher.
- Pupils using computers in classrooms must ensure that confidential or sensitive data is not accessible to pupils or anyone else by logging off or locking the computer when away from the computer. In other areas, computers must not be left logged on when left unattended.

**12. Unacceptable Use**

You must not deliberately view, copy, create, download, save, print or distribute any material that:

- is sexually explicit or obscene
- is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
- contains material the possession of which would constitute a criminal offence
- promotes any form of criminal activity
- contains unwelcome propositions
- involves gambling, multi-player games or soliciting for personal gain or profit
- contains images, cartoons or jokes that may cause offence
- appears to be a chain letter
- brings the School into disrepute or exposes it to legal action

This list is not exhaustive and the School may define other areas of unacceptable use.

**13. Breaches of Policy**

Usage of school systems is subject to agreement to abide by this policy and any breach of the conditions will be dealt with, but not limited to some of the following:

- A warning
- A removal of access to services and/or devices i.e. internet, email, school computers and mobile devices
- Consequences such an official warning added to personnel file

In more serious cases or persistent breaches of this policy:

- Report to the school governors
- Report to appropriate external agencies like the police, CEOP or trade union
- Consequences such as disciplinary action for pupils

All pupils must sign and return this policy where it will be kept on their pupil file.

- I understand and accept that the School and HET will fully monitor my use of the school digital technology and communications systems.
- I understand that if my activity causes any concerns, safeguarding software installed across the School and Trust may automatically alert appropriate safeguarding specialists who may choose to investigate depending on the content of the alert.
- I understand that the rules set out in this agreement also apply to use of ICT technologies (e.g. iPads, laptops, email, school/Trust data etc.) out of school, and to the transfer of personal data (digital or paper based) inside or outside of the schools or Trust.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the Trust.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may access it.
- I will always lock or sign out of any device I am not actively using or will be leaving unattended and all devices under my control will require a username/password prompt or pin code before access is gained.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to my Tutor, a member of staff or appropriate safeguarding lead.
- I understand that if I leave the school/HET, all my digital accounts will be suspended, and my data deleted at the School's/Trust's discretion.

| | |
|---|---|
| I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, or when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information). | Yes / No |
| I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, suspensions and in the event of illegal activities involvement of the police. | Yes / No |

**I have read and understood the above information.**

| | |
|---|---|
| Pupil Name: | Pupil/Parent Signature: |
| Date: | |

## 14. Monitoring & Review

This policy will be reviewed annually and is up for review in August 2026