Acceptable Use of IT Policy - Employees

Reviewed on	Sept 2026	Review frequency	Annually
Next review due	Aug 2027	Template Yes / No	Yes
Owner	Director of IT	Approved by	Executive

1. History of Policy Changes

Date	Page	Change	Origin of Change
11/08/2026	3	Introduction: added statement on digital accessibility	
11/08/2026	4	Definitions section removed	
11/08/2026	6	Monitoring: added line defining digital services and use of the monitoring for disciplinary	
11/08/2026	8	Filtering Content: New section added on filtering & monitoring	
11/08/2026	8	Email: added line on not using work email for personal use	
11/08/2026	8	Email: added lines on meeting data protection requirements, and that data can be disclosed for FOI and SAR requests	
11/08/2026	11	Passwords: added line on using password manager, and need for multi-factor authentication	
11/08/2026	11	Software: added line on approval for any new software to be followed through DCO and IT team	
11/08/2026	12	Back Procedures: added a section on backups	
11/08/2026	13	Breach of Policy changed to be handled under the HET/school disciplinary procedures	

2. Contents

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. 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.

HET will try to ensure that everyone has access to digital technologies to enhance their teaching & 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.

In line with the Department for Education's *Digital Accessibility* standards, the school has due regard to ensuring that digital systems, content, and services are accessible and usable for all members of the school community regardless of individual needs or circumstances

4. Scope

This policy applies to all use of IT hardware, software, devices, networks, communications and AI 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 purposes of this policy, "users" means all employees, agency workers, contractors, consultants, trustees, governors, volunteers, trainees and individuals undertaking work experience who are authorised to access HET information, systems, networks or devices.

5. Terms of Use

Employees 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 HET 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 HET 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. Where these are automated, you must ensure that you are restarting your computer every 2 or 3 days to ensure security updates and patched are installed.
- The installation of any applications or software packages must be authorised by Hamwic, fully licensed and only carried out by HET IT employees. You must not make copies of any HET software for use outside the organisation or outside the rules prescribed by the software's license.
- Data must be saved to the HET/school 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 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.

- In normal circumstances you should not be using personal equipment for work purposes. Without prejudice to HET'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 HET IT employees to ensure the hard drive is clear of any 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 must 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.
- On termination, resignation, transfer or change of role, all HET/School equipment must be returned in accordance with the leaver process. Users must provide details of any HET/School systems, shared resources or official accounts for which they are responsible but must not disclose their passwords.

Personal Use

HET information technology and communication systems are provided primarily for authorised HET and school business. Limited and reasonable personal use may be permitted in an employee's own time, provided that it:

- does not interfere with work responsibilities;
- does not incur material cost;
- does not compromise safeguarding, security or data protection;
- does not contravene this or any other HET policy; and
- is not used for commercial, political campaigning or unlawful purposes.

Users should not use their HET email address to register for personal shopping, financial, social media or subscription services.

You also need to ensure that you:

- Understand that you are personally accountable for what you do on the devices.
- Ensure that any personal information stored is appropriate i.e. legal, applicable and compliant with this policy and data protection laws. 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 HET 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 HET or its schools, its pupils, or colleagues, regardless of whether these sites are accessed while at work or not. Any derogatory comment which expressly or impliedly criticises HET, its schools, it's employees, pupils or a relevant third party may be cause for disciplinary action (in addition to any claim for defamation).
- You understand that the device will still be filtered and monitored even when outside of the HET/school network.

Other Terms

- **Responsibility**: HET 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**: HET will monitor use of the systems, devices and digital communications.
- **Vandalism**: Please report any cases of vandalism to the HET IT support team, and appropriate action will be taken by the school/HET to recover any costs for loss or damage.

- **Concerns**: If you have any concerns about the IT, data or content such as 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.
- **Protect 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 Employees & 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 HET/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.
  Digital services including the internet and associated internet-enabled technologies including emails, video calls, video messaging, instant messaging, webinar applications or conferencing applications and email use. Auditing and monitoring of the use IT services may form part of disciplinary procedures.
  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:** HET will dispose of or reuse IT equipment through approved processes in accordance with applicable environmental, information security, data protection and asset-management requirements. Storage media must be securely erased or physically destroyed using an approved method before disposal, resale, reuse or return to a supplier. Disposal and data-erasure records will be maintained where required.

6. Use of Personal Devices to Access Work Data

You must seek authorisation from HET/School leaders before being able to use your own devices. If allowed to use your own devices in HET/School, you agree to follow the rules set out in this agreement, in the same way as if you were using HET/School equipment.
Employees may use personal devices (e.g., smartphones, tablets, laptops) to access work-related data, provided they follow these guidelines:

a. **Data Protection**:
   - Ensure that all work-related data accessed or stored on personal devices is protected by strong passwords and, where possible, encryption.
   - Regularly update device software to protect against security vulnerabilities.
   - Do not download any documents or data from HET/School storage areas onto your personal devices. This includes OneDrive, SharePoint and email attachments as well. This will make the data accessible to third party apps as laid out below.

b. **Third-Party Apps**:
   - Avoid downloading or using third-party applications that may access or store HET/School-related data.
   - Be cautious of granting permissions to third-party apps that could compromise the security of HET/School data.
   - Ensure that third party apps such as Tik-Tok do not have access to downloaded material on your personal devices.

c. **Security**:
   - Install and maintain up-to-date antivirus and anti-malware software on personal devices.
   - Report any lost or stolen devices immediately to the IT department to mitigate potential data breaches.

d. **Duty of Care**:
   - Handle all work-related data with the same level of care and confidentiality as if using HET/School provided devices.
   - Ensure that personal devices are used in a manner that does not compromise the security or integrity of HET/School data.

By following these guidelines, employees can help ensure the security and confidentiality of work-related data when using personal devices.

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	• 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
• Employees 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 HET/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 where there is no authorised need for it

	• 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. Specific Systems

HET/School will provide various IT resources, including but not limited to:

- Classroom Equipment: Desktop/Laptops, Interactive Screens/Boards, Speakers, Docking Stations, Tablet, etc
- Laptops for employees
- Curriculum Delivery devices (pupil 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.

Filtering & Monitoring Content

HET have filtering & monitoring systems in place to block harmful and inappropriate online content, in line with statutory safeguarding requirements. While filtering systems reduce risk, they cannot guarantee that all inappropriate content will be blocked.

Any access to inappropriate content, whether accidental or otherwise, must be reported immediately to the DSL for assessment and action.

Users must not attempt to bypass, disable, or undermine filtering, monitoring, proxy, or security controls under any circumstances.

HET uses technical monitoring systems that may record relevant user, device, application and network activity, subject to the technical capabilities of the systems in use. This includes monitoring on the HET/School network, within Google or MS 365 environments (including Teams or chat), email, internet usage.

Monitoring is conducted for cybersecurity, business continuity, and legal compliance per KCSiE, DfE filtering and monitoring requirements, and relevant cybersecurity standards. Only authorised employees can access monitoring data, which is kept according to the organisation's retention policy and not used for routine performance evaluations.

These monitoring systems alert the correct personnel within the HET/School to any unusual or potentially inappropriate actions—like safeguarding issues or cybersecurity incidents. Any concerning activity is investigated, documented, and, if needed, referred to the Headteacher, Digital Lead, or IT support as part of safeguarding or security processes.

Where changes to filtering or monitoring settings are required for legitimate educational or operational reasons, the user must request the change by contacting the HET/School IT support team, so that the rationale can be documented in accordance with the DfE Filtering and Monitoring Standards referenced in KCSiE. Such changes must be approved in advance by the Headteacher and/or the DSL.

Filtering and monitoring arrangements form a core part of the HET/School's safeguarding responsibilities under KCSiE, the Prevent Duty (as set out in the Counter Terrorism and Security Act 2015), and the DfE Digital and Technology Standards for Schools and Colleges.

Email

You will be provided with an email address by HET/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 HET/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. Where possible, users should share links to files held in approved HET/School systems rather than sending duplicate attachments. Large or sensitive files must be shared using HET approved secure file sharing methods.
- 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 HET/School 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

- You must only use HET/School provided email systems to send and receive HET/School information.
- Users are not permitted to use the email system for personal communication
- Any personal information sent via email, the Internet and associated internet-enabled services is covered by Data Protection legislation. All employees are required to handle personal information in accordance with the HET Data Protection Policy.
- Emails, messages, files, recordings and other information created, sent, received or held through HET/School systems are organisational records. They may be retained, accessed, searched or disclosed where required for safeguarding, audit, complaint investigation, legal proceedings, Freedom of Information requests, Subject Access Requests or other lawful purposes, subject to applicable exemptions and the rights of other individuals.
- Employees will always exercise the same caution on email content, video calls, instant messaging or conferencing applications as in more formal correspondence.
- 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.
- 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.

- Where an employee is absent or has left employment, the employee's line manager may authorise access to a HET/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 HET Compliance team (compliance@hamwic.org).

Biometric Data

HET/School uses biometric data for access into systems such as devices compliant with Microsoft Windows Hello (facial recognition), and catering systems (fingerprint scanners).

Where HET uses biometric recognition systems, the collection and use of biometric information will be managed in accordance with the HET Protection of Biometric Information Policy. Users must not introduce, enable or use biometric identification systems for HET purposes without prior approval.

Please refer to the Protection of Biometric Data Policy for further detail and information.

Remote Working/Access

It is recognised that working offsite, or remote or mobile working, is required in many roles and situations in the HET/School, but this brings with it several potential risks, to data protection, confidentiality and privacy.

The HET/School offers remote access to employees, and appropriate use of this technology is important.
The remote access system will enable employees to access their documents and some HET/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. HET/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. 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.
- Data should never be sent to a personal email address; all electronic data must be worked on through the HET/School's systems.
- 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 HET/School data on personal devices only for exceptional circumstances and if 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 HET/School premises.
Any breach or misuse of this technology will lead to disciplinary procedures.

Printers and Consumables

Printers are provided across HET/School for use by employees. Employees 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 HET/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 may be subject to disciplinary procedures.

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.

8. Artificial Intelligence (AI)

HET supports the responsible use of approved artificial intelligence tools. Users must follow the HET AI Guidance and must not enter personal, special category, confidential, commercially sensitive or safeguarding information into an AI service unless that service and use have been expressly approved.

Users remain responsible for checking the accuracy, appropriateness, bias, copyright implications and accessibility of AI-generated outputs. AI-generated content must not be treated as automatically accurate or used as the sole basis for significant decisions about pupils, employees or other individuals.

9. Passwords

Users receive individual accounts with the least privilege needed for their role. Passwords should follow best practices: they must comply with policy, be strong, not written down or shared, avoid personal information, and be changed if compromised. Accounts and credentials must never be used by others.

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.

Passwords must be long, unique and difficult to guess. Where a password is created by the user, HET recommends the use of three random words or a password generated by an approved password manager.
Passwords must not:

- be reused between work and personal accounts;
- contain easily identifiable personal information;
- be shared with another person;
- be entered following an unexpected request; or
- be stored in an unapproved location.

Users must use the HET-approved password manager where one is provided. A password must be changed immediately if compromise is known or suspected.
Multifactor authentication must be used wherever required by HET or supported by the relevant service. Users must never approve an unexpected authentication request.

Microsoft Edge Password manager is recommended for secure password management.

Multi-factor authentication (MFA) will also be required for access outside of the HET network.

10. Software

- Devices have a predetermined list of software installed, where a need for additional software is identified it must be requested through the school DCO for appropriate data protection checks, and then through the HET IT support team to ensure that the appropriate installation process has been followed.
- Software and web-based accounts that use personal data may be subject to a Data Protection Impact Assessment (DPIA) and so will not be installed or set up until this has been carried out.
- 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 HET/School.

11. **Network Access and Data Security**

- Employees must only access information held on the HET/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 HET/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 HET compliance team as a data breach using the online incident system.
- Employees 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 HET/School.

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 HET/School into disrepute or exposes it to legal action.

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

13. Backup Procedures

Information stored in approved HET locations will be protected in accordance with HET backup, retention and business continuity arrangements. Users must save work only in approved locations and must not assume that information held locally, on removable media or within an unapproved service is backed up.

If software/hardware problems arise, a device may need to be restored to its original settings. Work files may be lost during the restore process, therefore it is the responsibility of all users to ensure that files are saved to the appropriate cloud-based work areas.

Encrypted removable media is not an approved permanent storage or backup location. Information temporarily stored on approved removable media must be transferred to an approved HET storage location as soon as possible and securely removed from the media when no longer required.

14. 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.

15. Breach of Policy

Usage of HET/School systems is subject to agreement to abide by this policy, and any breach of the conditions will be dealt with under the HET/School disciplinary procedures

16. 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 HET must be subject to the Software Approvals process though the HET 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 HET 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

17. Link to other HET policies & legislation

- AI Guidance
- Protection of Biometric Data Policy
- BYOD Policy
- Data Protection Policy
- Equipment Loan Agreement
- Online Safety Policy
- Social Media Policy
- Keeping Children Safe in Education

18. Appendices

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

- I understand and accept that HET/School may monitor and record the use of its devices, networks, accounts and digital services for safeguarding, cyber security, system administration, audit, legal compliance and the investigation of suspected misconduct.
- I understand that if my activity causes any concerns, safeguarding software installed across HET/School 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, HET/School data etc.) out of HET/School, and to the transfer of personal data (digital or paper based) inside or outside of HET/School.
- I understand that HET/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, an employee or appropriate safeguarding lead.
- I understand that if I leave HET/School, all my digital accounts will be suspended, and my data deleted at HET/School's discretion.
- I understand that the HET/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 HET/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 HET/School network/internet, suspensions and in the event of illegal activities involvement of the police.

I have read, understood and accept the above information.

Employees Name:	Employee Signature:
Date:	