Acceptable Use Policy

ICT Code of Conduct

St John's Primary School	
Policy: Acceptable Usage Policy	
Policy Originator: E Rinttila	**Review Period:** Annual **Last reviewed:** January 2024
Status: Non- Statutory	**Next review Date:** January 2025

Introduction and aims

ICT and the related technologies, such as email, the internet and devices, are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign to say they have read this policy and adhere to its contents at all times. Any concerns or clarification should be discussed with the Online Safety Coordinator/ DSL– Ellen Rinttila.

The school provides a secure method to access the school network remotely, in addition, the school email solution is cloud based and authenticator protected, and can therefore be accessed anywhere there is an internet connection. These systems are provided to ensure that no data needs to leave the school systems.

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 disciplinary policy, behaviour policy and staff code of conduct.

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 2023
- Searching, screening and confiscation: advice for schools
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

Acceptable use – expectations for staff

- I appreciate that ICT includes a wide range of systems, including mobile phones, tablets, email, social networking, and that ICT use may also include personal ICT devices being used for school business.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.

- I will only use the school's email, internet and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Head or Governing Body.

- I will not use any school computer to access my personal (home) email to avoid transmission of viruses.

- I understand that the use of memory sticks, memory cards and other removable storage is prohibited, unless I have express permission from the ICT manager.

- I will comply with the ICT system security and not disclose any passwords or PINs provided to me by the school or other related authorities.

- I understand that I am responsible for all activity carried out under my login and will not allow other staff members or pupils to use it.

- I will not leave my passwords or PIN unprotected (eg by writing it down).

- If accessing the school email system from home, I will not download or save attachments to my home computer/tablet.

- I will only take images of pupils and/or staff for professional purposes in line with school policy. I will not distribute images outside the school network without the permission of the Head.

- Outside of school, emails can be accessed online via the Microsoft 360 secure site; however, emails should not be stored on personal devices.

- I will ensure that school data is kept securely and is used appropriately, whether in school, taken off the school premises, or accessed remotely.

- I will not use a personal device for personal reasons while supervising children.

- I will ensure that any photos or videos of children are deleted from devices before they are taken off the school premises.

- I will not install any hardware or software without the permission of the IT Manager.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- I will respect copyright and intellectual property rights.

- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or the Head.

- I will support the school's Online Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies. I will promote online safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

- I will report any incidents of concern regarding children's safety to the Online Safety Coordinator, the Designated Safeguarding Lead (DSL) or Head teacher.

- I will take responsibility for my personally-owned devices and will ensure that they should be switched off (or silent) at all times. The Bluetooth functionality of a mobile phone or tablet may not be used to send images or files to other mobile phones.

- Mobile phones and personal devices, cameras and videoing equipment are not permitted in certain areas within the school site such as changing rooms and toilets.

Social media:

- I will ensure that all electronic communications with parents, pupils and staff, including email, chat functions and social networking, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

- I will show awareness of my digital tattoo and exercise caution in my use of social media or any other web based presence I have. This includes written content, videos or photographs and views expressed either directly or by 'liking' certain pages or posts or following certain individuals or groups.

- I will not make contact with pupils or ex pupils, must not accept or initiate friend requests, nor follow pupil/student or ex pupil accounts on any social media platform. I must not communicate with pupils/students or ex pupils via social media, websites, instant messenger accounts or text message. The only acceptable method of contact is via the use of school email accounts or telephone equipment.

- I should not make contact with pupils' family members, accept or initiate friend requests, or follow pupils' family member's account on any social media platform.

- As a parent and a member of staff, I must exercise caution and professional judgement in these communicating with other parents. I should not have any contact with pupils' family members via social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.

- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serious infringements may be referred to the police.

Sanctions

Staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on our disciplinary policy and staff code of conduct.

Staff (including governors, volunteers, and contractors)

Access to school ICT facilities and materials

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

- Computers, tablets, iPods 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 eduthing directly using eduthing@bflt.org.uk or by calling 0203 750 9796.

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. Staff should enable multi-factor authentication on their email accounts.

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 or sent via Egress 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 that contains the personal information of another person, they must inform eduthing 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. Staff may also use the 3CX app to contact parents, or in case of an emergency, may withhold their caller ID when using a person device.

School phones must not be used for personal matters.

The school can record in-coming and out-going phone conversations.

All incoming callers are made aware that the conversation is being recorded when the reach the school switchboard at the beginning of a call.

Staff who would like to record a phone conversation should speak to Ellen Rinttila as callers will need to be made aware of reasons for this.

All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

Remote access

We allow staff to access the school's ICT facilities and materials remotely via the virtual private network (VPN) or via Office 365 if documents are stored in this area.

Explain the remote access system you use, including:

- This is managed by school and outsources to eduthing for technical support.
- Staff need to follow the same expectations for acceptable use if accessing remotely
- Staff will be given instructions for use of the VPN when starting at school
- 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.

School social media accounts

The Federation has an official Facebook page, managed by SLT, Office Administrators. 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.

Filtering and Monitoring of internet usage

The school has a responsibility to monitor the use of its ICT facilities and network.

Ellen Rinttila is assigned to monitor filtering and monitoring as DSL. This includes auditing.

Vicky Wood is the allocated Governor responsible for filtering and monitoring.

Monitoring includes, but is not limited to, the 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

Monitoring of all internet usage on school devices in completed using the SENSO tool. This tool has been checked for high standards and is regularly monitored. Please see report for further information.

Critical alerts from this service are dealt with immediately. A weekly report of incidents is checked with follow up actions completed and recorded on the DSL weekly log.

Filtering is completed using Smoothwall software. This service has also been check for high standards- please see report for further information. Audits of filtering are completed using the TestFiltering Tool. This is completed by the DSL each week using different devices and is recorded in the DSL minutes.

Pupils

Access to ICT facilities

- Chromebooks are available to pupils only under the supervision of staff.
- Children are able to use school iPads, but only with supervision by staff.
- Pupils will be provided with an account linked Google Apps for Education, which they can access from any device by signing into Google. Login details for this account are also shared with parents to support home/school development of learning.

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.

Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains an online element.

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
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- 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

Parents

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 head teacher's discretion.

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

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.

Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore 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.

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.

Members of staff 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.

Pupils will be allocated passwords and these will be stored on staffshare.

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.

Any personal devices will use BYOD WIFI.

Data protection

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

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 eduthing.

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 Eduthing 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.

Protection from cyber attacks

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- All staff complete Cyber Security Training using the training from the National Cyber Security Centre - https://www.ncsc.gov.uk/information/cyber-security-training-schools
- New staff will complete this training as part of their induction training.
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents (information head teacher).
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - **'Proportionate'**: the school will verify this using a third-party audit to objectively test that what it has in place is up to scratch
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up-to-date:** with a system in place to monitor when the school needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be
- Back up critical data once a day and store these backups on school servers.

- Delegate specific responsibility for maintaining the security of our management information system (MIS) to Eduthing.
- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication where they can, on things like school email accounts
    - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and seeing if they have the Cyber Essentials certification

Internet access

The school wireless internet connection is secured.

- Smoothwall filters and monitors all internet usage in school.
- Staff and pupils are briefed in reporting any concerns that may not have been filtered by Smoothwall.
- All Smoothwall flags are immediately emailed to DSLs and addressed in a timely manner. Any outcomes from this are recorded on CPOMs/ as part of DSL minutes weekly.
- SENSO software monitors all device usage. DSLs monitor this daily and view a weekly report.
- Both systems are audited by the DSL and are checked by the assigned governor.

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 head teacher.

All visitors will only have access to the BYOD WIFI network.

The head teacher 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.

Monitoring and review

The head teacher and Eduthing monitor the implementation of this policy, including ensuring 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.

Related policies

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

- Online safety

- Safeguarding and child protection
- Behaviour Policy
- Staff discipline – Code of Conduct
- Data protection
- Computing Policy