St. Rose's
Inspiring Education, Therapy & Care

Staff ICT and Internet Acceptable Use policy

Person responsible:	Principal
Date approved by governing body:	December 2022
Review cycle:	Every year
Date of policy review:	December 2023

Contents

1. Introduction and aims

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school. However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

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

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

Breaches of this policy may be dealt with under our Staff Behaviour and Code of Conduct policy.

2. Relevant legislation and guidance

This policy agreement must be read in conjunction with the other policies and legislation:

- On Line Safety Policy
- Data Breach Policy and Procedure
- Data Protection Policy
- Information and Records Retention Policy
- Information Security Policy
- IT Password Policy
- IT Bring Your Own Device Policy

And also the following:

- Safeguarding Children and Young People
- Safeguarding Adults with Care and Support Needs
  Along with the following documents:
- Guidance for safer working practice for those working with children and young people in educational settings
- Keeping Children Safe in Education 2021

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 2021
- 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 Senior Management Team and IT Manager 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 Principal's discretion.

4.2 Sanctions

Staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on Staff Behaviour and Code of Conduct.

This can be found on the School website or at this location on the network – \\SR-FILES\CPP\Staff\POLICIES\POLICY DOCUMENTS\Statutory

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

5.1 Access to school ICT facilities and materials

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

- Desktop computers, laptops, tablets, smart phones, and other devices
- Access permissions for certain applications 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 notice they have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT Helpdesk.

5.2 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 Data Protection Officer 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.

5.3 Personal use

Staff are permitted to 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 Line Manager, Business Manager or IT Manager 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 contact time/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 5.6).

Staff are permitted to use their personal devices (such as mobile phones or tablets) in line with the school's IT Bring Your Own Device 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 5.2) to protect themselves online and avoid compromising their professional integrity.

5.4 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 accounts (see appendix 1).

The school has an official Facebook and Twitter page, managed by Eve.Qurishi@stroses.org.uk. 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 always abide by these guidelines.

5.5 Remote access

We allow specific devices to access the school's ICT facilities and materials remotely.

St Rose's provides a VPN (Virtual Private Network) service for the purpose of connecting off-site devices to ICT resources on the St Rose's network. This service is managed by the IT Department.

Staff requiring remote access should request access via the IT Helpdesk.

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 must take any precautions communicated by the IT Manager/Business Manager to protect the integrity of the device and the school's network from cyber security threats. An example of what has previously been communicated is staff should not to use public Wi-Fi services for accessing any St. Rose's data.

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.

5.6 Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network infrastructure. 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

6. Pupils

6.1 Access to ICT facilities

- Computers and equipment in the school's ICT suite are available to pupils only under the supervision of staff
- Specialist ICT equipment, such as that used for music or design and technology must only be used under the supervision of staff

6.2 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) 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.

8. Data security and protection

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

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

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and devices and keep these passwords secure. For further information on how to set a password, please see our IT Password Policy.

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

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

8.2 Software updates, firewalls, and anti-virus software

All the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly and automatically where possible. However, some manual intervention may be required by staff at times, and this must be completed when instructed by the IT Department.

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

Any personal devices accessing St. Rose's data in any way (including work e-mail accounts) must notify the IT Department.

8.4 Access to facilities and materials

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

These access rights are managed by the IT Department.

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 IT Department immediately.

Users should always log out of systems when no longer in use and lock their equipment when step away from the equipment, even if only for a moment to avoid any potential unauthorised access. Equipment and systems should always be logged out of 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 advised by the IT Manager.

9. Internet access

The school wireless connection (SR Corp Wi-Fi) is for school devices only. This has filtered internet access.

A separate wireless connection (SR Guest Wi-Fi) is available to members of the public e.g., parents, visitors and staff using personal devices.

Please be aware that filters are not fool proof. If you access a site which you feel may be inappropriate, please immediately report this to the IT Department via the IT Helpdesk.

9.1 Pupils

The SR BYOD Wi-Fi wireless connection is available throughout the buildings to all pupils. Access to this can be requested via the IT Helpdesk.

9.2 Parents and visitors

Parents and visitors to the school are permitted to use the school's guest Wi-Fi without the need for any authorisation from the IT Department. The password is changed periodically by the IT Manager, and this is provided to all staff freely.

The IT Department can and will revoke access to the guest Wi-Fi network for anyone who is found not complying to the rules of this policy (see section 4).

S. Talwar 7.12.2022.

7.12.2022

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 Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi 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 https://www.facebook.com/help/236898969688346/?helpref=uf_share 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 https://www.facebook.com/help/124518907626945/?helpref=uf_share 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 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 Facebook page
- 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 Facebook groups, email groups, or chats (through apps such as WhatsApp).

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, the school's Facebook page, 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, the school's Facebook page, 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 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:
- Disclose my username or password to anyone and will adhere to the IT Password Policy
- Report any illegal, inappropriate or harmful material or incident
- 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, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic
- 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
- 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 ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school and college's photo permission list on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so from a senior member of staff. Any image must be downloaded as soon as possible to the school or college system and deleted from personal equipment without being shared at any point. Where these images are published (e.g. on the school or college website) no personal information will be linked to those who are featured.
- I will double check what I have written in reports, emails or any other documents in case they contain a disclosure breach.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will let the designated safeguarding lead (DSL) and IT 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:**

I have read and understood this policy.

Name .... Signature .... Date ....

New starters: Please return signed copy to the school office.