



Acceptable Use of IT Policy - Pupils

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

2. Contents

1. History of Policy Changes.....	2
2. Contents.....	2
3. Introduction	3
4. Scope.....	4
5. Principles.....	4
6. Pupil responsibilities	4
6.1 Accounts and passwords.....	4
6.2 Respectful communication and conduct.....	4
6.4 Devices, Software and Networks	5
6.5 Copyright and academic integrity	5
7. Artificial Intelligence (AI).....	5
8. Mobile phones and personal smart devices	5
9. Filtering, Monitoring and Privacy.....	5
10. School responsibilities.....	6
11. Parent and Carer Responsibilities	6
12. Unacceptable Use	6
13. Breaches of Policy	6
14. Linked HET policies and guidance	7



Sam's Entitlement

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."

This Acceptable Use of IT Policy is intended to ensure:

- That pupils 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.

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 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 school leaders are responsible for supervising and supporting their team to read, understand and comply with this procedure if they have access to IT.

5. Principles

- Technology should enhance learning, inclusion, creativity and communication.
- Safeguarding and the welfare of pupils take priority.
- Access should follow the principle of least privilege and be appropriate to age, role and educational need.
- Pupils should be taught to manage risk, seek help and behave responsibly online.
- Filtering and monitoring reduce risk but do not replace education, supervision and professional judgement.
- Responses to misuse should be fair, proportionate and consistent with safeguarding and behaviour procedures.

6. Pupil responsibilities

6.1 Accounts and passwords

- Pupils must use only the account issued or authorised for them.
- Passwords and authentication methods must not be shared.
- Pupils must not attempt to use another person's account or access information beyond their permission.
- Pupils must lock or sign out of devices when instructed or when leaving them unattended.
- Suspected account compromise must be reported promptly.

6.2 Respectful communication and conduct

- Pupils must communicate respectfully and must not bully, threaten, harass, discriminate against, impersonate or deliberately embarrass another person.
- Pupils must not create or share content that is illegal, harmful, hateful, abusive or unsuitable.
- Pupils must not use school systems to organise harmful behaviour or encourage others to breach school rules.
- Safeguarding concerns, harmful contact or requests for personal information must be reported to a trusted member of staff.

6.3 Privacy, data and images

- Pupils must protect their own and others' personal information.



- Photographs, video, audio and screen recordings may only be created or shared where permission has been given and the activity is authorised.
- School information must be stored and shared only through approved services.
- Personal, confidential, safeguarding or assessment information must not be uploaded to unapproved websites, social media, AI tools or file-sharing services.

6.4 Devices, Software and Networks

- Pupils must handle equipment carefully and report faults, loss or damage.
- Software, apps, browser extensions and devices may only be installed, connected or configured with authorisation.
- Pupils must not damage, disrupt, scan, test or interfere with systems, security controls, networks or data.
- VPNs, proxies, anonymising tools and other methods must not be used to bypass filtering, monitoring or access restrictions.
- Suspicious messages, links, files, pop-ups or authentication requests must be reported and not investigated by the pupil.

6.5 Copyright and academic integrity

- Pupils must respect copyright, licences and the work of others.
- Sources must be acknowledged as required by the school.
- Pupils must not present copied or AI-generated work as entirely their own where this is contrary to teacher instructions or assessment rules.

7. Artificial Intelligence (AI)

Pupils may use AI only where the tool and activity have been approved by HET/school and their teacher. Pupils remain responsible for checking accuracy, suitability, bias and sources. They must not enter personal, special category, confidential, safeguarding or assessment information into an AI service unless expressly authorised.

AI must not be used to avoid learning, misrepresent authorship, create harmful content, impersonate others, facilitate bullying, bypass assessment rules or make significant decisions about another person.

8. Mobile phones and personal smart devices

HET schools will operate as mobile phone-free environments by default throughout the school day, subject to the school's published arrangements and proportionate authorised exceptions. This includes phones and other personal smart technology with similar communication or recording functions. Pupils must follow local rules for bringing, storing and using devices.

9. Filtering, Monitoring and Privacy

HET/School applies filtering to reduce access to illegal, harmful and inappropriate content. Filtering cannot guarantee that every risk will be blocked. Pupils must not attempt to disable or circumvent filtering, monitoring, proxy, device-management or security controls.

HET will monitor and record relevant activity on its devices, networks, accounts and digital services for safeguarding, cyber security, system administration, audit, legal compliance and investigation of suspected misuse. Monitoring may include internet activity, email, messaging, files, applications, device events and alerts generated by safeguarding or security systems.



Monitoring information will be available only to authorised personnel and handled in accordance with HET privacy information, retention arrangements and applicable law. Automated alerts will be assessed by an authorised person before significant action is taken.

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

10. School responsibilities

- Provide age-appropriate online safety education and clear expectations.
- Maintain appropriate filtering and monitoring arrangements.
- Provide secure accounts, devices and approved digital services.
- Make reasonable adjustments and provide accessible information.
- Respond to safeguarding and security concerns promptly.
- Communicate material expectations to pupils and parents or carers.
- Review arrangements and risks regularly.
- Apply behaviour and safeguarding procedures fairly and consistently.

11. Parent and Carer Responsibilities

- read and discuss the age-appropriate agreement with their child.
- support the school's expectations for safe and respectful use.
- encourage their child to report concerns without fear of losing access solely because they asked for help.
- inform the school of relevant accessibility, medical or safeguarding needs.
- follow school arrangements for mobile phones and personal devices.
- report concerns about an HET account, device or service promptly.
- understand that school systems are filtered and may be monitored for the purposes described in this policy.

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 HET/School may define other areas of unacceptable use.

13. Breaches of Policy

Possible breaches will be considered according to the pupil's age, understanding, intent, impact, any additional needs, safeguarding context and previous incidents. The school may provide education and support, contact parents or carers, restrict or remove access, apply behaviour sanctions, recover costs where lawful and appropriate, or refer matters to external agencies where required.

All incidents will be dealt with according to the school behaviour policies.



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 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
	Do not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
	Do not use any programmes or software that might bypass the filtering/security systems in place to prevent access to inappropriate content
	Do not open any hyperlinks in emails or any attachments to emails, unless from a trusted person/organisation who sent the email
	Do not forward emails to home computers or personal email addresses

14. Linked HET policies and guidance

- AI Guidance
- Behaviour Policy
- Data Protection Policy
- Filtering and Monitoring procedures
- Mobile Phone Policy
- Online Safety Policy
- Safeguarding and Child Protection Policy
- Social Media Policy

This policy will be reviewed annually by Southampton Hospital School.