ICT and Internet Acceptable Use Policy

Approved by:	PWG	**Date:** Updated 5th June 2025
Last reviewed on:	5th March 2024	
Next review due by:	February 2027	
SLT Lead:	Business Manager	

Contents

St George Catholic College is in the Trusteeship of the Roman Catholic Diocese of Portsmouth and maintained by Southampton City Council Local Authority. Our school leaders and governors are entrusted by the Bishop with the ministry of school leadership and will always act in recognition of the love of Christ for all members of our College community and one another.

We share a vocation for the common good in our world and we are committed to working together as a family. All of our policies and procedures are formed to enable all members of our St George family to be safe and cherished, feel happy and fulfilled and be treated fairly in a positive environment founded on mutual respect and shared values. This policy is part of the foundation that enables everyone to **aspire to be all that God has created us to be.**

1. Introduction and aims

1.1 Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including senior leadership teams), governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

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

1.3 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

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

1.5 Breaches of this policy may be dealt with under our Behaviour & Exclusions Policy or Staff Disciplinary Policy & Procedure.

2. Relevant legislation and guidance

2.1 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
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

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

"Personal Devices" or **"portable computers"** are defined as laptop, notebook, tablet computers and smart phones.

- **"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

3.1 See Appendix 6 for a glossary of cyber security terminology.

4. Unacceptable use

4.1 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).

4.2 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
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- 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, 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, such as Virtual Private Networks (VPNs) or Proxy Sites
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

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

4.4 Exceptions from unacceptable use

4.4.1 Where the use of school ICT facilities (on the school premises and/or remotely) 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 in liaison with the DSL.

4.5 Sanctions

4.5.1 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, staff discipline and the staff code of conduct.

4.5.2 The school's Behaviour & Exclusions Policy, Staff disciplinary policy & Procedure and Staff Code of Conduct can be found on the staff drive under Teaching & Learning – Policies.

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

5.1 Access to school ICT facilities and materials

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

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programs or files

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

5.1.3 Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the network manager.

5.2 Use of phones and email

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

5.2.2 This email account should be used for work purposes only.

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

5.2.4 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.

5.2.5 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.

5.2.6 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.

5.2.7 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.

5.2.8 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.

5.2.9 If staff send an email in error that contains the personal information of another person, they must inform the Network Manager immediately and follow our data breach procedure.

5.2.10 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. In exceptional circumstances (i.e. for safeguarding reasons) staff can provide their mobile number if it ensures the safety of our students.

5.2.11 School phones must not be used for personal matters.

5.2.12 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.

5.3 Personal use

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

5.3.2 Personal use is permitted provided that such use:

- Does not take place during 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

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

5.3.4 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.

5.3.5 Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with this policy.

5.3.6 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.

5.3.7 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.

5.4 Personal social media accounts

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

5.4.2 The school has guidelines for staff on appropriate security settings for Social Media accounts (see Appendix 1).

5.5 Remote access

5.5.1 We allow staff limited access the school's ICT facilities and materials remotely using various approved methods and systems.

5.5.2 When accessing the school's ICT facilities remotely, staff must adhere to the same policies and security protocols as when using them on-site. Extra caution should be exercised when accessing the system off-site, particularly in ensuring devices are secure and following any security measures required by the Network Manager to prevent viruses, data breaches, or other security risks.

5.5.3 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.

5.5.4 The school's Data Protection Policy can be found on the staff drive under Teaching & Learning – Policies.

5.6 School social media accounts

5.6.1 The school has an official Facebook, Twitter and Instagram page, managed by a member of staff. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

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

5.7 Monitoring of school network and use of ICT facilities

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

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

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

5.7.3 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"
- "Pupils will be provided with a Microsoft Office 365 account, which they can access by visiting office.com
- Pupils on occasion are issued a device that can be used at school and home for the purpose of completing school work. These devices are usually provided by the school to assist pupils with their specialist education needs. These are issued for an agreed period of time and require Pupils and Parent/Guardian to sign an Acceptable Use Agreement. These devices are managed and controlled by the schools' IT department

6.2 Search and deletion

6.2.1 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.

6.2.2 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.

6.2.3 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.

6.3 Unacceptable use of ICT and the internet outside of school

6.3.1 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

7. Parents

7.1 Access to ICT facilities and materials

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

7.1.2 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.

7.1.3 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

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

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

8. Data security

8.1 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.

8.2 Passwords

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

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

8.2.3 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.

8.2.4 All staff should use a password manager to help them store their passwords securely. The IT Department will generate passwords for pupils using a password generator and keep these in a secure location in case pupils lose or forget their passwords.

8.2.5 On rare occasions, students will be permitted to use their mobile phone in ICT lessons to complete authentication when logging in as Microsoft now require two factor authentication.

8.2.6 Members of Staff should not leave any devices unsecured and unattended. They should lock their screen or log off to prevent unauthorised access to data and devices.

8.3 Software updates, firewalls and anti-virus software

8.3.1 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.

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

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

8.4 Data protection

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

8.4.2 The school's Data Protection Policy can be found on the staff drive under Teaching & Learning – Policies.

8.5 Access to facilities and materials

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

8.5.2 These access rights are managed by the Network Manager

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

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

8.6 Encryption

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

8.6.2 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.

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

9. Protection from cyber attacks

9.1 Please see the glossary (appendix 6) to help you understand cyber security terminology.

9.2 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 statutory annual training for staff and Governors (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
  - Deal with requests for bank details, personal information or login details
  - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- 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 (such as 360safe.org.uk) annually, 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 and store these backups on cloud-based backup systems and a copy on internal systems.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to Southampton City Council (SCC) ICT Strategy Team.
- Make sure staff:
  - Enable multi-factor authentication where they can, on things like school email accounts
  - Store passwords securely using a password manager
- On rare occasions students will be permitted to use their mobile phone in ICT lessons to complete authentication when logging in as Microsoft now require two factor authentication.
- 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
- Develop, review and test an incident response plan with the IT department and SCC, for example, including how the school will communicate with everyone if communications go down, who will be contacted when, and who will notify Action Fraud of the incident. This will be reviewed and tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Work with SCC to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

10. Internet access

10.1 The school wireless internet connection is secured.

- Fortinet filtering is used
- There are WiFi separate connections for staff and pupils. Additionally, there is a Guest WiFi Access for Visitors to the School. This provides time limited or device limited access to the WiFi on a temporary basis.
- Filtering systems are not fool-proof. Inappropriate sites that the filter has not identified are reported to the network manager, as are sites that have been filtered in error. On Occasion some websites can be misclassified and can be blocked incorrectly. Users can request a unblock and which is assessed live by Fortinet.

10.2 Pupils

- WIFI access for pupils is only available on school devices with the exception of students with SEND where individual access is approved by the SENDCO.
- Temporary Guest WiFi access with a time limited voucher, may be provided in certain cases where a student needs to access the internet on their personal devices for school purposes, but only with permission from their Progress Leader

10.3 Parents and visitors

10.3.1 Parents and visitors to the school will be able to use the Guest WiFi by requesting a Guest WiFi Voucher from Reception. Parents and Visitors will not be permitted to use the school's Staff WiFi network unless specific authorisation is granted by the headteacher.

10.3.2 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)

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

11. Monitoring and review

11.1 The headteacher and network manager monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

11.2 This policy will be reviewed every 2 years.

11.3 The governing board is responsible for approving this policy.

12. Related policies

12.1 Adapt this list as required.

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

- Safeguarding and child protection policies
- Behaviour Policy and Statement of Behaviour Principles
- Staff Disciplinary Policy and Procedure
- Data Protection Policy
- Remote learning Policy

Appendix 1: Social Media cheat sheet for staff

Don't accept friend requests from pupils on social media

10 Guidelines for school staff on Social Media

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 Social Media apps from your phone. The apps recognise Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as parents or pupils)

*With the exception of school social media platforms.

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 to do 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 Facebook, Twitter and Instagram pages • Email/text groups for parents (for school announcements and information) 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 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 any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo
- 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:**

Signed (pupil):	**Date:**

Appendix 4: 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 • Leave a device unattended and unsecured without logging off or locking my device • 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 Network 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:**

Appendix 5: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber-attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.

TERM	DEFINITION
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.

Appendix 6: Student Portable Computer Issue Agreement

Name of Person Issued To:

Date Issued:

1. Introduction

This document comprises of the IT Security policy, acceptable usage policy and equipment loan agreement for portable or mobile computer systems as described below and supplied by the College IT Support department. Non-college purchased portable computers must be assessed prior to being connected to the St George network. Any devices that are used in the college to store data are covered within this policy.

For the sake of this document portable computers are defined as laptop, notebook, tablet computers and smart phones. This document works in conjunction with the main college's Acceptable ICT Use Agreement for Students which is subject to review.

Only authorised students are allowed access to and use of the Portable Computer Systems. Persons accessing data and using it for educational purposes should afford all material stored and processed on these systems adequate protection. Please consult IT Support for advice.

Failure to follow the procedures within this policy may result in disciplinary action.

2. Ownership of Equipment

Any portable computer issued to you under this policy remains the property of St George Catholic VA College.

On leaving the college or at the agreed end of loan, the college will require the portable computer and any accessories to be returned.

The college reserves the right to demand the portable computer be returned at any time. A maximum of 7 calendar days is acceptable between the request to return the portable computer and it being returned.

3. Physical /Hardware Security

The user of the portable computer should always adhere to the following guidelines:

- The portable computer must be securely locked away when not in use
- Portable computer security is your responsibility at all times
- Do not leave the portable computer unsecured and unattended in a public place; this includes areas within the college
- All computers should be logged off/locked when user is away from the devices
- Do not allow anyone else to use the portable computer
- Avoid leaving the portable computer within sight of ground-floor windows or within easy access of external doors, unless secured

4. Software Security

Software is installed on The Portable Computer System to aid learning. If users of Portable Systems require additional Software, they must request this with IT Support. All software must be fully licensed, obtained legally and will be installed by the IT Support either in school or remotely, with their approval.

The college reserves the right to inspect the portable computers at any time.

5. Virus and Spyware Control

The Portable Computer System will have an Anti-Virus software package installed by IT Support. Users are not to alter the configuration of this package unless express permission has been obtained from IT Support. The anti-virus system's database of virus definitions must be updated on a regular basis, each day if possible, but at least once a week. To update your virus definitions then it is necessary to connect to the network, either wired or over a wireless connection. This package has been installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files.

If a virus is discovered the following actions must be carried out:

- Turn the computer off
- Isolate any USB memory sticks, external hard drives or SD cards that have been used on that machine
- Inform IT Support as soon as possible

IT Support will have the software and technology available to eradicate any infections and recover infected files if possible.

6. Password Security

Password security is the responsibility of the individual. Passwords should be formulated in such a way that they are easily remembered but difficult to guess and should be formulated using letters (upper and lower case), figures and other characters.

- When allocated a new/temporary password for start-up use by IT Support the user must immediately change it
- Passwords must consist of a minimum of 6 characters and for strong passwords should also include 2 numerics as part of the 6 characters
- Passwords must not be shared amongst users. Any malicious or questionable activity detected under a user account will be attributed to the account owner
- Passwords must not be written down
- Passwords should not relate to the system or the user, although passwords must be easy to remember
- Passwords should be changed regularly, at intervals not exceeding 60 days
- Portable computers connected to the college network will have a password policy enforced on their devices.

7. Data Storage & Backup

It is the sole responsibility of the user to ensure any data stored on their device is backed up to a Cloud storage or other suitable storage media. IT Support is not responsible for any loss of data which has been stored locally on any device. IT Support are happy to advise users on available options, however, it is highly recommended for the users to utilize their Office 365 account to store data.

If work is lost it is unlikely that IT Support will be able to recover work from it without significant cost, which will be chargeable to the user.

8. Internet/e-mail

The portable computer has been provided by the organisation for use at college and at home. It should be noted that the Internet is an uncontrolled, unmanaged and largely unsupported global network. It is a source of much valuable information; however, it is also an unrestricted source of much illegal and illicit material. Additionally, it has a large recreational attraction.

Every computer issued has monitoring software which records all internet browser history, including website visited off site. If a concern is raised, the Network Manager will request the return of the portable computer to investigate further.

Please refer to the Acceptable ICT Use Agreement for pupils for further information.

9. Maintenance

- Please do not drop or bump your portable computer
- Please do not place heavy objects on the case
- Please do not touch the screen
- Do not use any other power pack than you were assigned
- Do not disassemble your portable computer
- Do not clean the portable computer with anything other than products specifically designed for use on computers. Please see IT Support for advice on this.
- Take care of accessories issued with the portable computer
- Always turn off your portable computer before storing it in its travelling bag for extended periods
- Avoid subjecting the portable computer to extremes of temperature, for example leaving it in a car during hot days or cold nights
- Please keep all liquids away from your portable computer
- Please do not continual leave your portable computer on charge, as this will shorten battery life. Allow the portable computer to run on battery power when possible.

Maintenance is to be controlled by IT Support in conjunction with external suppliers. Software is installed on all devices to enable IT Support to offer remote support and maintenance, however from time to time your portable computer will be recalled by IT Support for maintenance purposes. It may not be possible to properly support the portable computer until it has been returned for maintenance.

If the portable computer requires external repair, all data will be removed from the laptop ahead of repair.

10. Losses of Hardware or Data

All incidents that constitute a Loss of Hardware or Data should to be reported to the Network Manager. The Network Manager will instigate investigation procedures to try and establish the nature and potential threat of the incident.

Incidents could involve:

- Loss of Hardware
- Loss of Software/Data
- Virus attack
- Unauthorised access
- Misuse of System/Privileges
- Illegal software download

11. Portable Computer Information

Make:	
Model:	
St George Catholic College Asset Number:	
Serial Number or service tag:	
Additional Hardware Issued:	
Additional Serial numbers:	-
Intended Duration of loan	

12. Acceptance of policy

I have read and understood the St George VA College Portable Computer Issue Agreement and Acceptable Usage Policy detailed above and I agree to abide by the requirements laid down in it. I further acknowledge I have been issued the equipment itemised in section 11 of this document.

Student Name:

Student Signature:

Parent/Guardian Name:

Parent/Guardian Signature:

Approved By:

Approvers Signature:

Date:

Appendix 7: Student 4G Router Issue agreement

Name of Person Issued To:

Date Issued:

1. Introduction

This document comprises of the use and ownership of 4G Internet Router. This is issued under a loan agreement for a period agreed by The College and is intended for Educational use only.

2. Ownership of Equipment

The 4G Internet Router issued to you under this policy remains the property of St George Catholic VA College. On leaving The College or at the agreed end of Loan, The College will require the device to be returned.

3. Physical /Hardware Security

The device settings and configuration, including Username, passwords and SSID should not be changed. The user should not remove the SIM Card. All issues or configuration changes are to be made by IT Support.

4. Internet Access

The Personal Computer has been provided by the organisation for use at college and at home. It should be noted that the Internet is an uncontrolled, unmanaged and largely unsupported global network. It is a source of much valuable information; however, it is also an unrestricted source of much illegal and illicit material. Additionally, it has a large recreational attraction.

This 4G Router is provided by the College to allow the user access to Educational resources on the internet.

5. Maintenance

Please keep the device secure and do not leave unattended in an unsecured location. Avoid subjecting the device to extreme temperatures and keep away from liquids. Please do not continual leave device on charge, as this will shorten battery life. Use the battery whenever possible.

If you experience an issues please contact IT Support.

4G Internet Router

Make:	
Model:	
St George Catholic College Asset Number:	
Serial Number or service tag:	
SSID	
Password	
Intended Duration of loan	

6. Acceptance of policy

I have read and understood the St George VA College Student 4G Router Issue Agreement and Acceptable Usage Policy detailed above and I agree to abide by the requirements laid down in it. I further acknowledge I have been issued the equipment itemised in section 11 of this document.

Student Name:

Student Signature:

Parent/Guardian Name:

Parent/Guardian Signature:

Approved By:

Approvers Signature:

Date:

Appendix 8: Staff Portable Computer Issue Agreement

Name of Person Issued To:

Date Issued:

1. Introduction

1.1 This document comprises the IT Security policy, acceptable usage policy and equipment issue agreement for portable or mobile computer systems as described below and supplied by the College IT Support department. Non-College purchased Portable Computers must be assessed prior to being connected to the St George network. Any devices that are used in the College to store data are covered within this policy.

1.2 For the sake of this document Portable Computers are defined as Laptop, Notebook, Tablet computers and smart phones. This document works in conjunction with the main College's computer usage access agreement which is subject to review.

1.3 Only authorised persons are allowed access to and use of the Portable Computer Systems. Persons accessing data and using it for educational purposes should afford all material stored and processed on these systems adequate protection. Please consult IT Support for advice.

1.4 Failure to follow the procedures within this policy may result in disciplinary action.

2. Ownership of Equipment

2.1 Any Portable Computer issued to you under this policy remains the property of St George Catholic VA College.

2.2 On termination of employment or for extended absences, The College will require the Portable Computer and any accessories to be returned.

2.3 The College reserves the right to demand the Portable Computer be returned at any time. A maximum of 7 calendar days is acceptable between the request to return the Portable Computer and it being returned.

3. Physical /Hardware Security

3.1 The user of the Portable Computer should always adhere to the following guidelines:

a) The Portable Computer must be securely locked away when not in use.
b) Portable Computer security is your responsibility at all times.
c) Do not leave the Portable Computer unsecured and unattended in a public place; this includes areas such as the staff room and assembly halls.
d) All computers should be logged off/locked when user is away from the devices.
e) Do not allow students to use the Portable Computer.
f) Do not leave the Portable Computer in view inside of your car. Please lock it away in your car's boot.
g) Avoid leaving the Portable Computer within sight of ground floor windows or within easy access of external doors, unless secured.

4. Software Security

4.1 Users of Portable Systems are authorised and are able to load any software onto the Portable Computer system. All software must be fully licensed and obtained legally. All new software installations must be approved by IT Support. If you require advice or additional licensed software contact IT Support.

4.2 The College reserves the right to inspect the Portable Computers at any time.

5. Virus and Spyware Control

5.1 The Portable Computer System will have an Anti-Virus software package installed by IT Support. Users are not to alter the configuration of this package unless express permission has been obtained from IT Support. The anti-virus system's database of virus definitions must be updated on a regular basis, each day if possible, but at least once a week. To update your virus definitions then it is necessary to connect to the network, either wired or over a wireless connection. This package has been installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files.

5.2 If a virus is discovered the following actions must be carried out:

a) Turn the Computer off
b) Isolate any USB memory sticks, External Hard drives or SD Cards that have been used on that machine
c) Inform IT Support as soon as possible

5.3 IT Support will have the software and technology available to eradicate any infections and recover infected files if possible.

6. Password Security

6.1 Password Security is the responsibility of the individual. Passwords should be formulated in such a way that they are easily remembered but difficult to guess and should be formulated using letters (upper and lower case), figures and other characters.

a) When allocated a new/temporary password for start-up use by IT Support the user must immediately change it.
b) Passwords must consist of a minimum of 6 characters and for strong passwords should also include 2 numerics as part of the 6 characters.
c) Passwords must not be shared amongst users. Any malicious or questionable activity detected under a user account will be attributed to the account owner.
d) Passwords must not be written down.
e) Passwords should not relate to the system or the user, although passwords must be easy to remember.
f) Passwords should be changed regularly, at intervals not exceeding 60 days.
g) Portable Computers connected to the College network will have a password policy enforced on their devices.

7. Data Storage & Encryption

7.1 All sensitive data and pupil records wherever possible should not be stored on Portable Computers, and should remain within SIMS or on network drives.

7.2 Any external storage devices, such as USB memory sticks, external hard drives, SD cards, smart phones, tablets or storage media CD/DVDs should not store sensitive data or pupil details. These should only be used for backing up of resources.

7.3 If access to sensitive data is required off site, it is the responsibility of the user to ensure that the portable computer and storage is adequately encrypted and the above security and password procedures are strictly adhered to.

7.4 Windows Portable Computers are encrypted as standard. Apple Mac computers require the encryption feature, FileVault, to be turned on. Note that with this feature if the user forgets their password that data on the laptop is lost and unrecoverable.

7.5 If you require assistance or have any queries regarding encryption, please speak to IT Support.

8. Internet/e-mail

8.1 The Personal Computer has been provided by the organisation for use on and off site. It should be noted that the Internet is an uncontrolled, unmanaged and largely unsupported global network. It is a source of much valuable information; however, it is also an unrestricted source of much illegal and illicit material. Additionally, it has a large recreational attraction.

8.2 Every computer issued has monitoring software which records all internet browser history, including website visited off site. If a concern is raised, the Network Manager will consult SMT and permission to view the Internet history can only be given by the Headteacher.

8.3 Please see the College's policies covering Internet and Email usage.

9. Maintenance

a) Please do not drop or bump your Portable Computer
b) Please do not place heavy objects on the case
c) Please do not touch the screen
d) Do not use any other power pack than you were assigned
e) Do not disassemble your Portable Computer
f) Do not clean the portable computer with anything other than products specifically designed for use on computers. Please see IT Support for advice on this.
g) Take care of network cables and projector adapters as these connectors can be easily broken.
h) Always turn off your Portable Computer before storing it in its traveling bag for extended periods
i) Avoid subjecting the Portable Computer to extremes of temperature, for example leaving it in your car during hot days or cold nights
j) Please keep all liquids away from your Portable Computer.
k) Please do not continual leave your Portable Computer on charge, as this will shorten battery life. Allow the Portable Computer to run on battery power when possible.

9.1 Maintenance is to be controlled by IT Support in conjunction with external suppliers. Software is installed on all devices to enable IT Support to offer remote support and maintenance, however from time to time your Portable Computer will be recalled by IT Support for maintenance purposes. It may not be possible to properly support the Portable Computer until it has been returned for maintenance.

9.2 If the Portable Computer requires external repair, all data will be removed from the laptop ahead of repair.

10. Damages

10.1 All staff are personally liable for any breakages or damage to the Portable Computer issued to them, except in cases of unavoidable circumstances as determined by the College.

10.2 Any misuse or negligence resulting in damage to the Portable Computer may lead to the staff member or relevant department being charged for repair costs.

10.3 All damage must be reported as soon as possible to the Network Manager. Staff must also complete a detailed written report outlining how the damage occurred.

10.4 The College reserves the right to investigate any reported damages. Disciplinary actions may be taken in cases of proven misuse or negligence.

11. Backup

11.1 It is the sole responsibility of the user to ensure any data stored on their device is backed up to their OneDrive account, their network drive or other suitable storage media. IT Support is not responsible for any loss of data which has been stored locally on any device. IT Support are happy to advise staff on available options.

11.2 If work is lost it is unlikely that IT Support will be able to recover work from it without significant cost, which will be charged back to the department in question.

12. Losses and Confidentiality/Security Breaches

12.1 All incidents that constitute a Loss of Hardware or Data, which could potentially lead to a breach of Student or Staff confidentiality, are to be reported to the Network Manager. The Network Manager will instigate investigation procedures to try and establish the nature and potential threat of the incident.

12.2 Incidents could involve:

a) Loss of Hardware.
b) Loss of Software/Data.
c) Virus attack
d) Unauthorised access.
e) Misuse of System/Privileges.
f) Illegal software download

13. Accounting and Audit

13.1 The software and information held on Portable Computer Systems is subject to the same audit procedures as the desktop/tower Computer Systems. This also covers information and data stored on removable media e.g. floppy disks and USB pen or sticks.

14. Legislation

14.1 Users of portable systems must comply with current legislation regarding the use and retention of student information and use of computer systems.

14.2 These include, but are not limited to:

a) The General Data Protection Regulation (Regulation EU 2016/679)
b) The Data Protection Act, 2018 (subject to Royal Asset)
c) The Copyright, Designs and Patents Act, 1988.
d) The Computer Misuse Act, 1990.

15. Portable Computer Information

Make:	
Model:	
St George Catholic College Asset Number:	
Serial Number or service tag:	
Additional Hardware Issued:	
Additional Serial numbers:	

16. Acceptance of policy

I have read and understood the St George VA College Portable Computer Issue Agreement and Acceptable Usage Policy detailed above and I agree to abide by the requirements laid down in it. I also confirm that I will adhere to the E-Safety Policy. I further acknowledge I have been issued the equipment itemised in section 14 of this document.

Name:

Signature:

Approved By:

Approvers Signature:

Date: