



# HEATHFIELD SCHOOL

## IT Acceptable Use Policy

<b>Policy Area:</b>	General
<b>Relevant Statutory Regulations:</b>	ISSR 2014 Part 3  NMS Part B, Standard 4 and Part D, Standard 8  Data Protection Act 2018  Keeping Children Safe in Education 2023
<b>Key Contact Personnel in School</b>	
<b>Nominated Member of Leadership Staff Responsible for the policy:</b>	Manager of IT Network and Services
<b>Version:</b>	2023.02
<b>Date updated:</b>	13 October 2023
<b>Date of next review:</b>	01 September 2024

*This policy will be reviewed at least annually, and/or following any concerns and/or updates to national and local guidance or procedures.*

### **Purpose and Scope**

---

This policy applies to all members of Heathfield School (the “School”): staff, governors, pupils, peripatetic teachers, parents and visitors who make use of the School’s computer network and services, the School’s remote services, a School device, or a personal device in order to access School resources or the School’s Internet provision.

The aim of the policy is to clarify the acceptable use of IT hardware and services provided by the School, and the provision of IT related support.

### **IT Overview**

---

#### **Network and Internet**

The School provides a network in the form of wired and wireless (WiFi) networking. Access to network resources and the wider Internet requires authentication, either via a pre-shared password, or individual usernames and password before access is given.

It is forbidden for anyone to disconnect Heathfield devices from power or network ports in order to connect their own unless approved by IT.

Connection to the Internet via the School network requires authentication for access and a security certificate to be installed on the device. Firewall and basic content filtering services are provided by a dedicated Fortigate firewall appliance, and detailed filtering and monitoring is provided by Smoothwall Advanced.

There are four available WiFi networks across the School site:

- **Heathfield WiFi** – For School-owned and managed devices such as desktops, teacher laptops, signage and other School equipment. Access is via multiple pre-shared keys (“MPSK”) – the key used determines the network access level.
- **Heathfield BYOD** – For staff and student personal devices, such as student laptops, staff personal laptops or mobile phones. Access requires a Heathfield username and password, and membership of a defined security group.
- **Heathfield Guest** – For guest devices only. Guest devices will be presented with a captive portal login screen in their browser, the current username and password will be printed on that day’s visitor badge.
- **Heathfield Residents** – For non-staff residents and other residential devices, such as Smart TVs. Access is via a pre-shared key.

Use of the Internet for non-education related activities is acceptable provided a balance is maintained and it does not encroach on the needs of work, study, research, or the delivery of lessons.

The School’s Internet filters are in place in order to protect pupils from content such as pornography, adult content, violence, gaming, chat rooms, self-harm and other sites not suitable for a school environment. The filtering operates 24 hours a day and may not be bypassed under any circumstances. All pages visited are logged to provide an audit trail.

Separate filtering policies exist for staff, senior pupils (Forms V – UVI), pupils in Forms III – IV and junior pupils Forms I – II, to provide age-appropriate content. Please see the separate Smoothwall Policies and Categories policy for further details.

Internet sharing from a 4G or 5G enabled phone, tablet or laptop device (also known as ‘personal hotspot’, ‘Internet sharing’ or ‘portable hotspot’) is strictly forbidden on school premises. Action will be taken when a hotspot is detected.

Further details of the School’s filtering of Internet content are available from IT Systems on request.

**Internet Timed Access**

Junior and Middle pupils (Forms I - IV) have additional timed access to selected multimedia sites. Access times are as follows:

<b>Group</b>	<b>Juniors</b>	<b>Middle</b>	<b>Seniors</b>
	Forms I-II	Forms III-IV	Forms V-UVI
Turned on	06:00	06:00	05:00
Turned off	21:00	22:00	00:00
Video streaming	16:00 – 19:15 weekdays 12:00 – 21:00 weekends	16:00 – 19:15 weekdays 12:00 – 22:00 weekends	Always

All Internet access for pupils is shut off at variable times in order to promote a healthy sleep pattern.

### **Email**

School email is provided through Microsoft 365. An email account is provided for staff, governors, peripatetic teachers and coaches, and all current pupils. Microsoft 365 is accessible from any computer over the Internet, and does not require being at School to access.

### **Printing & Copying**

All copying and printing is routed via PaperCut MF, the School's printer and copier accounting software. School departments are issued a set amount of credit each year; requests for additional departmental credit must be requested by the department head and approved by Finance. A pre-set credit is issued annually to students (in the amounts set out in the table below), and top-up credit can be purchased if required.

Printing and copying costs are actively monitored to ensure that the School's costs are maintained strictly according to budget. We are an eco-friendly school and seek to reduce paper usage and the costs of excess printing. Please only print if absolutely necessary.

The copiers are set to Print Release. This means that printing does not emerge automatically, users will need to swipe their card or login at the copier to release print jobs.

Printing from Bring Your Own Devices ("BYOD") devices is allowed only via the PaperCut web interface.

For most printers, a mono A4 page costs 2-3p to print and a colour A4 page 10-20p. Other sizes and types vary; the cost will be displayed in the PaperCut window before confirming the print job.

<b>User</b>	<b>Annual Quota</b>
Form I	£12.00
Forms II-III	£20.00
Forms IV-V*	£30.00
Forms LVI-UVI*	£40.00

\* Art and Photography pupils will receive an additional quota for exams

Paper for the printers can be obtained from the Copier room. Non-standard paper sizes should always be loaded into the manual feed slot, not the paper cassette. Transparencies designed for inkjet printers must never be used in a laser printer as severe internal damage will result – if in doubt, please check with IT Systems.

### **Remote Services**

Remote access to the school network is strictly controlled – please speak to IT Systems if you require this.

### **Security**

The School takes network and data security seriously and applies security-in-depth strategies to ensure systems and users are safe.

The School network is protected by dedicated firewall appliances, inspecting both north-south (in and out) traffic as well as east-west (cross network) traffic. Traffic across the network is segregated to ensure authorised devices have access only to what they need. Guest network traffic is separated from the School network entirely.


The School's email is monitored by Barracuda Email security, to help prevent spam and malware.

Multi-factor Authentication (MFA/2FA) is required for Staff accounts, and is recommended for use when offered by other 3<sup>rd</sup> party services.

Systems are maintained and monitored to ensure security updates are applied as and when they are available.

Additional security policies are applied when required, some conditional access policies may prevent access to services from outside the UK, for example. Exemptions from these policies are at IT Systems discretion.

All devices, irrespective of owner, must have up to date anti-virus software installed and running before connecting to the school network. If no anti-virus software exists, IT Systems staff will install an appropriate anti-virus software onto devices before connection to the network. There are no exceptions to this policy as the preservation of network security and its users' safety are paramount. School computers perform a quick anti-virus scan every morning or whenever the machine is next started.

Users must login to the network using their own login ID and password. It is forbidden for any person to disclose or exchange their network password details with anyone except IT Systems staff. When finished with a computer, it must be logged out. A computer must not be left unattended while logged in and should always be locked with the  - L key combination.

Attempting to access the School's secure systems or servers without authorisation, making use of a username/password assigned to another user, or attempting to gain access to the Server Room, IT Office, IT Store or any network cabinet is forbidden and constitutes gross misconduct. Any attempt to bypass the School's filtering systems by any means, including the use of external proxies or VPNs, also constitutes gross misconduct.

### ***Forbidden Software***

Illegally copied or unlicensed software must not be installed on any School computer.

Peer2Peer or torrenting software is not permitted on any device connected to the School network.

Software installation requests must go via the IT Systems team to ensure its suitability and security.

### ***File Sharing and Media Downloading***

It is an offence in the UK to possess, sell or pass on music or video files for which the user has not paid a royalty or a streaming service charge. Any such files found on any device within the school premises are subject to deletion and the user subject to disciplinary procedures.

### ***IT Strategy***

The IT Systems department works from a rolling strategy and continuously adapts it according to emerging trends, the needs of the staff, the needs of the administration and business groups, the needs of the pupils, and changes in the law and best practice. The School reserves the right to update applications and services whenever appropriate.

## **IT Services & Resources**

---

### ***File Storage***

Each user receives a personal OneDrive cloud storage folder, private to them and accessible from anywhere. All documents should be stored either here or in one of the Teams or SharePoint folders. A maximum quota is imposed, (in accordance with the table below) which should satisfy all users throughout their association with the school.

<b>User</b>	<b>File Space Quota</b>
Staff	1TB
Pupils	1TB

One Drive is designed for storing documents only and will prevent the storage of applications or executables.

It is inadvisable to save documents to the desktop or local folders as these documents will not be saved should the device experience a crash or require a rebuild. Transferring documents when switching devices is at IT Systems discretion. The School accepts no responsibility for the loss of documents not saved to the correct location.

### ***Shared File Storage***

Each user has access to shared file space, either inside a Team or within the SharePoint folders.

### ***Email Storage***

The quotas per user group are as follows:

<b>User</b>	<b>Mailbox Quota</b>
Staff	50GB
Pupils	50GB

All users are encouraged to maintain their inbox and delete old messages regularly. Folders at the root level (not under the inbox) should be used for the tidy storage of important messages.

The use of the School's email system for personal (non-Heathfield related) emails should be avoided. The use of the School email system for the purposes of operating another business is strictly prohibited.

The maximum single email size which can be sent or received through the School's email system is 25MB (and may also depend on the capabilities of the recipient). Large files can be shared through OneDrive or an alternate file transfer service, such as WeTransfer.

### ***Email Retention***

In order to prevent infinite storage growth, all email is subject to a retention policy as follows:

<b>Folder</b>	<b>Retention</b>
Inbox (and all folders underneath)	1 Year
All other folders	7 years
Drafts	1 year
Junk	30 days
Deleted items	7 days
Sent items	2 years
Contacts	15 years

Email which is required to last for the full 7 years should be placed in folders at the root level (not under the inbox). It is often convenient to create a master root folder (e.g. My Folder) and then create folders below this.

### ***Email Etiquette***

Email is subject to the same laws as the written word. Messages must not contain offensive, obscene, threatening or libellous language or be construed as such. Bullying messages (cyber bullying) will be treated with the same level of seriousness as physical bullying. The school will adopt a zero tolerance approach to any cyber bullying issues; all staff will challenge any abusive behaviour between pupils that comes to their notice and will report on to the DSL immediately any issues of this nature. Please see Safeguarding policy for further details about dealing with child-on-child abuse.

- Addresses in the **To:** field should be only for those recipients where a reply or action is required.
- Copies of messages for information should be sent to users in the **Cc:** (carbon copy) field.
- The **Bcc:** (blind carbon copy) field should be used where confidentiality is required, including when sending to multiple external recipients. It should also be used when sending email to large groups of recipients to avoid "Reply All" email overload.

Attachments should be kept as small as possible and consider zipping or archiving multiple files where appropriate.

Emails should not be written entirely in upper case (capitals). Messages should be marked as sensitive/confidential if appropriate; and the "high priority" flag should be used sparingly, if at all.

All School emails are signed off with the sender's name and position through an automatically applied signature. It is strongly recommended that messages are spell checked before sending. There is no ability to recall emails when sent outside of the School's domain.

### ***Email Security & Monitoring***

The School reserves the right to retrieve the contents of messages for the following purposes:

- to monitor whether the use of the email system is legitimate and in accordance with this policy;
- to find lost messages or to retrieve messages lost due to computer failure;
- to assist in investigations;
- to comply with any legal obligation.

The European Court of Human Rights has ruled that "it is not unreasonable for an employer to want to verify that employees are completing their professional tasks during working hours". Monitoring will only be carried out to the extent permitted or required by law. The School does not routinely monitor email messages. Spot checks or tailored searches may be undertaken in the context of disciplinary proceedings (whether actual or contemplated) or where the School has reason to believe that this policy may have been breached. All messages created on the School email system remain the property of the School, even after a pupil or member of staff has left.

### ***Email Spam and Phishing***

The School filters all mail upon receipt and quarantines or marks as suspect any spam (unsolicited bulk email) or suspected phishing emails found. All effort is made to filter out spam before it reaches a user's inbox. However, spam filtering is not fool-proof. The occasional spam message may reach a user and should be deleted in the normal way and/or added to the junk mail list.

Measures are taken to ensure that no false-positives (legitimate messages treated as spam or phishing) are filtered, however it is possible that the occasional message is falsely identified as spam. Incorrectly quarantined incoming messages can be retrieved by IT Systems where requested. IT Systems will not whitelist an email address or domain for the entire school – email addresses incorrectly marked as spam can be whitelisted for an individual account only.

All email is scanned for viruses and malware, however, emails with attachments from unrecognised senders should be checked before opening as they may contain a link to a virus or other undesirable payload.

### ***Email and Data Protection***

Email is subject to General Data Protection Regulations 2018 (“GDPR”) and to safeguarding rules. Any outbound email containing sensitive information (such as full names, dates of birth, addresses etc.) must be sent encrypted. An encrypted email service is available through the Barracuda Email Security platform – simply enter #*encrypt* in the email subject – your recipient will receive a link to access the email securely.

The email system stores all incoming and outgoing messages regardless of whether they are deleted from individual mailboxes. It is also subject to a GDPR Subject Access Request so always be mindful of what is written and do not express opinions on staff, pupils or parents. Keep the content strictly factual.

### ***Microsoft Office***

Microsoft Office is provided on all School machines, including staff laptops. Staff may install Office in their home machines via the Office Portal at <https://portal.office.com>.

Pupils may have Microsoft Office installed on their primary device and liaise with the IT Systems for further details. Such installations of Office will expire upon the pupil leaving the school.

### ***YouTube & Video Streaming***

YouTube and selected other video streaming services are allowed for use by some pupils during timed periods.

The needs of video delivery for lessons will always be given the highest priority. These timed periods are subject to change should usage be found to consume excessive bandwidth.

### ***Skype/Zoom and Video Conferencing***

Skype, Zoom and other video conferencing/communication platforms are allowed for use by pupils for contact with their family and friends.

### ***School Website***

The School website is self-hosted on a remote server by IT Systems on a Wordpress platform and is maintained by both the Systems and Marketing Departments. Any problems, incorrect or outdated information on the website is reported to IT Systems.

The website may be accessed via any standard web browser at the following URL: <https://www.heathfieldschool.net>.

### ***Classroom Facilities***

There are computers available in two dedicated ICT suites (C1 & C2), the Art suite, and the Library. All computers are connected to the school’s network and the Internet with content filtering.

C1 and C2 are available during break, at lunchtimes and after school for coursework and personal communications. The IT Technician can provide help when available.

Breakages in the IT suites are inevitable from time to time, but care should be taken not to abuse screens, keyboards, mice, cabling or other fragile equipment. Broken equipment should be reported to IT Systems as soon as possible.

Eating and drinking in the C1 and C2 classrooms, Art, and the Library is strictly forbidden at all times.

### ***Digital Cameras and Multimedia content***

Digital cameras are available for loan from the IT Systems office. Some notice is advisable as these resources are in constant demand. Staff should never use their personal devices to take photos or videos of pupils. Pupils may not, except with the teacher's permission, use their devices to take photos or video during a lesson.

### ***Joiners & Leavers***

For the detailed process for staff & pupil joiners and leavers, please see the separate document entitled IT Joiners and Leavers Procedures.

### ***Door Access & CCTV***

The School operates an electronic door access system using proximity ID cards and fobs. Currently there are 26 doors provisioned with readers. Access to doors is by staff and pupil category and centrally controlled.

Each user must take care not to lose their card or fob. Any loss must be immediately reported so that IT Systems can deactivate it to prevent unauthorised entry. Replacement cards or fobs are chargeable. Cards and fobs are for the use of the issued user only and must not be loaned out to other persons. Doors must be kept closed at all times. Please report any faulty doors or card readers to IT Systems immediately.

Requests for doors to be held open (for events or facilities bookings) must be communicated to IT Systems with as much notice as possible.

The School operates several network connected CCTV cameras across the School site – please contact IT Systems via the Bursar for any information relating to the CCTV systems.

## ***E-safety***

---

### ***General***

In general, the School's policy is to require staff and pupils always be careful not to give away personal information via email, forums or any form of social networking. Staff and pupils must be aware of anonymous forum members ("you don't know who they are") and are advised to never 'hide behind the keyboard'; to say only what you would say to the person's face.

### ***Social Networking***

The proliferation of social networking sites means that staff and pupils are required to be very diligent in their use of such sites for personal networking. Any public page featuring a member of staff or a pupil must be kept clean, presentable and must not in any way bring the school into disrepute. All social network accounts are required to have basic security set to ensure maximum privacy against all non-'friends'.



Social networking between staff and pupils is strictly forbidden.

No pupil may possess or use a social network account on any device if they are under the age of 13 years. This is a child safeguarding issue and any breach will initiate a mandatory inquiry.

### ***Welfare & Safeguarding***

In order to ensure safe use of the Internet especially with regard to violence, radicalisation, extremism, terrorism, adult content, plagiarism, software and music piracy, hacking, phishing and other malware, gambling, weight loss and other undesirable content, these complete categories (and others) are blocked from being accessible by pupils. This is in accordance with the **PREVENT** directive and further information may be found on the CEOPS site [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

### ***Monitoring***

All Internet access is monitored by automated systems for breaches of Safeguarding. A daily report of potential issues is sent to the DSL (Designated Safeguarding Lead) or Deputy DSL for any appropriate actions to be taken.

## **Data Protection - GDPR**

---

### ***Key Points for Staff***

In accordance with the GDPR, information relating to pupils or parents must be kept confidential and within the School's systems. This means that data must not be copied onto a home PC or personal device, nor may it be transmitted via electronic means outside of the School without encryption.

### ***Encryption***

The GDPR stipulates that all devices containing school and, particularly, pupil personal information, must be protected via PINs, passwords and encryption. All School laptops and tablets taken outside of the premises are subject to encryption. USB drives used for the purposes of transporting School data must also be encrypted – School computers will prompt for drives to be encrypted when attached.

### ***Intellectual Property***

All documents, applications and email messages which are created or developed at School or on a School computer remain the property of the School. Such documents, applications or messages may not be used at another workplace without specific consent in writing from the Headmistress.

## **School Equipment**

---

### ***School Computers***

A School computer is provided for the purposes of teaching and administration at the School. At times, staff may place sensitive data on the computer and must therefore be responsible for its safe-keeping and storage.

Use of the computer to conduct business outside of the School's interests is not permissible. Use of the computer by any third party is also not permissible, including family members or any non-staff.

Staff are not permitted to enter into any contract or subscription on the Internet on behalf of the School, without specific permission from IT Systems and the Bursar.

Care should be taken to avoid pupils having access to Staff computers.

### ***Staff Laptops & Tablets***

While School laptop/tablet users are free to access the Internet at home or from another location via their own ISP (Internet Service Provider), Staff and pupils are made to be aware that content may be downloaded which would otherwise be filtered by the School network. Such files are frequently retained in the cache of the computer and can be subsequently retrieved. Inappropriate content may therefore be inadvertently brought into School premises via the computer. Exercise caution and never allow anyone else to use the School device. Anyone found importing unsuitable material may be in breach of this policy and will be subject to investigation with possible disciplinary action following.

All School devices must be returned, complete with charger and any other supplied accessories, on termination of employment. The cost of replacing any device not returned or returned damaged may be deducted from the staff members final salary payment.

### ***Software and Maintenance***

The installation of other software should be with prior authorisation of IT Systems. Steps will be taken to ensure the software is licensed appropriately, is safe to use and will be unlikely to cause issues on the School computer or network.

The computers may be recalled from time to time in order to carry out required OS or application software upgrades or to apply critical updates. Reasonable notice will be given wherever possible.

### ***Personal Photos, Music & Video***

The School is not responsible for the storage of personal files on a School computer. The member of staff are required to make their own arrangements for backup of any such files and any loss is the sole responsibility of the user. These files are deliberately not stored on the School's servers in order to save storage space and keep work and leisure activities distinct and separate.

### ***Laptop Security***

It is the responsibility of the user to ensure that their computer is kept secure, both on and off the School premises. Staff are required to keep it safe in a carry case when not in use and avoid invitations to theft such as leaving it in view in a car. If travelling by air, always carry it as hand luggage. Computers may not be left in the Staff Workroom overnight except in locked storage. Care must be taken to secure the computer if leaving it on School premises during school holidays.

Acceptance of a laptop computer implies agreement in full with this IT Acceptable Use Policy. If a computer is lost, stolen or damaged, the Bursar or Manager of IT Network and Services must be notified in the first instance. The staff user may be charged for the cost of replacement if the device is lost or damaged due to negligence.

## **Personal Equipment**

---

Pupils are required to have a functional primary laptop or tablet computer complying with the current *Laptop Recommendations* guidelines, separately distributed.

All personal laptops and tablets brought to the School and connected to the network must comply with this policy. They must be running an approved Operating System and must have operational and up-to-date anti-virus software running.

Staff and pupils are responsible for the safe-keeping of their own computers. To prevent accidental loss, important work must be stored in OneDrive or Teams. All devices and chargers must be clearly marked with the owner's name. Pupil chargers will normally be kept in the Lapsafes for overnight charging (Forms I - III); laptops are expected to be used on battery during the day since trailing cables in the classrooms are not permitted, being a health and safety hazard.

### ***Pupil Laptop Usage***

Laptop computers are not to be used by junior pupils after 'lights out'. They are not to be loaned to another pupil and should never be shared with other users outside of the School without parental permission. Computers and their accessories must not be left unattended in classrooms or they are liable to be deposited with 'lost property'.

School email may be accessed on mobile devices via the official Microsoft Outlook app, this allows for the email data to be remotely wiped should a security breach or device-loss event occur – the School reserves the right to take this action.

## **IT Support**

---

### ***Support Priority***

IT Systems support will prioritise requests for help, to maintain school business and the delivery of Teaching & Learning. There is no strict priority hierarchy – best efforts will be made to support the core functions of the School, ensuring teaching & learning can continue.

### ***Fault Repairs***

Responsibility for the upkeep and correct functionality of school computers is with the IT Systems Department. Responsibility for pupil computers remains with the parents. IT Systems will provide general troubleshooting support and hardware support where appropriate. We recommend that staff and pupil personal devices are covered by an extended manufacturer's or third-party warranty in the event of hardware issues.

### ***Support Hours***

IT support is available between 0730 and 1700 Monday – Friday.

### ***Reporting an IT Fault***

Prompt repair of a faulty computer or service is dependent on the issue being reported to IT Systems in the correct manner. All issues should be reported by sending an email to Systems (full address [systems@heathfieldschool.net](mailto:systems@heathfieldschool.net)). If a support request is made in person, either in passing or over the phone, please follow this up with an email when you can to ensure all issues are logged.

## **Review**

---

### ***Policy Revision***

The School reserves the right to amend this policy and publish changes at any time.

## **Related Policies**

---

- Anti-Bullying Policy
- Data Protection Policy
- Record Keeping Policy
- Safeguarding Children and Child Protection Policy

- Social Media Policy
- Telephone Acceptable Use Policy