Saint Ambrose College ICT Acceptable Use Policy

Approved	To be reviewed
January 2023	January 2024

ICT Acceptable Use Policy

1. Introduction

ICT is an integral part of the way our school works, and is a critical resource for students, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, our ICT resources and facilities also pose a risk to data protection, online safety and safeguarding. This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, students, 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 students about safe and effective internet and ICT use.

Breaches of this policy may be dealt with under our disciplinary policy and behaviour policy.

The College may use CCTV footage as evidence if required and can be used to support disciplinary action. This may include exclusion from the college, suspension, and contact with parents/carers and, in the event of illegal activities, involvement of the police.

2. Unacceptable use

2.1
The following actions are considered to be unacceptable use of ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings.

Staff and students must follow the following guidance:

Equipment

2.2
Never install, attempt to install or run programs of any type on the computers which have not been authorised by the school's Network Manager or Principal

2.3
Be respectful and do not intentionally damage ICT equipment. Damaging, disabling, or otherwise harming the operation of computers, or intentionally wasting resources, puts your work and the work of others at risk..

2.4
Only use the computers for educational purposes. Activities such as gaming, buying or selling goods are inappropriate.

2.5
Always check removable media (i.e. flash drives) with antivirus software before using them for school work, and only use if virus free.

2.6
Always check mobile equipment (e.g. laptops, tablet PCs, etc.) with antivirus software,

and ensure they have been found to be clean of viruses, before connecting them to the network or the Wi-Fi.

2.7
Protect the computers from spillages by eating or drinking well away from all the ICT equipment.

2.8
Treat the computers at school as you would at home.

Security and privacy
2.9
You are responsible for any activity logged on your account. Protect your work and yourself by keeping your password to yourself. Never use someone else's logon name or password and always log off at the end of your lesson/session.

2.10
Never use the computers to harass, harm, offend or insult other people. Under no circumstances should you delete another person's work.

2.11
To protect yourself and the systems, you should respect the security on the computers. Attempting to bypass or alter the settings may put you or your work at risk.

2.12
School staff might review your storage, files, removable media, devices and communications to ensure that you are using the system responsibly. Spot checks might be carried out.

Internet
2.13
You should access the Internet only for study or for school authorised/supervised activities.

2.14
Only access suitable material. Using the internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene, offensive or abusive is not permitted.

2.15
People you contact online are not always as they seem. Always be mindful of using the internet in a safe way. Never arrange to meet anyone.

2.16
Make sure you use all forms of social media in the appropriate manner inside and outside of school hours. The use of social media inside school is not permitted.

2.17
Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright and data protection laws.

Email
2.18
Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the internet as it is on the street.

2.19
Only open attachments if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.

2.20
If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report the message to a member of staff. The sending or receiving of an email containing content likely to be unsuitable for children or schools is strictly forbidden.

2.21
This is not an exhaustive list. The school reserves the right to amend this list at any time. The Principal 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.

2.22
Exemptions may be provided by the Principal if required for clear and explicit reasons, for example if an exemption would be required as part of an investigation.

2.23
New students will be asked to sign their acceptance of the guidance. This will remain in place throughout their time at Saint Ambrose.

3. Sanctions

3.1
Staff and students who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's behaviour policy or disciplinary polciy. Other sanctions in place for unacceptable ICT use include revoking permission to use the school's systems.

4. Access

4.1
The school's Network Manager manages access to the school's ICT facilities. That includes, but is not limited to computers, tablets and other devices and access permissions for certain programmes or files.

4.2
Staff and students will be provided with unique log-in and account information and passwords that they must use when accessing the school's ICT facilities.

4.3
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.

4.4
Supply teachers have limited and restricted access to the network and to Sims.

5. Email

5.1
Staff email accounts should be used for work purposes only. All work-related business should be conducted using the email address the school has provided.

5.2
Staff must not share their personal email addresses with parents and students, and must not send any work-related materials using their personal email account.

5.3
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.

5.4
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.

5.5
Staff must take extra care when sending sensitive or confidential information by email. Any external emails with attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

5.6
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.

5.7
If staff send an email in error which contains the personal information of another person, they must inform the Data Protection officer, Network Manager or Business Manager immediately.

6. Personal use

6.1
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. School may withdraw permission for it at any time or restrict access at their discretion.

6.2
Personal use is permitted provided that such use:

- Does not take place during teaching hours
- Does not constitute ‘unacceptable use’, as defined in section 2 of this policy
- Takes place when no students are present
- Does not interfere with their jobs, or prevent other staff or students from using the facilities for work or educational purposes.

6.3
Staff are also permitted to use their personal devices (such as mobile phones tablets) as long as the use meets the criteria outlined in section 6.2.

6.4
PE staff and staff who coach a sports team are permitted to use their personal device in order to take photographs of sports teams, for the sole purpose of using those pictures on social media or other relevant school marketing materials, such as the newsletter. Any photographs:

- Must be deleted from the device immediately after the image has been uploaded to social media
- Must not constitute unacceptable use as defined in section 2 of this policy.

6.5
Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

6.6
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 5.4). Where breaches of this policy are found, disciplinary action may be taken.

6.7
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 students and parents could see them.

7. Social media

7.1
The School has an official Facebook and Twitter page. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

8. Remote access

8.1
Staff who access the school's ICT facilities and materials remotely must do so in accordance with the school's Remote Learning Policy.

8.2
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 take such precautions as the Network Manager may require from time to time against importing viruses or compromising system security.

8.3
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.

9. Monitoring

9.1
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.

9.2
Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

9.3
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.

10. Search and deletion

School has the right to examine files and data found on confiscated items such as students' phones, computers and other devices. School will do so in accordance with the guidance contained within the DfE's document *Searching, Screening and Confiscation - Advice for schools,* released July 2022.

School has the right to examine files and data anywhere on its network and equipment.

School has the right to delete files and data from confiscated devices if the item being deleted is not likely to constitute an offence, is not needed for an investigation, and if the continued existence of the file or data would cause harm. At all times, deletion will be in accordance with the document referenced above, and with approval of the Principal or Designated Safeguarding Lead.

11. Passwords

11.1
All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

11.2
Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

11.3
Members of staff or students 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.

12. Software, firewalls, and antivirus

12.1
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.

12.2
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.

12.3
Any personal devices using the school's network must all be configured in this way.

13. Access

13.1
All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

13.2
These access rights are managed by the Network Manager.

13.3
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.

13.4
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.

14. Encryption

14.1
The school ensures that its devices and systems have an appropriate level of encryption.

14.2
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 Principal and if data taken out of school is encrypted.

14.3
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.