ICT and the Internet Acceptable Use Policy

Broad Heath Community Primary School

Approved by:	Jane Frankish	**Date:**	March 2022
Last reviewed on:	March 2022		
Next review due by:	March 2023		

Contents

1. Introduction and aims

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under staff code of conduct and teacher standards.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000

- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2018
- Searching, screening and confiscation: advice for schools

3. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- **"Users":** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose
- **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs
- **"Devices":** any form of technology that connects to the internet such as laptops, mobile phones, tablets, smart watches or any other smart device.

4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel

- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Senior Leadership Team will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion.

A request must be made via email to the headteacher in good time to allow a reply. If accepted, on all occasions, another member of staff must be present to protect against accusation of malpractice.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on behaviour and ICT policy.

A copy of these policies can be found on the school website.

5. Staff (including governors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The school's ICT Technician manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the ICT Technician

5.1.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the ICT Technician immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The headteacher may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during teaching hours unless otherwise agreed with the headteacher.
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's Staff Handbook.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts.

5.3 Remote access

Please refer to the remote learning policy found on the school website.

5.4 School social media accounts

The school has an official Twitter page, managed by the ICT Technician and headteacher. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

5.5 Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

5.5.1 Removal Drives/External Hard Drives

The use of removal drives/external hard drives are not permitted at Broad Heath Primary School. Any external device used to transfer data or to hold data must be encrypted by ICT before they are allowed to be used.

6. Pupils

6.1 Access to ICT facilities

Explain which ICT facilities are available to pupils, when and under what circumstances. For example:

- “All classes have access to a number of iPads. These are to be used under the supervision of staff.”
- “Computers and equipment in the school’s ICT suite are available to pupils only under the supervision of staff.”
- “Laptops are available outside of classroom for use under the supervision of staff.”
- “Specialist ICT equipment, such as that used for music or design and technology must only be used under the supervision of staff”
- “Pupils will be provided with an account linked to the school’s website as well as subscription based resources.”

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

Sanctions may include: missed playtimes, attending re-training programmes, missing "skills academy/golden time", letters of apologies, parents being called in to discuss sanctions in the home, possible exclusion.

7. Parents

7.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

Parents are aware of our expectations in our home/school contract which they sign.

8. Data security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

8.2 Software updates, firewalls, and anti-virus software

All of the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

Our Data Protection Policy can be found on the school website.

8.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the ICT Technician.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the ICT Technician immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

8.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT Technician.

9. Internet access

The school wireless internet connection is secured.

The school's Wi-Fi arrangements are:

- The web filtering is provided by Coventry City Council.
- The school have the ability to block or unblock specific websites.
- We have separate SSID for pupil iPads, Staff and visitors.

We acknowledge that no filtering system is foolproof. In the event of a person encountering an inappropriate website, that was not blocked by our filtering system, they must contact the ICT Technician immediately via email.

9.1 Pupils

The school's approach to the use of Wi-Fi by pupils includes:

- Pupils have access to Wi-Fi using school devices only.
- Google Safe Search is locked upon every device.
- Pupils must always be under supervision whilst using Wi-Fi.

9.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

10. Monitoring and review

The headteacher and Computing coordinator monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year.

The governing board is responsible for approving this policy.

11. Related policies

This policy should be read alongside the school's policies on:

- Online safety
- Safeguarding and child protection
- Behaviour policy
- Staff code of conduct
- General Data Protection Regulation (GDPR) policy and the privacy notices
- Social Media Policy
- Remote Learning Policy
- Video conferencing Policy

Appendix 1: Device loan agreements & Acceptable Use for staff

1. The agreement:

This document is between the end user and Broad Heath Primary School; it governs the proper use and care of devices that are assigned to the individual member of staff. This agreement will cover the period of date the device is issued through to the return date of the device to the school.

All issued equipment shall remain the sole property of the school and is governed by the school's policies.

1. The school is lending the employee the equipment for the purpose of working from home or other means of work-related usage.
2. This agreement sets the conditions for the employee taking the equipment home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this document confirms that I have read and agreed to the terms.

2. Damage/Loss

I agree to take full responsibility for the equipment issued to me and I have read this agreement and understand the conditions of the agreement.

I understand that I am responsible for the equipment at all times, in or out of school.

If the equipment was to be damaged/lost or stolen then I will immediately inform *Shaun HB (ICT*) and *Jane Frankish (Headteacher)*, and I acknowledge that I am responsible for full replacement costs. If the equipment is stolen, I will also immediately inform the police.

- I agree to keep the equipment in good condition and to return it to the school on demand from the school in the same condition.
- I agree to not leave this equipment unsupervised in an unsecured area.

3. Unacceptable use

- I am aware that the school monitors my activity on the devices. Routine checks will take place on the device at any time.
- I will not conduct any activity that constitutes 'Unacceptable Use'.

This includes:

- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to, or sending material that is pornographic, offensive, obscene, or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications, or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts, or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting, or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Using websites or mechanisms to bypass the school's filtering mechanisms

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Senior Leadership Team will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities

- I accept that if I engage in any activity that constitutes as 'Unacceptable Use' then I may face disciplinary action in line with the school's policy and the device(s) will be taken away.

4. Personal Use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The headteacher may withdraw permission for it at any time or restrict access at their discretion. Personal use is permitted provided that such use:

- Does not take place during teaching hours unless otherwise agreed with the headteacher.
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes
- Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities.
Where breaches of this policy are found, disciplinary action may be taken.
For more information and in-depth regarding Personal Use, please refer to the Acceptable User Policy.

I agree to not use this device for any personal use unless agreed with the Headteacher and will not loan the equipment to any other person.

5. Data Protection

I agree to take the following measures to keep the data stored on this device protected.

- To create a strong password/code on the device (at least 8 characters, with a combination of upper and lower-case letters, numbers and or special characters).
- To make sure the device locks itself after being inactive.
- To not share the equipment among family or friends.
- Keep the device secure with security checks and anti-virus scans.
- Install latest updates on the operating system, this includes security updates.

If I need any support doing the following, I can speak with Shaun HB (ICT).

6. Returning of equipment

I agree that I will return the device in its original condition that it was given to be in with all it is peripherals (charger cables). I will return the equipment to the school upon resignation dismissal or if I leave the employment of the school for any reason.
By signing this form, I can confirm that I have read and agree to all the rules and conditions above.

Staff member to fill		
Full name		
Signature		
ICT to fill		
Device		
Device		

Appendix 2: Device loan agreements and Acceptable Use for pupils

1. The agreement:

This document is between the end user and Broad Heath Primary School; it governs the proper use and care of devices that are assigned to a student. This agreement will cover the period of date the device is issued through to the return date of the device to the school.

All issued equipment shall remain the sole property of the school and is governed by the school's policies.

1. The school is lending the student the equipment for the purpose of doing schoolwork from home, standard internet usage such as blogging and the playing of designated games.
2. This agreement sets the conditions for the pupil taking the equipment home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this document confirms that I have read and agreed to the terms that the pupil must follow.

2. Damage/Loss

I agree to take full responsibility for the equipment issued to the pupil and I have read this agreement and understand the conditions of the agreement.

I understand that I am responsible for the equipment at all times, this means the pupil will not use the device without myself being present in the home.

If the equipment was to be damaged/lost or stolen then I will immediately inform the school, and I acknowledge that I am responsible for full replacement costs. If the equipment is stolen, I will also immediately inform the police.

- I agree to keep the equipment in good condition and to return it to the school on demand from the school in the same condition.
- I agree to not leave this equipment unsupervised in an unsecured area.

3. Unacceptable use

- I am aware that the school monitors my activity on the devices. Routine checks will take place on the device at any time.
- I will not conduct any activity that constitutes 'Unacceptable Use'.

This includes:

- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to, or sending material that is explicit, offensive, obscene, or otherwise inappropriate
- Setting up any software, applications, or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts, or data
- Causing intentional damage to ICT facilities
- Removing, deleting, or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Using inappropriate or offensive language
- Using websites or mechanisms to bypass the school's filtering mechanisms
- Trying to install software that was not intended to be installed on the device.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Senior Leadership Team will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities

- I accept that if any activity that constitutes as 'Unacceptable Use' then I may face disciplinary action in line with the school's policy and the device(s) will be taken away/police will be informed if it constitutes breaking the law.

4. Personal Use

Pupils are to use the device for schoolwork only. However, if this device will support other siblings or household members; then it can be used beyond the limits of just Broad Heath. However, I agree to follow the 'Unacceptable Use' terms set above.

I agree to not use this device for any personal use unless agreed with the Headteacher and will not loan the equipment to any other person.

5. Data Protection

I agree to take the following measures to keep the data stored on this device protected.

- To make sure the device locks itself after being inactive.
- To not share the equipment among family or friends, unless agreed with.
- Keep the device secure with security checks and anti-virus scans.

If I need any support doing the following, I can speak with Shaun HB (ICT).

6. Returning of equipment

I agree that I will return the device in its original condition that it was given to be in with all it is peripherals (charger cables). I will return the equipment to the school when requested.
By signing this form, I can confirm that I have read and agree to all the rules and conditions above.

Parent/Carer to fill			
Pupil's name		Pupil's class	
Parent Signature			
ICT to fill			
Device			
Check date history			

Unlawful damage will lead to a fine. Any damage that results in us having to replace and or sort will also lead to a fine.
These fines will be up to a maximum of £200 varying on the damage.
To prevent damage, please refrain from trying to clean the device yourself. **Please keep the device away from water.**