



# St Mary's Catholic Academy

## Computer and Network Use Policy

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

### ***Network Security and Privacy Policies***

1. All users should be aware that the Academy may use monitoring software that records all Internet access including SSL, file access, keystrokes and screen images.
2. Unauthorised attempts to gain privileged access or access to any account or system not belonging to you on any Academy system are not permitted.
3. 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.
4. Each user is responsible for the proper use of his or her account and any activity conducted with it. This includes choosing safe secure passwords and protecting them accordingly.
5. No Academy system or network may be used as a vehicle to gain unauthorised access to other systems.
6. 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.
7. All users should be aware that the system administrators conduct periodic checks of Academy systems and networks, including password checks. Any user found to have a weak password will be required to choose a secure password during the next login process.
8. 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***

9. No Academy system or network may be used for any purpose or in a manner that violates trust regulations or constitutes a legal offence.
10. 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.
11. Use of any Academy system by outside individuals or organisations requires special permission from the systems administrator.

12. Use of Academy systems or networks for commercial purposes, except where explicitly approved, is strictly prohibited.
13. Any attempt to vandalise or steal ICT equipment will be treated with the utmost severity.
14. Users must not attempt to use or install any software not authorised by the Academy.
15. 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***

16. Users must obtain permission from a system administrator before connecting any portable equipment to the network.
17. All laptops connecting to the 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.
18. 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.
19. Laptops provided to staff are for use by the assigned member of staff only and are provided subject to the conditions on the 'Laptop Loan Scheme' form.

#### ***Email Usage Policies***

20. No E-mail may be sent or forwarded through an Academy system or network for an illegal or criminal purpose.
21. 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 Academy and its 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.
22. 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.
23. Nuisance E-mail messages or other online messages such as chain letters, obscene, harassing, or other unwelcome messages are prohibited.
24. Unsolicited emails to multiple users are prohibited.
25. The Academy reserves the right to refuse E-mail and other connections from outside hosts that send unsolicited, mass or commercial messages, or messages that appear to contain viruses to 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 account 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 from the Academy and/or criminal prosecution.

## Google Apps Acceptable Use Policy

This Acceptable Use Policy (AUP) applies to all users of the Academy's Google Apps system. This policy should be considered part of the Acceptable Use Policy at St Mary's Catholic Academy. You should also read the Academy's Information Security Policy.

### General Principles

Use of the Google system is permitted and encouraged where such use is suitable for educational purposes and supports the goals and objectives of the Academy. Email is to be used in a manner that is consistent with the Academy's standards of business conduct and as part of the normal execution of an employee's job responsibility or student's role.

- Email is to be used for school related communication
- The use of computing resources is subject to UK law and any illegal use will be dealt with appropriately, for example, the Police can have a right of access to recorded data in pursuit of a crime.

### Unacceptable Use or behaviour:

It is unacceptable to;

- Send offensive or harassing email messages or content
- Send spam email messages or content
- Send email containing a virus or other malicious content
- Read email at inappropriate times, such as during class instruction
- Use the account of another person

### Users should:

- Try to check emails at least once per day
- Keep emails brief and use meaningful subject lines
- Re-read messages before sending to check for clarity and to make sure that they contain nothing which will embarrass the organisation or make it liable
- Understand how to use - and don't mismanage - CC and BCC: only CC in people that really need to receive the email
- Archive effectively - use folders (called labels in Gmail) and delete any messages you no longer need
- Take care when replying to emails previously sent to a group.
- Ensure your computer is locked or logged out when you leave your desk, a malicious user could send messages in your name.

## Monitoring

The Academy accepts that the use of email is an extremely valuable business, research and learning tool. However misuse of such a facility can have a detrimental effect on other users and potentially the Academy's public profile. As a result;

- The Academy maintains the right to access user email accounts in the pursuit of an appropriately authorised investigation
- The specific content of any transactions will not be monitored unless there is a suspicion of improper use.
- We are obliged to monitor to fulfil our responsibilities with regard to UK law.
- Action as deemed appropriate by the Head Teacher or Academy Governors may be taken.