HAREFIELD

ICT Policy

• Acceptable use of ICT
• Data Security
• E-safety

Policy reviewed and updated	May 2025
Date of next review	May 2026
This policy will be subject to ongoing review and may be amended prior to the scheduled date of the next review in order to reflect changes in legislation where appropriate	

Contents

Role	**Name**
IT Manager	Mr Jared Martin
Headteacher	Salma Riley
Data Lead	Helen Howley

1. Introduction

Harefield School seeks to promote and facilitate the proper and extensive use of Information and Communications Technology (ICT) in the interests of learning, teaching and research, including business and community engagement partnerships. This requires responsible and legal use of the technologies and facilities made available to students, staff and partners of the school.

The Acceptable Use Policy applies to all computing, telecommunication, and networking facilities provided at the school and should be interpreted such that it has the widest application. ICT services should, where appropriate, be taken to include departmental or other system managers responsible for the provision of an ICT service. This policy should be interpreted so as to encompass new and developing technologies and uses, which may not be explicitly referred to.

Harefield School ICT resources are provided to facilitate the essential work of employees or students and to help enhance the wider experience of students attending the school. Use of ICT Services should not interfere with duties or studies, nor should their use bring the school into disrepute.

Commercial work for outside bodies, using centrally managed services, requires explicit permission from the IT Manager; such use, whether or not authorised, may be liable to charge.

2. Authorisation

Registration is required to use the ICT facilities at Harefield School. Such registration is conditional upon acceptance of and adherence to this policy which must be signed by all employees and students.

The registration procedure grants authorisation to use the core ICT facilities of the school. Following registration, a username, password and e-mail address will be allocated.

Individually allocated usernames, passwords, laptops, iPads and e-mail addresses are for the exclusive use of the individual to whom they are provided. The user is personally responsible and accountable for all activities carried out under their username. The password associated with a particular personal username must not be divulged to any other person. No one may use or attempt to use ICT resources allocated to another person, except when explicitly authorised by the provider of those resources.

All users must correctly identify themselves at all times. A user must not masquerade as another, withhold their identity or tamper with audit trails. A user must take all reasonable precautions to protect their resources. Passwords will only be accepted if they:

- Are at least 6 characters in length
- Contain at least three of the following four-character groups: an uppercase letter (A-Z), a lowercase letter (a-z), a number, (0-9,) a non-alphanumeric character (e.g.! $, #, %).

Additionally, passwords are forced to be changed every 3 months for additional security. This is automated and will prompt the user near the time when a change is due. Reset passwords can only be issued in person, over the phone or via email from ICT Services.

3. Data Security

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. The Data Protection Act (1998) governs the storage and transfer of data and any breach can result in prosecution.

This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the IT Manager. By logging on to ICT systems, users agree to abide by this acceptable use policy.

It is important that staff are aware that within the terms of the Data Protection Act and the Telecommunications Regulations 2000, (Interception of Communications), the school may record or inspect any information transmitted through or stored in its computers, including e-mail communications and individual login sessions, without notice when:

- There is reasonable cause to believe the user has violated or is violating this policy, any guidelines or procedures established to implement this policy.
- An account appears to be engaged in unusual or unusually excessive activity.
- It is necessary to do so to protect the integrity, security or functionality of ICT resources or to protect the school or its partners from liability.
- Establishing the existence of facts relevant to the business.
- Ascertaining or demonstrating standards which ought to be achieved by those using the ICT facilities.
- Preventing or detecting crime.
- Investigating or detecting unauthorised use of ICT facilities.
- Ensuring effective operation of ICT facilities.
- Determining if communications are relevant to the business (for example in the last resort where an employee is off sick or on holiday and business continuity is threatened.)

This policy also assumes a common interpretation and application of associated guidance contained within the following:

- General Data Protection Regulation, 2018
- Copyright, Designs and Patents Act 1988
- Malicious Communications Act 1988
- Computer Misuse Act 1990
- Obscene Publications Act 1959
- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Freedom of Information Act 2000
- Communications Act 2003

4. General ICT Use

- Users should not allow any student or family members to use their Harefield login, PC, ID badge, iPad or laptop, these are for staff use only.
- When leaving a classroom, it is required that users log off and turn off their SMART board. If a computer is unattended for even a short period of time, it should be locked by using CTRL+ALT+DEL and selecting LOCK. Alternatively pressing down the WINDOWS key and pressing L will lock the screen.
- Users must take care to store sensitive information, e.g. student data, safely and to keep it password protected, on all school systems and devices.
- Any problems with ICT should be reported to ICT either by e-mail to or by phoning the ICT office.
- Use of portable storage devices is prohibited within the school and access is routinely prevented.
- All Staff have access to change student passwords using the tool provided in the start menu called Password Control. Students should never be allowed to use this software.
- Staff are allocated 6GB of local storage space for use. When this limit is reached it will not be possible to save further data without freeing up storage space.
- Students are allocated 3GB of local storage space for use. When this limit is reached it will not be possible to save further data without freeing up storage space.
- Staff and students can also store files and documents in Google Drive.
- Where additional storage is required for educational purposes, this would need to be approved by the IT Manager.

5. Staff Laptops/iPads

- The device always remains the property of Harefield School and is only for the use of the member of staff it is issued to. It must be returned to the school on request.
- Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the device screen.
- Devices should not be dropped, exposed to extreme heat or cold, stored in vehicles or have heavy items place upon them.
- Insurance covers theft and but excludes loss and theft from an unattended car. ***Repairs or replacements not covered by the insurance policy will be deducted from the relevant departmental budget.***
- When transporting the device, it is important that the device is not left attached to the charging cable as this can lead to damage of the device's charging port.
- The device is for educational purposes only. Any software being added needs to be first checked with the IT Manager before attempting to install it.
- Should any faults occur, IT must be advised as soon as possible. Under no circumstances should staff attempt to fix suspected hardware faults.
- All files/folders are automatically backed up every night, including home drives, staff shared area and student shared area. Google drive data is also backed up every evening.
- No files should be held locally on the device (files should only be stored within the school's network area accessible remotely or in Google Drive.)
- The device must be kept secure and logged off when not in use.

- Laptops should be brought into school and connected to the network at least every 6 weeks to keep antivirus software, Bromcom updated and receive Windows updates.

6. Projectors and Interactive Whiteboards (IWB)

- Projectors should only be turned on/off using the software provided on the desktop.
- The freeze button should be used to enable teachers to complete registers during lessons. Bromcom/emails/student sensitive information should never be projected onto the whiteboard.
- If the Projector or Whiteboard malfunction this should be reported to IT.
- Only the IWB SMART pen provided should be used to write on the IWB.
- All new SMART 75" MX Boards should be turned off from the power button when not used. Boards are set to automatically turn off after 2 hours of inactivity.

7. E-Mails

- Harefield School e-mail addresses (@hfschool.org.uk) and associated school e-mail systems must be used for all official school business, to facilitate auditability and institutional record keeping.
- The e-mail system is intended for school related communication. It should not be used for personal e-mail and should not be used as a personal e-mail account.
- Access to the school e-mail account will cease when employment ends.
- Mailboxes are stored in Google cloud and backed up via the cloud daily. The school does not routinely monitor the content of emails but we would have to make it available in response to a lawful request from the police or other agency.

The following guidance should be adhered to by all staff:

- Emails should only be sent to those who need to receive them, to eliminate time spent by others sifting through unwanted messages. When using predefined groups, think carefully about whether the majority of staff in that group need to receive the email.
- Double check when sending an email that it is going to the intended recipient only, to avoid risk of breaching confidentiality.
- Think carefully about sending confidential information by email which can be duplicated and circulated to others very easily.
- School email may be used to contact parents or students at the discretion of the member of staff. Staff must not contact students or parents using personal email accounts.
- Keep the size of any attachments to a reasonable value (e.g. avoid large images or audio files). For large files/folders, send a drive file link.
- Staff are required to use the same personal and professional courtesies and considerations in electronic mail as they would in other forms of communication.
- If you receive emails with attachments, do not open the attachments unless you are certain you know who they are from and what they contain.
- Save any attachments you want to keep in your private network folder or Google Drive.

8. Internet

The following content should not be created or accessed on ICT equipment at any time:

- Pornography and “top-shelf” adult content.
- Material that gratuitously displays images of violence, injury or death.
- Material that is likely to lead to the harassment of others.
- Material that promotes intolerance and discrimination on grounds of race, sex, disability, sexual orientation, religion or age.
- Material relating to criminal activity, for example buying and selling of illegal drugs.
- Material relating to any other unlawful activity, e.g. breach of copyright.
- Material that may generate security risks and encourage computer misuse.
- It is possible to access or be directed to unacceptable internet sites by accident. These can be embarrassing, and such sites can be difficult to get out of. If staff have accessed unacceptable content or are in receipt of unacceptable material via email, they should inform the IT Manager and Designated Safeguarding Lead. This may avoid problems later should monitoring systems be alerted to the content.

9. Social Media

- You must not talk about your professional role in any capacity when using personal social media such as Facebook, X, YouTube or any other online publishing websites.
- Social media tools must not be used to communicate with current or former students of school age.
- Your profile on social networking sites should be set to maximum privacy and give access to known friends only.
- If you experience any derogatory or slanderous comments relating to the school, colleagues or your professional status, you should take screenshots for evidence and escalate to the IT Manager and Designated Safeguarding Lead.

10. Cameras/Videos

- Under no circumstances will staff use any personally owned equipment for recording video, sound or images of students.
- Images of students and/or staff should only be taken and/or stored on school cameras and videos and are only used for professional purposes and with consent. Students who do not wish to have their photo taken have watermarked photos on their MIS records.

11. ICT suites

- Staff should be vigilant in any lesson where ICT is used by students and leave careful briefing notes if the lesson is being covered by someone else.
- Each time students log on to a PC they are required to agree to the code of conduct. (Acceptable Use Policy)
- When using any of the IT rooms, staff should adopt the following procedure to ensure the minimum of damage to the equipment. ***Please be aware that ICT equipment damaged in lessons may be charged to faculty budgets where policy has not been adhered to and the following checks have not been completed.***

At the Start of the Lesson

- Through observation of the students, quick check that all of the equipment is working. Report any faults to the IT Manager.
- Use Impero to monitor the students' screens. Training provided if necessary.
- If any student has food or drink with them, it should be contained in their school bag and not be removed in an IT room at any time.

At the End of the Lesson

- Do a quick room check to see if there are any signs of damage.
- Switch the IWB off if the room is no longer being used at the end of the lesson.
- Ensure each student leaves the keyboard, mouse and chair neatly where they belong, and the room is tidy.
- If any faults have occurred during the lesson, report these to the IT Manager.
- Always use the app Projector Control on the PC to turn on/off projectors in classrooms. This is located on the desktop. THE MX boards can be turned off by pushing the power button located on the screen. The theatre projector has a panel on the back wall that can be used to turn the projector on/off.
- Ensure that all printed sheets are collected and not left in the room. Any confidential information printing should be disposed of in the correct way. Shredders are available in the school for use.

12. Equipment Booking Process

- All equipment to be loaned out must be authorised by a member of staff before being collected by a student. This will then be entered into a spreadsheet by the IT manager and the equipment will be issued.
- If the equipment is required for longer than a double period, a charger will also be allocated.
- No one other than the allocated user is to use the equipment.
- Laptop requests from the welfare officer in relation to student injuries will take priority. Laptops allocated for SEND and Exams are assigned at the member of staff's discretion. These are the responsibility of the departments they are assigned to.
- All equipment is to be returned to the IT office by the end of the school day unless booked for a set period of time, in which case the students can store these in their lockers.
- If the IT office is locked, the equipment is to be left with the corresponding student manager for collection. Failing this, the equipment is to be left at reception for collection via the IT manager.
- All equipment is to be returned in good working condition. Any damage such as missing keys, graffiti, cracked screens/broken hinges will result in charges.
- The student allocated the equipment is responsible for the safekeeping of the equipment whilst in their use or possession.

13. Harefield School Wireless Service

This includes the following wireless networks:
Harefield-WiFi, Harefield-Guest, Harefield-Open, THA-Domain-Staff, THA-Domain-Student

Harefield-WiFi – For staff and students that work/learn at the school. To connect to this Wi-Fi the user must have a user account at the school so they can login with their credentials.

Harefield Guest – For guest users that come to the school during the day. To connect the guest user must register with their email address and enter a sponsor email address for authorisation. Members of staff who can approve access are: IT Manager, Headteacher, Finance Manager, Receptionist, Welfare Officer & Data Protection Officer. Once authorised the guest user will be emailed a code which they use to sign into the guest Wi-Fi. Guest users can use the guest network for up to 30 days should they come back on a different day before they will have to register again. The guest Wi-Fi operates and can be connected to between the hours of 08:00-16:00.

Harefield Open – For lettings and guest users outside of school hours and on weekends. Guest users will have to register to connect but this does not require authorisation from a sponsor. The Harefield Open Wi-Fi operates and can be connected to between the hours of 16:00-23:00 Mon-Fri and 08:00-23:00 on weekends.

THA-Domain Staff/Student – For Apple school devices/non-Windows devices. This is setup and configured by the IT manager on specific devices within the school.

When using the school wireless services, you must obey various regulations and acceptable use policies. These broadly fall into the two categories below:

- The Law – Use of the school wireless services is subject to applicable law.
- The policies and regulations of the school. These include:

13.2 Wireless service regulations

1. **Acceptance of responsibility:** A user will be held responsible for any breach of regulations carried out using a connection authenticated with their username. This includes action taken by others.
2. **Identification:** You must not attempt to authenticate yourself using another person's or organisation's credentials.
3. **Network security:** The school reserves the right to conduct scans of the network in order to determine what computers are connected to it and what services they are operating. You may not configure your computer to use any network address other than those allocated to you.
4. **Computer security:** You must ensure that your computer has up-to-date anti-virus software and that all operating system updates and other security updates are installed. You must remove any malware found on your computer.
5. **Service operation:** You must not do anything that interferes with the operation of the wireless service. This includes using an unfair or excessive share of the available network bandwidth.
6. **Copyright:** It is illegal to copy or share movies, music, software and other copyrighted material without permission from the copyright holder. You must not do this, whether intentionally or as a failure to correctly configure a file-sharing program on your computer.
7. **Data protection:** Personal data can only be processed under strictly limited circumstances.

13.2 Penalties

1. **Withdrawal of facilities:** ICT services may withdraw or restrict your access to the wireless service or other ICT services.
2. **Disciplinary action:** Any breach of regulations may be reported to your line manager or head of department. In more serious or repeated minor cases, a breach of school

regulations may be reported to the headteacher to be dealt with under the school disciplinary procedures.

3. **Fines:** ICT services may request that a user be charged for extra work that has arisen as the result of computer misuse.
4. **Police action:** When required to do so, or when the school deems necessary, the school may inform the police.

When a connection to the school network has been made, you are confirming your acceptance of this policy.

- You agree and accept that the wireless service is used at your own risk.
- You agree and accept that your equipment is used at your own risk.
- You agree and accept that no technical support will be provided for personal devices.
- You agree and accept that this wireless service will not be misused. Examples of misuse include but are not limited to:

  - Fraud and theft.
  - System sabotage.
  - Introduction of viruses, trojans, malware, spyware and time bombs.
  - Obtaining unauthorised access to any services.
  - Breaches of Software Licensing Copyright Act, Computer Misuse Act, Data Protection Act.
  - Sending abusive, rude or defamatory messages via email or any other means.
  - Accessing pornographic web sites.
  - Transmission of unsolicited advertising.
  - Hacking or attempted hacking.
  - Disabling or overloading any school computer systems or network, or circumventing any system intended to protect the privacy or security of another user.

All ICT usage is monitored in the school at all times.

14. Harefield School ICT Acceptable Use Agreement for staff.

User Signature

I agree to adhere to the ICT acceptable use policy at all times.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the schools most recent e-safety policies.

I wish to have an email account; be connected to the intranet and internet; be able to use the schools ICT resources and systems.

Signature
…….……Date……..…….....

Full Name
……..…….....
(printed)

Job
title……..……
……

School
……
…

Authorised Signature

I approve this user to be set-up.

Signature
…….Date……..…….....

Full Name
…….…….
(printed)

15. Harefield School ICT Acceptable Use Agreement for students.

- Your password is confidential and **must not** be given to anyone else.
- You **must not** allow anyone else access to the network though your network account.
- You **must not** damage any computer equipment. Students are responsible for the safekeeping of any IT equipment in their use or possession. Any equipment damaged intentionally or accidentally is likely to result in charges. This applies to all equipment used in the school day and any equipment lent to the student for educational use.
- You **must not** undertake any activity that could lead to damage of any software on the network.
- You **must not** disconnect any of the computer equipment.
- You **must not** eat or drink near any of the computer equipment.
- You **must not** copy any software or data onto the network that infringes British Law or may be considered offensive. (This includes any copyrighted music and video files)
- You **must not** copy, delete or modify any files on the network that are not in your user account area.
- You **must only** use the internet for activities that are directly related to your registered school course, you cannot access chat rooms, games or download ring tones, etc.
- You **must not** send any email messages that could be considered to be offensive.
- You will be responsible for all information and data stored in your account area of the network (H:) or Google Drive. (My Drive)
- You accept that all of your files that you store or access on the school network can be remotely and locally viewed by any member of the school staff.

Student User Signature I agree to abide by all the requirements above.

I wish to have an email account; be connected to the Intranet and Internet; be able to use The schools ICT resources and systems.

Signature ……
Date ……

Full Name ……
(Printed)

Tutor group ……

Parent/Carer Signature I approve this user to be set-up and understand that continued use is subject to the conditions above.

Signature ……
Date ……

Full Name ……
(Printed)

16. E-Safety: Code of Practice

What is E-Safety?
Whilst the internet and associated technologies are an excellent tool and resource to enrich learning there are still dangers related to their use, especially in relation to young students. Some examples of this are:

- Bullying via chat or email
- Obsessive internet use
- Exposure to inappropriate materials
- Inappropriate or illegal behaviour
- Physical danger of sexual abuse

Harefield School will endeavour to ensure the E-Safety of all school members. It will use education, technology, accountability, responsibility and legislation as the key ways to achieve this.

Within the school all members of staff and students are responsible for E-Safety. Responsibilities for each group include:

Students

- Participating in and gaining an understanding of E-Safety issues and the safe responses from E-Safety training sessions.
- Compliance with a highly visible student's Acceptable Use Policy (AUP) which students must agree to each time they use school ICT equipment either in the school or remotely.
- Reporting any E-Safety issue to the teacher, team leader or parent/carer.
- Take responsibility for their own actions using the internet and communications technologies.

All Staff

- Have a clear understanding of E-Safety issues and the required actions from E-Safety training sessions.
- Reporting any E-Safety issues to the IT Manager and the Child Protection Officer as soon as the issue is detected.
- Compliance with the school Data Security, E-safety and acceptable use of ICT Policy which staff must agree to each time they use school ICT equipment either in the school or remotely which connects to the internet.

Teaching Staff

- Educating students on E-Safety through specific E-Safety training sessions and re-enforcing this training in the day-to-day use of ICT in the classroom.

IT Manager

- Ensure that the best technological solutions are in place to ensure E-Safety as much as possible whilst still enabling students to use the internet effectively in their learning.
- Ensure that all information captured using these systems is secure, accessible to the appropriate members of staff, and stored in a robust manner. In addition, securing and preserving evidence of any E-Safety breach.

17. How the school ensures E-Safety in the classroom

Educating students in E-Safety
A key objective of the school is to educate students in safe use of ICT and the internet. We feel this is one of the best ways to minimise the potential for any E-Safety issues to occur.

Students will receive specific E-Safety lessons/assemblies aimed at ensuring that:

- Students know the E-Safety risks that exists and how to identify when they are at risk.
- Students know how to mitigate against E-Safety risks by using e-safe practices whilst online.
- Students know when, how and to whom to report instances when their E-Safety may have been compromised.
- Students know that they are in an environment that encourages them to report E-Safety issues without risk of reprimand, humiliation or embarrassment.

In addition to this specific training all members of staff will have a duty to reinforce E-Safety practices wherever possible and will offer students advice and support in the classroom where minor E-Safety incidents have occurred. E-Safety education information will have high visibility in all areas of the school.

How E-Safety is monitored
Harefield School deploys and utilises Smoothwall Monitor across all student devices in the school. Smoothwall Monitor is a real-time digital monitoring solution that offers a 24/7 human moderated service. A highly trained team monitor alerts and notify of risks appropriate to their grade, providing support for the pastoral/safeguarding team and the pupils in the school's care. Teaching staff also have the capability to directly monitor the students ICT and internet use in the classroom.

How technology is used
Harefield School utilises many different technologies to help to ensure E-Safety for students. These include:

- School firewall for internet filtering to block inappropriate content and in addition block websites which are irrelevant to the students' programme of study and considered time wasting.
- Smoothwall Monitor uses text analysis which captures text input via keyboard, whether online or offline, monitoring all activity within sites or applications. Content is reviewed by a team of moderators around the clock to analyse instances and alert safeguarding officers of any high-risk incidents. Smoothwall Monitor builds an up to the minute profile of activity per individual, allowing the risk profile and context of a situation to be accurately analysed.
- Screen capture functionality sits within the solution, allowing any online and offline incidents that require investigation to be screen grabbed for later review or evidence. Alerts are based upon specific categories that are identified as serious incidents and are sent to the designated safeguarding/pastoral team.
- Impero Education Pro is also deployed across all student devices that allows for real time monitoring of the student activity on the computers for staff to use during a lesson.
- Control mechanisms are in place for staff via this software to restrict which activities the students can perform using built in controls to block internet access and lock screens within a lesson.
- Harefield School also restricts student activity on the computers via system group policies and access control.

Examples of unacceptable student behaviours that would infringe E-safety include, but are not limited to:

- Use of websites not directly linked to classwork.
- Unauthorised use of email.
- Accidentally accessing offensive material and not notifying a member of staff of it.
- Deliberately corrupting or destroying someone's data.
- Sending an email that is regarded as harassment or of a bullying nature.
- Deliberately trying to access offensive or pornographic material.
- Any purchasing or ordering of items over the internet.
- Transmission of commercial or advertising material.
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent.
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988.
- Bringing the school's name into disrepute.

Any behaviour which compromises E-safety will be addressed in line with the behaviour policy and sanctioned accordingly.

Working with parents and the community

Many school students will also have access to IT and the internet at home, often without some of the safeguards that are present within the school environment. Therefore, parents must often be extra vigilant about their child's E-Safety at home. One of the goals of the school is to support the parent's role in providing an e-safe environment for their children to work in outside the school.

The school will do this in several ways:

- Provide advice on E-Safety.
- Upon request publish E-Safety information and direct parents to external E-Safety advisories via the school website.