



St Mary's Catholic Academy

Computer & Network Acceptable Usage Policy

Version: 2.0
Adopted: February 2024
Next Revision Date: February 2025

Introduction

St Mary's Catholic Academy maintains certain policies with regard to the use and security of its computer systems, including the network. All users expected to be familiar with these policies and consequences of violation as listed below.

Network Security and Privacy Policies

- All users should be aware that the academy monitors and filters internet access. Additionally the academy may also monitor file access, keystrokes and screen images.
- Unauthorised attempts to gain privileged access or access to any account or system not belonging to you on any academy system are not permitted
- Computer and network accounts provide access to personal, confidential data. Therefore, individual accounts cannot be transferred to or used by another individual. Sharing accounts or passwords is not permitted
- Each user is responsible for the proper use of his or her account and any activity conducted within it. This includes choosing safe secure passwords and protecting them accordingly
- No academy system or network may be used as a vehicle to gain unauthorised access to other systems
- Any user who finds a possible security lapse on any academy system or network must report it to the system administrators. To protect your files and the system, don't attempt to use a system under these conditions until a system administrator has investigated the problem
- All users should be aware that the system administrators conduct periodic checks of academy systems and networks, including password checks. Passwords must adhere to the academy password complexity requirements and any user found to have a weak password will be required to choose a secure password during the next login process
- User files on the academy servers are kept as private as possible. Attempts to read another person's protected files will be treated with the utmost seriousness. The system administrators will not override file protections unless necessary in the course of their duties, and will treat the contents of those files as private information at all times

Network and Computing Usage Policies

- No academy system or network may be used for any purpose or in a manner that violates academy regulations or constitutes a legal offence
- Please keep in mind that many people use academy systems and networks for daily work. Obstructing this work by consuming gratuitously large amounts of system resources (disk space, CPU time, print quotas and network bandwidth) or by deliberately crashing the machine(s) will not be tolerated
- Use of any academy system by outside individuals or organisations requires special permission from the Network Manager or technical team
- Use of academy systems or networks for commercial purposes, except where explicitly approved, is strictly prohibited
- Any attempt to vandalise or steal ICT equipment will be treated with the utmost severity
- Users must not attempt to use or install any software not authorised by the academy
- Copying, storing, displaying, or distributing copyrighted material using academy systems or networks without the express permission of the copyright owner, except as otherwise permitted under the copyright law, is prohibited

Portable Device Usage Policies

- Users must obtain permission from a system administrator before connecting any portable equipment to the network
- All laptops connecting to an academy domain must have the managed Anti-Virus client installed and configured to automatically update from the central update server. Any personal devices connecting to the Academy wireless network must have adequate Anti-Virus protection
- Users are permitted to configure their laptops for Internet access at home but are required to frequently connect to the academy network to ensure that they check in with the licence server and relevant updates are applied
- Devices provided to staff are for use by the assigned member of staff only and remain the property of the academy
- All devices provided to staff must be kept securely at all times. The expectation is that when not in use, including when taken home, that devices are locked away securely to prevent theft

Email Usage Policies

- No Email may be sent or forwarded through an academy system or network for an illegal or criminal purpose
- Electronic mail, like user files, is kept as private as possible. Attempts to read another person's electronic mail will be treated with the utmost seriousness. The administrators of email systems will not read mail unless necessary in their duties. Also, there may be inadvertent inspection in the ordinary course of managing and maintaining the computer network and in carrying out other day-to-day activities
- Users should be aware that their "deletion" of electronic information will often not erase such information from the system's storage until it is overwritten with other data and it may, in any case, still reside in the academy's network either on various backup systems or in other forms, and even if erased, may still exist in the form of printouts
- Nuisance E-mail messages or other online messages such as chain letters, obscene, harassing, or other unwelcome messages are prohibited
- Unsolicited emails to multiple users are prohibited
- The academy reserves the right to refuse Email and other connections from outside hosts that send unsolicited, mass or commercial messages, or messages that appear to contain viruses to specific academy or other users, and to filter, refuse or discard such messages.

Limitations of Liability

The academy is NOT responsible for any loss or damage to users' data or disks or for any other problems incurred as a result of using its ICT services, whether the cause originates with the user (for example, misuse of equipment, work left unattended, etc.) or from another source (for example, computer viruses, equipment malfunction, etc.).

Violations of these policies may result in the immediate suspension of computer accounts and network access pending investigation of circumstances and may lead to their eventual revocation. Serious violations of the policy will be referred directly to the appropriate authorities; unauthorised use of academy computing facilities can be a criminal offence. The penalties may be as severe as suspension, dismissal or exclusion for an individual and/or criminal prosecution.

Appendices 1 – Pupil Acceptable Use Policy for Older Pupils (Secondary Academy)

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the students/pupils to agree to be responsible users.

For my own personal safety

- I understand that the academy will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it. My passwords will be secure and using best practice with regards to complexity
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the academy systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the academy systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

- I recognise that the academy has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the academy.
- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the academy, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the academy community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could result in loss of access to the academy network, detentions, suspensions, contact with parents and in the event of illegal activities involving the police.

I must ensure when using my personal device for accessing any academy data that:

- The operating system and apps are fully supported by the vendor.
- Any software based firewalls are activated and configured correctly according to best practice
- All devices are receiving regular security updates, which includes updates for any applications
- Recommended password requirements are followed as outlined in the ICT Security Policy
- Anti-Malware/Virus software is installed and kept up to date