



IT ACCEPTABLE USAGE POLICY

Headteacher	Anita Spires
Chair of Governors	Katherine Russell
Date Policy Reviewed	January 2025 May 2026
Date Ratified by LGB	June 2026
Renewal Date	June 2028

Contents

Page No.

Introduction	3
Aims	3
Consultation/Formulation of Policy	3
Related Statutory Requirements/non-statutory guidance which inform policy	3
Link to other school/MAT policies, documents and required practice	3
Procedure/Practice/Guidelines	3
Password Security	3
General Conditions	4
Personal use of the Computing Services	5
Use of Telephones	5
Use of Email	6
Use of the Internet	6
Use of the Printing Facilities	7
Images and Videos	7
Monitoring	7
Data Security	7
Data to which this Acceptable Usage applies	7
Security of paper-based data	8
Security of electronic data	8
Release of data to others	9
Anti-Virus and Firewall Security	9
Physical Security	9
Encrypted USB Drives	10
Chromebooks	10
Beechwood Data	10
IT Acceptable Usage Policy Staff Agreement	11

Introduction

This policy sets out the responsibilities and minimum expected behaviours of persons who use the school's IT system as part of their employment at Beechwood School.

Aims

Beechwood School is committed to safeguarding its IT infrastructure to ensure it can be used in the most effective manner to support teaching and learning processes. The safety and integrity of the school's IT infrastructure is the responsibility of all staff.

Consultation/Formulation of Policy

This policy has been drawn up following the provisions of the DPA 2018.

Related Statutory Requirements/non-statutory guidance which inform policy

General Data Protection Regulations (2018)

Link to other school/MAT policies, documents and required practice

Disciplinary Policy

Data Protection Policy

Professional Practice Guidance

Safeguarding Policy

Mobile Device Policy

Procedure/Practice/Guidelines

As a user of IT services of the school you have a right to use its computing services; that right places responsibilities on you as a user which are outlined below. If you misuse school computing facilities in a way that constitutes a breach or disregard of this policy and data protection regulations, this may result in disciplinary action being taken against you and the immediate revocation/disablement of your user account as a consequence.

Staff are advised of this policy during their induction by the IT Department and of the school's requirement for them to adhere to the conditions therein.

For the purposes of this policy the term 'computer services' refers to any IT resource made available to you, any of the network services, applications or software products that you are provided access to and the network/data transport infrastructure that you use to access any of the services (including access to the internet). Staff who connect their own IT device to the school's network and the services available are particularly reminded that such use requires compliance to this policy.

Password security

Access to all systems and services is controlled by a central computing account and password. Staff are allocated their User ID and initial password as part of their induction with Beechwood School. Issuance and continued use of your User Account is conditional on your compliance with this policy.

Initial default passwords issued to any user should be changed immediately following notification of the account set up. You should change these passwords on a regular basis ensuring that the password is strong. Passwords will not be shared or revealed to any other party. Those who use another person's user credentials and those who share such credentials with others will be in breach of this policy. Staff user accounts should not be logged onto multiple computer's at once for the use of students who do not have login details and if such situations arise within the school day then staff can immediately contact itsupport@beechwood.slough.sch.uk

Staff will not at any time write down their passwords for their user account or any school related system onto paper whereby this could become data in the hands of the wrong person.

The school operates Wi-Fi for lettings visitors with guest access. Staff members should not hand students the access key nor obtain access keys from main reception to be handed from person to person. The lettings facilitator for the booking should enable the internet usage for that client using the passcode themselves.

General Conditions

In general, use of the school's 'computing services' should be for study, research, teaching or the administrative purposes of the school.

- Your use of the computing services must at all times comply with the law.
- Your use of the computing services must not interfere with any others' use of these facilities and services.
- You are not entitled to use a computer that you have not been authorised to use.
- You must not access any program or data that has not been specifically authorised for your use.
- You must not use or copy any data or program belonging to other users without their express and specific permission.
- You must not alter computer material belonging to another user without their express and specific permission.
- You must not use the computing services to harass, defame, libel, shame, intimidate, impersonate or abuse another person.
- You must not use the computing services for the access (or even trying to access), creation, collection, storage, downloading, display or sending any material which is:
 - o Violent (or that which glorifies violence)
 - o Criminal, terrorist or glorified criminal activity (including drug abuse)
 - o Racist or designed to incite racial hatred
 - o Homophobic
 - o Of extreme political opinion
 - o Pornographic or with otherwise unsuitable sexual content
 - o Crude, profane or with otherwise unsuitable language
 - o Blasphemous or mocking of religious and moral beliefs and values
 - o Offensive in the normal context
 - o In breach of the law, including copyright laws, Data Protection and computer misuse
 - o Belongs to other users of IT systems and for which you do not have explicit permission to use.
- You must not publish anything defamatory and/or knowingly false material about the school, your colleagues, students etc on social networking sites, blogs, on-line journals, wikis and any online publishing format that could bring yourself and the school into disrepute.
- You must not have any Beechwood students as friends on any social networking site you may belong to and are not to "Follow" "Friend Request" or use social media to make connection or become in direct contact with pupils.
- You must not search for, or use websites (proxies / VPNs) that attempt to bypass the school's internet filtering system unless specific permission has been granted to access these sites. Any such request to view a particular website should be directed to the IT Department for approval.

- You must not access Putlocker or other P2P sharing platforms for the illegal download of movies.
- You must not use Google Hangouts/instant messaging on the school's IT system. ▪ You must not use the computing services to conduct any form of commercial activity without express permission from the Headteacher.
- You must not use the computing services to disseminate mass (unsolicited) mailings. ▪ You must not install, use or distribute software for which you do not have a licence and which is not first authorised by the IT Department for installation.
- You must not introduce any form of malicious software onto the school network. ▪ You must not use any IRC or messenger software including but not limited to AOL, Yahoo, Facebook, Snap Chat, Tik Tok, Messengers, IRC or chat clients unless expressly authorised to do so for work purposes.
- You must not post or subscribe to newsgroups, on-line discussion boards or email list groups from the school's facilities unless specifically related to school activities.
- You must not form any form of network monitoring which will intercept data not specifically intended for you unless this activity is part of your normal job responsibilities or has been specifically authorised by the Headteacher.
- You must not play computer games of any nature whether preinstalled with the operating system or available online.

Staff Must Ensure:

- When IT Software/Hardware is being sourced for the benefit of learning and education the IT Manager must be consulted first to ensure its Network Compatibility and Budget commitments can be fulfilled.
- That if they do hold Social Media accounts personally that they hold the securest personal settings within their accounts so that students do not see staff personal information if they were to be searched for as well as adhering to the previously stated motion that Staff should not make direct connection (please see "General Conditions" above).
- When using Beechwood Remote Access platform that they do not download any personal data locally if it has personal first last names and therefore defies the standards set out in the GDPR act of 2018.
- When using Beechwood Remote that SIMS access is fully closed after use and that other people do not have direct access to this information.

Personal use of the computing services

It is recognised that there are occasions when employees might legitimately make private use of the schools' computing services. Modest use of the facilities for personal use is accepted during your non contracted working times so long as such activity does not contravene the conditions of this policy.

Use of telephones

There will be occasions when employees need to make short, personal telephone calls on school telephones in order to deal with extraordinary and emergency situations. Where possible, such calls should be made and received outside of the employee's normal working hours or when they do not interfere with work requirements.

Where internal school phones have access codes to dial out externally which has been put in place for the prevention of prank calling staff must not label as a reminder or write down anywhere the access codes that could be in eye-line of anyone apart from Beechwood staff.

The use of school telephones or private mobile phones for personal purposes, which are unreasonably excessive may be treated as gross misconduct under the disciplinary procedure. It is

absolutely not acceptable or within the IT acceptable use policy that staff use school phones to dial international numbers for personal calls.

Where the school has grounds to suspect possible misuse of its telephones, it reserves the right to audit the destination and length of outgoing calls and the source and length of incoming calls. This would not normally involve the surveillance of calls but in certain rare circumstances where there are reasonable grounds to suspect serious gross misconduct, the school reserves the right to record calls.

Use of email

As with telephones, it is recognised that employees may need to use e-mail for personal reasons and as described above, this would not normally be during your usual contracted working hours except in the case of an urgent or emergency basis.

If accessing a personal email employee should be careful before they open any attachment they receive, they are reasonably confident that the content is in no sense obscene or defamatory to avoid contravening the law. Equally, if an employee receives an obscene or defamatory email, whether unwittingly or otherwise and from whatever source she/he should not intentionally forward the email to any other address, unless specifically requested to do so by the IT Manager/Headteacher. Any other use of email for either personal or school purposes to send or forward messages or attachments which are in any way defamatory, obscene or otherwise inappropriate will be treated as gross misconduct under the appropriate disciplinary procedure. Where the school has reasonable grounds to suspect misuse of email in either scale of use, content or nature of messages, it reserves the right to audit the destination, source and content of email to and from a particular address.

E-mail should be treated like any form of written communication and, as such, what is normally regarded as unacceptable in a letter or memorandum is equally unacceptable in an e-mail communication. E-mails should be written in a professional context at all times in both emails to colleagues and those outside of school.

The school also reserves the right to access an employee's email account in her/his unexpected or prolonged absence (e.g. due to sickness) in order to allow it to continue to undertake the employee's normal role. In normal circumstances the employee concerned will be contacted before this is done, in order to provide him/her with prior knowledge.

Users should take care when opening any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if they have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).

Use of the Internet

The primary reason for the provision of internet access is for the easy retrieval of information for educational purposes, or to make use of learning resources, or to make legitimate authorised purchases to enhance the ability of its staff to undertake their school role. However, it is legitimate for employees to make use of the internet in its various forms in the same way as email above as long as it is not used to view or distribute improper material such as text, messages, or images which are derogatory, defamatory or obscene. The use of the internet for personal use will only be made outside your contracted working hours unless in the case of an urgent or emergency basis. This includes but is not limited to accessing the internet for personal shopping, personal emails, social networking sites and internet browsing etc.

Unauthorised use of the internet, which is unreasonably excessive for personal use or for purposes which are defamatory, obscene or otherwise inappropriate will be treated as gross misconduct under

the appropriate disciplinary procedure. The school reserves the right to audit the use of the internet from particular personal computers or accounts where it suspects misuse of the facility.

Users are not permitted to enter into any contract or trial subscription on the internet on behalf of the School, without specific permission to do so. Please contact the IT Manager.

Use of printing facilities

There may be an instance when employees may need to print an occasional personal document using the school's printing facilities. This would only be on an urgent and emergency basis and would not be routine practise. If an employee needed to print a personal document it would not be in volume nor interfering with work requirements.

The use of school printing facilities on a personal basis which are unreasonably excessive may be treated as gross misconduct under the disciplinary procedure.

Where the school has grounds to suspect possible misuse of its printing facilities, it reserves the right to audit the destination and length of this printing against the employee's printing card. Where there are reasonable grounds to suspect serious misuse, the school reserves the right to cancel the printing facility.

Images/Videos

The school will obtain written consent from parents/carers or students aged 18 and over for photographs and videos to be taken of students for communication, marketing and promotional materials.

Photographs of the school/students/staff or visitors should not be uploaded to any kind of website or shared externally to people/online sites without the relevant consent being in place.

Monitoring

Information made available within ICT facilities and networks will not normally be used to monitor the activity of individual staff members (e.g. to monitor their working time, activities, files accessed, internet sites accessed, reading of emails or private files) without prior knowledge except in the following circumstances:

- In case of an allegation of misconduct, the SLT or Governors can authorise such access of information when investigating the allegation.
- When suspected abuse of the school's ICT facilities is reported by an authorised body or individual.
- When the information is accessed inadvertently whilst fixing a problem with the ICT facilities.
- At the discretion of the Headteacher or Governing body, to ensure safety and well-being of the school community and the effective operation of the school.

Data Security

The school holds a variety of sensitive data including personal information about students and staff. If you have been given access to this information, you are reminded of your responsibilities under Data Protection law.

Data to which this Acceptable Usage applies

- Personal data is defined as data with two or more personal identifiers (e.g. name and address, name and date of birth).

- Sensitive data is any data that could harm, discomfort or embarrass an individual if it were to become public or be made available to an authorised individual. For example, SEN, racial or medical data, bank details, phone numbers etc.
- This AUP also applies to other confidential data such as performance management documents.

Security of paper-based data

- Staff are responsible for ensuring that data issued to them remains secure. On site this means keeping data away from being easily accessible by unauthorised personnel e.g. students. 2. If taking data off site, paperwork should be stored securely at all times. You should remain with the data when in transit, and store it in a secure area e.g. a locked cupboard.
- Data should never be taken outside of the EU.
- Particularly sensitive data e.g. SEN or medical records, payroll details etc, should never be removed from the school site and remain in a secure area e.g. locked cupboard, filing cabinet or office at all times.
- All paper-based records containing data should be securely shredded when no longer of use. You should not keep records beyond this time, unless advised otherwise (e.g. child protection records must be kept for longer).

Security of electronic data

- Ensure that your passwords for access to the network, email, SIMs etc are strong. You should change these on a regular basis, and not tell other members of staff or students these passwords.
- Ensure that caution is exercised when logging onto the school's network so that your password cannot be viewed by others.
- Ensure that you always use your own passwords to log onto the computer system. You never share or use another person's password to log onto the computer system.
- Ensure you do not log students onto the computer system with your own passwords in order for them to do their own work, browse the internet, watch YouTube during Lunch clubs etc.
- Ensure that you lock or log out of your computer when leaving it unattended, even for a short period of time. You are responsible for activity that takes place using your credentials, which can be monitored.
- When storing data in the shared area, ensure that this cannot be accessed by students by making sure that the files are stored into the Public Data Staff area. Name files appropriately.
- Ensure that data is not visible to students or other unauthorised personnel. This includes any data in SIMS.net.
- Data must not be stored on staff laptops or any electronic device outside of school without being encrypted and must comply with the GDPR. In general, there should be no need to store data outside of school.
- If storing/transferring data using a removable device, this device must be an encrypted USB drive which will be supplied to you by the school on request. This USB drive should remain physically secure both in transit and when stored, in the same way as paper-based records. It must not be taken out of the EU. Should this USB drive go missing, you must inform the Headteacher immediately. When your employment with the school terminates, you should return the USB drive to the IT Manager for secure disposal. Data must not be copied from the encrypted USB drive onto any computer equipment used off site (this includes home computers).
- Photos and videos of students must only be taken using the school owned devices. Any exception to this can only be authorised by the Headteacher. The placing of photos on websites and social media must be approved by the Headteacher or a member of staff to who this approval has been delegated to by the Headteacher.
- Files should be deleted from the network and encrypted USB drives when no longer needed, in line with the school's data retention policy. When deleting a file from a USB drive outside of

school you should shift and delete to avoid the risk of a copy of the file being stored in the recycle bin.

- If you use your mobile device(s) to access school email you must make sure that they are protected with a password or pass-code login. If your device is lost or stolen or you believe your accounts have been compromised then you must inform the Data Protection Officer/IT Manager or Headteacher as soon as possible.
- When you leave the school, be aware that your accounts for the network, email and other systems will be disabled when your contract ends. You should ensure that any USB drive issued to you is returned to the IT Department for secure wipe returning it to a re-usable condition and to make sure you have transferred your online Google Drive data to other members of staff to return or share them in a way that is accessible for your co-existing school colleagues.
- Upon termination of employment staff should not attempt to copy files from any shared drive or personal area to their own personal external drives. This intellectual data remains the property of Beechwood School.
- Staff must not transfer or store any confidential information on cloud services such as Dropbox or OneDrive. The only cloud storage that may be used is the School provided Google Drive account.

Release of data to others

- Staff may share information with each other regarding students as necessary in the performance of their duties, as long as this sharing of information is in the best interests of the student. The only exception to this is where a manager has explicitly stated that information is not to be shared.
- When sharing data with another organisation e.g. another school, you should check the legitimacy of the potential recipient. Wherever possible, school to school student data transfers will be made by the data admin staff using the secure B2B and S2S systems. If you are unsure you should consult the Headteacher, and always check before sending data out of the country.
- Staff with access to data regarding other staff, such as contracts and pay scales, should ensure they have been granted permission to access this data by the Headteacher.
- You should use your school provided email account for all email related to your work for the school. Your personal email account should never be used.
- The school takes any data breach very seriously. Should you become aware of any such breach, or the potential for one, you should inform the Headteacher immediately.

Anti-Virus and Firewall Security

All computers are installed with current versions of virus protection and firewall software by the IT Department. Users are not to alter the configuration of this software unless express permission has been obtained from the IT Manager. This software is installed to prevent an attack from malicious external rogue's and to prevent loss of data and corruption of programs/files. Users personal devices connected to our Guest wireless access must ensure they are running with the most adequate and up to date anti-virus software at all times.

If any user suspects viral infection on their machines, they should inform the IT Manager immediately. If the IT Department detects a machine behaving abnormally due to a possible viral infection it will be disconnected from the network with immediate effect until deemed safe.

Physical Security

The users of the school's computing services should always adhere to the following:

- Never to move any of the IT hardware and equipment to another location without the express permission of the IT Manager.
- Treat equipment reasonably in a safe manner.
- Keep liquids away from IT equipment.
- Do not place heavy objects on IT equipment.

- Do not drop IT equipment or objects onto it.
- Any portable computers must be securely locked away when not in use.
- Portable computer security is your responsibility at all times.
- Do not leave the portable computer unattended in a public place.
- Do not leave the portable computer on view inside your car. It should be locked away in your car's boot out of sight.
- Extra reasonable care must be taken to prevent the loss of encrypted USB drives containing school data.
- Staff supervising students using IT equipment should ensure they take reasonable care of such equipment.

Should there be an issue with the equipment or the staff member finds that something is not working correctly, a fault log containing full details of the issue should be sent immediately to itsupport@beechwood.slough.sch.uk so that this can be rectified.

Encrypted USB Drives

Encrypted USB drives issued by the school should be returned to the IT Department in the event of the employee's employment being terminated. The IT Department will arrange for the secure wipe of this data and the return to a reusable condition.

Chromebooks

- As a requirement set by the DfE devices and Chromebooks are installed with relevant software that can monitor via various methods internet traffic and keywords when both onsite and offsite. Users should not assume browsing internet on their Chromebooks outside of school is totally private.
- Upon contract termination of employment at Beechwood School the Chromebook and all loan equipment relating to it must be returned to the School's IT office. The School reserves the right to remotely wipe the Chromebook and de-install the license if this does not happen.

Beechwood Data

Staff are reminded that any document or data that has been created, received and stored during their employment with the school remains the intellectual property of Beechwood. On termination of employment employees are not permitted to take this intellectual property with them and any attempt to download or copy data onto personal hard drives or email systems may be intercepted. This includes but is not limited to personal documents, files, emails and attachments. Staff should not delete any necessary documents/files from their personal accounts at this time.

IT Acceptable Usage Policy Agreement

It is your responsibility to use the School's IT resources in line with this policy. Should you have any questions regarding this Acceptable Usage Policy, you should contact the HR Manager.

I hereby acknowledge that I have read and understood the Beechwood School IT Acceptable Usage Policy. I agree to abide by this policy at all times when using School IT. I understand that if I violate this Acceptable Usage Policy Agreement, I may face legal or disciplinary action according to applicable law or School policy.

Staff Name (printed):

Signature:

Date:

When completed, please return this IT Acceptable Usage Policy Agreement to the Trust HR Manager.