




Southville Primary School

IT Acceptable Use Policy

Policy written by:	Andy Bowman (Headteacher) from model policy (Bristol TWS)	
Ratified by Governing Body:	24.1.24	
Future review date:	December 2026	
Signed: (Headteacher)		Date: 24.1.24
Signed: (Chair of Governors)		Date: 24.1.24

Contents

1. Introduction and Aims	3
2. Relevant legislation and guidance	3
3. Definitions	3
4. Unacceptable use	3
4.1 Exceptions from unacceptable use	4
4.2 Sanctions	4
5. Staff (including governors, volunteers, and contractors)	4
5.1 Access to school ICT facilities and materials	4
5.1.1 Use of phones and email	5
5.2 Personal use.....	5
5.2.1 Personal social media accounts.....	6
5.3 Remote access	6
5.4 School social media accounts	6
5.5 Monitoring of school network and use of ICT facilities	6
6. Pupils	7
6.1 Access to ICT facilities	7
6.2 Search and deletion.....	7
6.3 Unacceptable use of ICT and the internet outside of school	7
7. Parents	8
7.1 Access to ICT facilities and materials	8
7.2 Communicating with or about the school online	8
8. Data security	8
8.1 Passwords	8
8.2 Software updates, firewalls, and anti-virus software	8
8.3 Data protection.....	9
8.4 Access to facilities and materials.....	9
8.5 Encryption.....	9
9. Internet access	9
9.1 Pupils	9
9.2 Parents and visitors	9
10. Monitoring and review	9
11. Related policies	10

1. Introduction and Aims

ICT is an integral part of the way our school operates, and is an essential 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 our staff disciplinary policy.

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 2020;
- 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.

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 Headteacher 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.

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 policy.

The school's behaviour policy and BCC code of conduct can be accessed from the school website.

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

5.1 Access to school ICT facilities and materials

The school's network manager manages access to the school's ICT facilities and materials for school staff alongside Bristol Trading With Schools. 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 network manager and the School Business Manager.

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 network manager immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Where appropriate staff can use phones provided by the school to conduct all work-related business. In usual circumstances, 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 network manager and 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
- 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) at the discretion of the Network manager and the Headteacher.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance if 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 (see appendix 1) 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 always appropriate. The school has guidelines for staff on appropriate security settings for Facebook and other social media accounts.

5.3 Remote access

Where certain staff require remote access to the system this is carefully controlled and facilitated through Bristol City Council (TWS).

We allow staff to access the school's ICT facilities and materials remotely. Bristol City Council continue to manage the system. Bristol City Council provide permission for the member of staff to access the system remotely.

All permissions for remote access must be carried out in writing to the Headteacher and the School Business manager. Bristol City Council will then be contacted to gain access.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the network manager and/or School Business Manager may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

5.4 School social media accounts

The school has official X (Twitter), Instagram and Facebook pages, managed by identified members of staff. 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.

The guidelines are as follows:

Posts should:

- Positively represent all members of our school community;
- Either publicise school-based events, show support for school-related community events (eg Bedminster Lantern Parade) or share news of school activities (including but not limited to curriculum, extra-curricular, off-site and residential activities and PTA events);
- Remain in line with the professional tone and content of communication expected of all staff.

Posts should not:

- Include an identifiable image of any child who does not have parent/carer permission for social media publication;
- Convey the personal opinion of an individual member of staff;
- Include political opinion or discriminatory/ prejudicial messaging.

In addition, school social media accounts must not be used to:

- Promote, circulate or suggest support for posts from other users in which political opinion, discriminatory or prejudicial messaging is used or suggested;
- Promote or suggest support for any third party user whose values are not aligned with our school values, or who are associated with political, illegal or activity.

5.5 Monitoring of school network and use of ICT facilities

The school and Bristol City Council 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;
- Fulfil its statutory safeguarding duties.

6. Pupils

6.1 Access to ICT facilities

When on-site the children have access to:

- Computers and equipment in the school's ICT suite, available to pupils only under the supervision of staff;
- Laptop computers and tablets used across the school, available to pupils only under the supervision of staff;
- Specialist ICT equipment, such as that used for music or design and technology, used only under the supervision of staff.

Pupils are provided with an account linked to a number of the school's remote learning systems. These are all password protected and controlled by an administrator within school. These remote learning systems may include:

- Purplemash
- Google Classroom
- Learning Village
- Nessy

Pupils are not permitted to use personal devices on school grounds including, but not limited to, mobile phones, tablets and smart watches. If mobile phones are brought to school for use during the journey to and from school, they must be handed in to the class teacher upon arrival and will be stored securely until home time. They must not be used in the playground before or after school.

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 address online behaviour in line with the Relationships and Behaviour Policy and/or the Managing Bullying 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.

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.

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.

Where necessary passwords can be reset using either Bristol City Council ITT support team. This request must be carried out by the Network manager, School Business Manager or Headteacher. Internal passwords can be requested through the Network Manager.

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.

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.

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 Headteacher, Network Manager, external ICT support company (Bristol TWS).

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 network manager or the school's external ICT support company (Apollo Technology) 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 Network manager and School ICT manager.

9. Internet access

The school wireless internet connection is secured and school uses a filtering process provided by Bristol City Council. It is important to note that not all filters are fool-proof and children and adults should be aware of the dangers online. It is also very important that children and staff are aware of what to do if inappropriate content comes through the filter and how to report this.

9.1 Pupils

Pupils have a tier 1 level of access within the schools filtering process. They are limited to the sites they can access. Where the school feel more access is required written consent is supplied to Bristol City Council. This written consent must come from the Network Manager, School Business manager or Headteacher.

Children are taught internet safety Term 1 of each school year.

9.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's wifi 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 wifi 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 wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

10. Monitoring and review

The Headteacher, ICT manager and School Business Manager will 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 3 years. 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
- Relationships and Behaviour
- Managing Bullying
- Staff discipline
- Data protection