Acceptable Use of IT Policy - Employees

Prepared By:	Director of IT		
Approved By:	DCEO	Date:	
Start Date:	September 2024	Review Date:	August 2025

1. Introduction 3
2. Scope and Responsibilities 3
3. Terms of Use 3
4. School Specific Systems 7
5. Passwords 9
6. Software 9
7. Network Access and Data Security 9
8. Unacceptable Use 10
9. Incident Reporting 10
10. Breaches of Policy 11
11. Compliance 11
12. Associated Policies/Guidance 11

1. Introduction

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. Users should have an entitlement to safe access at all times.

This Acceptable Use Policy is intended to ensure:

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

Hamwic Education Trust (HET) will try to ensure that everyone has access to digital technologies to enhance their learning and will, in return, expect them to agree to be responsible employees. This policy aims to ensure a safe, secure, and productive IT environment for all employees, promoting responsible digital citizenship.

2. Scope and Responsibilities

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 employees 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.
- For the purpose of this policy 'employees' refers to staff, governors and work experience individuals.

3. Terms of Use

Staff 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.

- **Work Use**:
  - You may be supplied with Hamwic equipment to utilise at home and outside of your usual workplace setting. This includes laptop, tablets, mobile phones and mobile storage devices.
  - Such equipment must be treated and used in the same way as it would be in the workplace. You are expected to abide by this policy when using all such Hamwic equipment. This means that you remain liable for the use of the equipment and the passwords for it.
  - On request you must make portable and mobile IT equipment available for anti-virus updates and software installations, patches or upgrades. The installation of any applications or software packages must be authorised by Hamwic, fully licensed and only carried out by Hamwic IT employees. You must not make copies of any Hamwic software for use outside the organisation or outside the rules prescribed by the particular software's license.
  - Data must be saved to the Hamwic network. Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable devices. If it is absolutely necessary to do so then this should be for as short a period as possible and the local drive must be encrypted.

- You are responsible for ensuring that all equipment is stored and kept safely and securely. Any protective equipment must be utilised properly.
- On termination of employment, resignation or transfer, you must return all IT equipment to your Line Manager. You must also provide details of all of your system logons so that they can be disabled.
- In normal circumstances you should not be using personal equipment for work purposes. Without prejudice to Hamwic's position, in the event that personal equipment is used for work purposes, personal data should not be saved to the local device and when disposing of any such personal device, you are expected to allow Hamwic IT employees to ensure the hard drive is clear of any work files.
- IT equipment must never be left unattended in an area accessed by the public and/or when travelling. When travelling by car, if you have to leave the car unattended then IT equipment should be kept locked in the boot and out of sight where it is not possible for you to take the equipment with you.

- **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 employees.
- **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/HET, 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. However, we do permit the use of the devices at home but you need to ensure that you:
  - Understand that you are personally accountable for what you do on the devices
  - Understand that HET allow personal use of its IT resources in an employee's own time when not on official duty or 'flexed on' as per the Flexible Working Policy.
  - Ensure that any personal information stored is appropriate i.e. legal, applicable and compliant with this policy and GDPR legal requirements. In any event you may not browse, download, upload or distribute any material that could be considered discriminatory, abusive, pornographic, obscene, illegal, offensive, potentially libellous or defamatory.
  - Understand that the ability to store personal information on owned devices and systems is a privilege and Hamwic has a right to require the data is removed should this data interfere with business activity or use.
  - Personal use of social media, personal websites, blogs, etc. should make no reference to Hamwic or its schools, its students, or colleagues, regardless of whether these sites are accessed while at work or not. Any derogatory comment which expressly or impliedly criticises Hamwic, its schools, it's employees, pupils or a relevant third party may be cause for disciplinary action (in addition to any claim for defamation)
- **Own devices:** If allowed to use your own devices in school, you agree to follow the rules set out in this agreement, in the same way as if you were using school equipment.
- **Concerns**: If you have any concerns about the validity of an email (due to the risk of the attachment containing viruses or other harmful programmes), 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 the IT support team immediately so that they can check if it can be recovered.
- **Artificial Intelligence (AI)**: HET does not intend to prohibit the use of AI for employees, however, there are protocols that would need to be followed when using AI. Please refer to the AI Guidance and ensure that you follow this guidance for the use of AI.
- **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.

- **Protect the Confidentiality** of individuals and of school matters, including complying with the HET 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 IT equipment in accordance with Waste Electrical and Electronic Equipment (WEEE) directive e 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 • 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 employees 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
• Staff to notify any change in circumstances, e.g. address/bank details, annually	• Do not open any hyperlinks in emails or any attachments to emails, unless from a trusted person/organisation who sent the email
• 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 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

4. School Specific Systems

School IT Resources

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

- Classroom Equipment: Desktop/Laptops, Interactive Screens/Boards, Speakers, Docking Stations, Tablet, etc
- Laptops for employees
- Curriculum Delivery devices (student use devices e.g. laptops, tablets, etc.)
- IT Suites

All these resources must 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 or HET, 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/HET network
- Not engage in mass transmission of unsolicited emails (SPAM)
- Not alter the content of a third party's message when forwarding it unless authorised to do so
- Not try to assume the identity of another user or create or send material designed to mislead people about who originated or authorised it (e.g. through misuse of scanned signatures)
- Be vigilant to scam targeting communications especially phishing emails and know how to spot and report suspicious emails

General Email Guidance

- Email is an extremely efficient means of communication but always ask yourself whether a quick internal telephone call or in person communication would be more effective than sending an email message.
- 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/HET provided email systems to send and receive School/HET 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.
- Where an employee is absent or has left employment, the employee's line manager may authorise access to a school email account to obtain messages that are work related. The line manager will inform the employee if this access on their return where they are absent.

Copyright

You may be in violation of copyright laws if you simply cut and paste material from one source to another. Most sites contain a copyright notice detailing how material may be used. If you are in any doubt about downloading and using material for official purposes, you should seek advice from the School Data Compliance Office or Trust's Data Protection Officer.

Remote Working/Access

We recognise that working offsite, or remote or mobile working, is required in many roles and situations in the school/HET, but this brings with it a number of potential risks, to data protection, confidentiality and privacy.

The school/HET offers remote access to staff members, and appropriate use of this technology is important.

The remote access system will enable employees to access their documents and some school programs from anywhere they have internet access. Users 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 being taken offsite should have appropriate security such as passwords on laptops and other devices. These devices should be backed up to the server as soon as possible. Any photographs should be downloaded from all devices as soon as possible and then erased.
- Devices and documents must be kept secure when offsite, not left unattended, not left in cars overnight, and special care should be taken when in public or travelling on public transport.
- Devices and documents should not be left onsite in cars, i.e. should be stored in the boot rather than on the passenger seats
- Data should never be sent to a personal email address, all electronic data must be worked on through the school's network
- Hard copy documents should not be kept with devices which are more likely to be targeted by thieves, to reduce the risk of theft.
- Use of Memory Sticks is NOT permitted

When working offsite:

- Ensure your screen cannot be viewed by any non-staff, including friends, family, visitors or any members of the public. Take special care if you are working in a public place.
- Ensure phone calls cannot be overheard by any non-staff, including friends, family, visitors or any members of the public

- Access school data on personal devices only for exceptional circumstances and if absolutely necessary, and please ensure this has been agreed with the line manager.

All issued laptops 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 employees. Staff are provided with a code that they must keep private and use it to release the print jobs. You must use the printers sparingly and for school purposes only.

Facilities are provided in as unrestricted a manner as possible to offer the best possible quality of service. It is the user's responsibility to ensure that they comply with the policy.

5. Passwords

Access to applications and information is controlled to protect you and our organisation. It is important that the passwords you use are strong and safe enough to keep our data secure.

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.
- Don't put punctuation marks or other symbols at the beginning or end of words.

6. Software

- Employees 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/HET.

7. Network Access and Data Security

- Employees must only access information held on the School's/HET'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 Data Compliance Office and/or Data Protection Officer as a data breach.
- Staff 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.
- Encryption: Sensitive or confidential information should be accessed via the network and should not be permanently stored on laptops or other portable devices e.g. memory sticks. Where the use of a memory stick to transfer or store data temporarily is unavoidable, this must be done using an encrypted memory stick provided by the school.

8. 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/HET may define other areas of unacceptable use.

9. Incident Reporting

- You should report any actual security breaches or attempted security breach, loss of equipment or data, to HET using the incidents system (https://incidents.hamwic.org)
- Concerns regarding virus, phishing emails, unsolicited emails, any unauthorised use or suspected misuse of IT or any of matter of concern, should be reported to your manager and to relevant IT members, as a matter of urgency.

10. 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 employees

11. Compliance

- If for any reason employees are unable to comply with this policy or require use of technology which is outside its scope, this should be discussed with their line manager in the first instance who can provide advice on escalation/exception routes.
- All requests to use new software not currently approved by Hamwic must be subject to the Software Approvals process though the Hamwic IT Team.
- Hamwic actively monitors employee and contractor personal use of IT and equipment to ensure everyone is complying with this policy (AUP) and the Social Media Policy. Monitoring complies with and respects the privacy rights of all employees as outlined in the Privacy Notice. The consequences of failing to comply with the personal use limitations of Hamwic IT and equipment are serious and attract disciplinary penalties up to and including dismissal.
- HET's Central IT Team will regularly assess for compliance with this policy and may need to inspect physical locations, technology systems, design and processes and speak to people to facilitate this. All employees, agents, contractors, consultants, business partners and service providers will be required to facilitate, support, and when necessary participate in any such inspection.
- Failure to report a security incident, potential or otherwise, could result in disciplinary action
- Breaching this policy may result in disciplinary procedures which could lead to dismissal, including criminal prosecution

12. Associated Policies/Guidance

- Data Protection Policy
- Equipment Loan Agreement
- Social Media Policy
- Biometric Data Policy
- Online Safety Policy
- AI Guidance

All employees must sign and return this policy where it will be kept on their personnel 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 HET 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 IT technologies (e.g. iPads, laptops, email, school/HET data etc.) out of school, and to the transfer of personal data (digital or paper based) inside or outside of the schools or HET.
- 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 HET.
- 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/HET's discretion.
- I understand that the school/HET 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).
- I understand that if I fail to comply with this Acceptable Use of IT 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.

I have read, understood and accept the above information.

Staff Name:	Employee Signature:
Date:	