ICT and internet acceptable use policy

St James CE Primary School

Approved by:	S Cross	**Date:** March 2021
	Shared with Governors	**Date: March 2021**
Last reviewed by:	Hardeep Grewal	**Date: February 2021**

Contents

1. Introduction and aims

The National Curriculum states:

"A high-quality computing education equips pupils to use computational thinking and creativity to understand and change the world. Computing has deep links with mathematics, science, and design and technology, and provides insights into both natural and artificial systems. The core of computing is computer science, in which pupils are taught the principles of information and computation, how digital systems work, and how to put this knowledge to use through programming. Building on this knowledge and understanding, pupils are equipped to use information technology to create programs, systems and a range of content. Computing also ensures that pupils become digitally literate – able to use, and express themselves and develop their ideas through, information and communication technology – at a level suitable for the future workplace and as active participants in a digital world."

In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail. Computer skills are vital to access life-long learning and employment; indeed, ICT is now seen as an essential life-skill.

The Importance of Internet Use

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems. Educational benefits are:
    - *access to world-wide educational resources including interactive sites, museums;*
    - *educational and cultural exchanges between pupils world-wide and in the community;*
    - *cultural, vocational, social and leisure use in libraries, clubs and at home;*
    - *access to experts in many fields for pupils and staff;*
    - *staff professional development through access to national developments, educational materials and good curriculum practice;*
    - *communication with support services, professional associations and colleagues;*
    - *improved access to technical support including remote management of networks;*
    - *exchange of curriculum and administration data with the LEA and DfES;*
    - *access to online lessons with teachers through remote home learning;*
    - *access to the school's website;*
    - *communicate real time information with parents and carers;*
    - *secure remote access for teachers and senior leadership group.*

- Internet access is an entitlement for students who show a responsible and mature approach to its use.

Most technologies present risks as well as benefits. Internet use for work, home, social and leisure activities is expanding in all sectors of society. This brings young people into contact with a wide variety of influences, some of which – as in life generally – may be unsuitable. It is important that schools, libraries and youth clubs, as well as parents, adopt strategies for the safe and responsible use of the Internet.

We endeavor to ensure throughout the school, that this curriculum is taught through safe internet platforms.

ICT is an integral part of the why our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. Birmingham LEA believes in the educational benefits of curriculum Internet use. It supports teaching and learning, pastoral and administrative functions of the school.

The school management recognises that the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding associated with inappropriate use and so plans accordingly to ensure appropriate, effective and safe pupil use.

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 disciplinary policy/behaviour policy/staff discipline policy/staff code of conduct.

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 and/or ICT lead 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. All inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

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.

The process for getting approval for such activities would be a written request to the head teacher.

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/discipline/staff discipline/staff code of conduct/etc.

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

- All staff are governed by the terms of the "Responsible Internet Use" in school.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by senior management.
- Staff development in safe and responsible Internet use and on the school Internet policy will be provided as required.

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
    - Teaching staff at the school are provided with a laptop and iPad for educational use and their own professional development. All staff understand that the Acceptable Use Policies apply to this equipment at all times.
    - A school mobile phone is issued to Head Teacher so that they may be contacted by pupils or parents out of school hours.
    - Staff must ensure the security of the school systems when using personal equipment connected to the school network e.g memory sticks, MP3 Players…
    - New technologies are evaluated and risk assessed for their educational benefits before they are introduced to the school community
- 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.

If these are files which contain highly, sensitive information (taking into account GDPR) permission will have to be granted from Senior Management Team (SMT) before any permissions can be updated or changed.

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 headteacher or ICT lead 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 and/or ICT technician 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/non-break time
- 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 mobile phone policy.

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 (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 appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

- The school is reviewing constantly the use of social networking sites and online communication and currently does not allow access to social networking sites such as Facebook, Twitter and Instagram.
- Age and role appropriate guidance is provided to the school community on how to use these sites safely and appropriately. This includes: not publishing personal information, not publishing information relating to the school community, how to set appropriate privacy settings and how to report issues or inappropriate content.

5.3 Remote access

We allow certain staff to access the school's ICT facilities and materials remotely.

- It is managed by ICT technician and Link2ICT.
- It is accessed through the St James domain, a secure VPN and password protected log in as they do in school.
- All the regulations which are in school, apply for remote access as well. Monitoring and filtering of activities are carried out and any misuse will be screenshot and sent to head teacher. Link2ICT also restrict/monitor access on certain websites.
- Staff need to send a request to the head teacher if they wish to have remote access. This will then be set up through the ICT technician.

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 ICT technician 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

This is not currently in use. Additional information will be added if a Twitter account is set up.

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. They will be reviewed regularly with regard to security. This includes, but is not limited to, monitoring of:

- Internet sites visited
    - In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor BCC can accept liability for the material accessed, or any consequences of Internet access.
    - Methods to identify, assess and minimise risks will be reviewed regularly.
    - The headteacher will ensure that the E-Safety policy is implemented and compliance with the policy monitored.
- Bandwidth usage

- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the LEA, particularly where a wide area network connection is being planned.
- Files held on the school's network will be regularly checked.
- The ICT Subject Leader / network manager will ensure that the system has the capacity to take increased traffic caused by Internet use.
- Use of portable media, such as memory sticks should be encrypted if sensitive or personal data is being taken off site.
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications
    - Personal data sent over the Internet will be encrypted or otherwise secured.

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

6. Pupils

6.1 Access to ICT facilities

- Use of school system:
    - Pupils may only use their individual e-mail account provided by school on the school system.
    - Pupils may only send to approved e-mail accounts on the school system.
    - Pupils must immediately tell a teacher if they receive offensive e-mail.
    - Pupils must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.
    - Pupils can send and receive e-mails internally and externally using the school e-mail system. Administrator and delegated senior staff can access individual pupil accounts to monitor use.
    - Access in school to external personal e-mail accounts may be blocked
    - Excessive social e-mail use can interfere with learning and may be restricted.
    - E-mail sent to an external organisation should be written carefully and senior leadership group are copied in (Cc), in the same way as a letter written on school headed paper.
    - The forwarding of chain letters is not permitted.
    - The forwarding of school e-mails to personal e-mail accounts is not permitted if the data includes any specific pupil data which can identify pupils individually.

- Pupils understand that their mobile phones should be handed in to the office staff that have lockable facilities and used in line with school policies at all other times.
- The Educations and Inspections Act 2006 grants the Head the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Head will exercise this right at their discretion
- Pictures / videos of pupils should not be taken on personal devices.
- Pictures/ videos of staff may be taken with their verbal permission and publishing of photographs must be with the full consent of the staff member.

- Computers and equipment in the school's ICT suite are available to pupils only under the supervision of staff
- iPads/laptops used in the classroom will be used under the supervision of staff. Apps and websites will be monitored.
- 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 virtual learning environment, which they can access from any device by using the following URL https://login.bgfl365.uk
- Pupils will not be allowed access to public or unregulated chat rooms.
  - Children should use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised.
  - User activity/access logs
    - The school will keep a record of any pupils whose parents have specifically denied internet or e-mail access.
    - At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
    - Parents will be informed that pupils will be provided with supervised Internet access (an example letter for primary schools is included as an appendix).
    - By using the Internet, KS2 students are agreeing to abide by the Responsible Internet Use statement.
    - Primary pupils will be issued with external individual email accounts, but will be authorised to a group/class email address under supervision for external communication.

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

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.

We ask parents to sign the agreement in appendix 2.

- Parents' attention will be drawn to the School Internet Policy in newsletters, the school brochure and on the school Web site.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations such as PIN, Parents Online and NCH Action for Children (URLs in reference section).

8. Remote learning

8.1 Microsoft Teams:

All staff and pupils using video communication such as Microsoft Teams must:

- Communicate in groups – one-to-one sessions are only carried out where necessary.
- TAs supporting the lessons will constantly monitor the Teams chat throughout – responding to issues/questions in order not to disturb the teaching. Where the teacher is in a group without the TA, the teacher will monitor the chat. Children who type anything inappropriate will receive a verbal/written warning. If this continues a follow up phone call will be made to the parent/carer.
- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable area within the home with an appropriate background. However, children are encouraged to switch off their cameras during lessons so it does not distract others.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material of school lessons for other purposes.
- Always remain aware that they are visible. Parents can support their child to access the session but must avoid being on screen or interacting with the teacher. Parents must ensure they have a stable connection to avoid disruption to lessons.

> All staff and pupils using audio communication e.g. recording audio on PowerPoint must:

- Use appropriate language – this includes others in their household.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they can be heard.

> The school will consider whether one-to-one sessions are appropriate in some circumstances, e.g. to provide support for pupils with SEND. This will be decided and approved by the SLT, in collaboration with the Inclusion Leader.

> Pupils not using devices or software as intended will be disciplined in line with the Behaviour Policy.

- The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required. The school will communicate to parents in writing about any precautionary measures that need to be put in place if their child is learning remotely using their own/family-owned equipment and technology, e.g. ensuring that their internet connection is secure.

> During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online. The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

9 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.

9.1 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.

9.2 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.

9.3 Data protection

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

9.4 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 or headteacher 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.

9.5 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 on encrypted devices only or through online password protected documents.

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.

10. Internet access

The school wireless internet connection is secured.

- **Management** of Filtering

  - **Blocking strategies** prevent access to a list of unsuitable sites or newsgroups. Maintenance of the blocking list is a major task as new sites appear every day.
  - **A walled-garden or allow list** provides access only to a list of approved sites. An allow list will inevitably restrict pupils' access to a narrow range of information.
  - **Dynamic filtering** examines the content of Web pages or e-mail for unsuitable words. Filtering of outgoing information such as Web searches is also required.
  - **Rating systems** give each Web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject these pages.

  - **Monitoring** records Internet sites visited by individual user. Access to a site forbidden by the filtering policy will result in a report. It is also possible to remove access automatically after a set number of policy violations. This is via a programme called Policy Central.

- Despite careful design, filtering systems cannot be completely effective due to the speed of change of Web content. Filtering may be performed by the ISP, by the LEA, at school-level or by any combination. School-level systems require considerable management to maintain effectiveness and place huge responsibility on the school if they are the only systems in place.

- Careful monitoring and management of all filtering systems will be required. It is important that the school establishes the filtering criteria rather than simply accepting filtering default settings.

  - The school will work in partnership with parents, the LEA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
  - If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to BCC using the e-mail *filtering@bgfl.org* via the E-Safety officer.
  - Policy central monitors key words when using the internet and if these words are used accidently or on purpose, then an e-mail is sent to the allocated policy central officer.
  - Any material that the school believes is illegal must be referred to the Internet Watch Foundation (please see references given later).

- Any visitors who need access to the wifi will be logged on as a Guest wifi account with restricted access so they cannot access any sensitive school data.

10.1 Pupils

School’s approach to the use of wifi by pupils:

- Wifi is provided across the school for laptop and iPad use in classrooms. Children can log onto laptops with their given username and password. iPads do not require a log in so they are accessible to all classes.
- iPads are restricted for users so they cannot download, delete or adapt any apps on the iPad. They cannot access any restricted websites.

- The following statements will require adaptation according to the pupils' age:
  - Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
  - Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
  - Training should be available to staff in the evaluation of Web materials and methods of developing students' critical attitudes.
- As children enter our school they will be required to sign the acceptable use policy outlining the rules they must follow when using any school based ICT facilities.
  - Rules for Internet access will be posted in all rooms where computers are used.
  - Pupils will be informed that Internet use will be monitored.
  - Instruction in responsible and safe use should precede Internet access.
  - Pupils will be reminded of the rules and risks of using the Internet as appropriate.
  - A module on responsible Internet use will be included in the PSHE programme and Computing curriculum covering both school and home use.
  - Formal lessons during the new computing curriculum will be taught at various times.

10.2 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. ICT technician then allows access through a password to connect to the wifi.

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)
- Parents or visitors will be granted access to the internet for supporting workshops after the acceptable use agreement form has been signed.

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

10.3 Staff

- All staff are governed by the terms of the 'Responsible Internet Use' in school.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by senior management.
- Staff development in safe and responsible Internet use and on the school Internet policy will be provided as required.

10.4 Use of Internet Across the Community

Example of Internet access rules in libraries/ Adult classes:

- *Adult users will need to sign the acceptable use policy.*
- *Parents/carers of children under 16 years of age will generally be required to sign an acceptable use policy on behalf of the child.*

11. Web Site Content Management

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Web site should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.
- Written permission will be obtained from parents or carers prior to pupils taking part in external video conferencing.
- Students understand that they must have their teacher's permission to make or answer a video conference call
- Supervision of video conferencing will be appropriate to the age of the pupil

12. Management of Newsgroups and E-mail lists

- Newsgroups will not be made available to pupils at St James unless an educational requirement for their use has been demonstrated and is appropriately controlled.

13. How Complaints Regarding Internet Use will be handled

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

- Sanctions available include:
  - interview/counselling by IT Subject Leader;
  - informing parents or carers;
  - removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system.

14. Monitoring and review

The headteacher and ICT lead 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.

15. Related policies

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

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection

Appendix 1: Facebook cheat sheet for staff

Don't accept friend requests from pupils on social media

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile

- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
  - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
  - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers

Name of parent/carer:

Name of child:

Online channels are an important way for parents/carers to communicate with, or about, our school.

The school uses the following channels:

- Our official school website
- Email/text groups for parents (for school announcements and information)
- Our virtual learning platform

Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year email groups, or chats (through apps such as Teams)

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way
- Use private groups, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers

Signed:	**Date:**

Appendix 3: Acceptable use agreement for older pupils

Acceptable use of the school’s ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When using the school’s ICT facilities and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher’s permission
- Use them to break school rules
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school’s network using someone else’s details
- Bully other people

I understand that the school will monitor the websites I visit and my use of the school’s ICT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school’s ICT systems and internet responsibly.

I understand that the school can discipline me if I do certain unacceptable things online, even if I’m not in school when I do them.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school’s ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school’s ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 4: Acceptable use agreement for younger pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Try to access Facebook or other social networking sites
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Share my password with others or log in using someone else's name or password
- Bully other people

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the school's ICT systems and internet.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**