Trinity Catholic School – ICT Acceptable Use Policy

Guidelines for Staff

The school has provided computers for use by staff as an important tool for teaching, learning, and administration of the school. Use of school computers, by both members of staff and students, is governed at all times by the following policy. Please ensure you understand your responsibilities under this policy, and direct any questions or concerns to the IT Network Manager in the first instance.

All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. Deliberate abuse of the school's computer system may result in disciplinary action (including possible termination), and civil and/or criminal liability.

Please note that use of the school network is intended to be as permissive and flexible as possible under current UK legislation and DfE guidelines. This policy is not intended to arbitrarily limit the ways in which you can use the system, but to ensure compliance with the legal responsibilities of the school and staff, to safeguard the reputation of the school, and to ensure the safety of all users. Please respect these guidelines, many of which are in place for your protection.

Lastly, the school recognises that the distinction between computer use at work and at home is increasingly blurred, with many of us now using our own computers for work. While the school neither wishes nor intends to dictate how you use your own computer, staff should consider that the spirit of this policy applies whenever you are undertaking an activity that stems from your employment with the school.

Computer Security and Data Protection

- You will be provided with a personal account for accessing the computer system, with your own username and password. This account will be tailored to the level of access you require, and is for your use only. As such, **you must not disclose your password to anyone**, including IT support staff. If you do so, you will be required to change your password immediately.
- You **must not allow a student to have individual use of a staff account** under any circumstances, for any length of time, even if supervised.
- When leaving a computer unattended, you **must** ensure you have either logged off your account, or locked the computer to prevent anyone using your account in your absence.
- You **must not** store any sensitive or personal information about staff or students on any portable storage system (such as a USB memory stick, portable hard disk, or personal computer) unless that storage system is encrypted and approved for such use by the school.
- You **must not** transmit any sensitive or personal information about staff or students via email without the data being encrypted by a method approved by the school.
- When publishing or transmitting non-sensitive material outside of the school, you **must** take steps to protect the identity of any student whose parents have requested this.
- If you use a personal computer at home for work purposes, you **must** ensure that any school-related sensitive or personal information is secured to prohibit access by any non-member of staff, and encrypted to protect against theft.
- You **must** make your own backup of data kept on any storage system other than the network storage drives or your 'My Documents' folder. This includes USB memory sticks (even those owned or issued by the school) or a personal computer.
- You **must** ensure that items of portable computer equipment (such as laptops, digital cameras, or portable projectors) are securely stored in a locked room or cupboard when left unattended.
- Equipment taken offsite is not routinely insured by the school. If you take any school computer equipment offsite, you should ensure that adequate insurance cover has been arranged to cover against loss, damage, or theft.

Laptop Computers

Laptop computers are issued to all teaching staff and support staff as required. Laptops remain the property of Trinity Catholic School at all times and their usage is subject to the following guidelines:

- The equipment remains the property of Trinity Catholic School at all times and must be returned to the School at the end of the lease agreement or contractual period.
- Maintenance of the equipment is the responsibility of the Network Manager. All maintenance issues **must** be referred to the ICT department, through the usual channels.
- All installed software **must** be covered by a valid license agreement held by Trinity Catholic School.
- All software installation MUST be carried out by ICT Department in accordance with the relevant license agreements.
- No software should be removed, uninstalled or disabled under any circumstances. Any software problems should be reported through the usual support channels.
- Antivirus software must be updated regularly. For laptop computers, it will be necessary to connect them to the School network to update the antivirus software. *This should be done at least weekly*.
- Staff **must not** let students access their laptop unless agreed by the Principal or Network Manager even if they are using their own logon credentials.
- The user of the equipment is responsible for all personal files and data stored on the equipment. Backup of the data is the responsibility of the user. It is strongly recommended that all data is regularly backed up, either to a CDRW disk, a memory stick or to the school's network. Where removable media is used the user must ensure that these mediums have not been used to download materials that are at risk of damaging the network. It is recommended that the school's facility to transfer files is used.
- The user of the equipment must not encrypt any data or password protect any files so as to ensure future usage of the equipment.
- Trinity Catholic School cannot be held responsible for loss of data in the event of either a hardware or software failure or user error.
- From time to time, it may be necessary for ICT Department to perform software updates and maintenance for which the equipment must be made available in School when reasonably requested.

Personal Use

The school recognises that occasional personal use of the school's computers is beneficial both to the development of your IT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use

- **must** comply with all other conditions of this AUP as they apply to non-personal use, and all other school policies regarding staff conduct;
- **must not** interfere in any way with your other duties or those of any other member of staff;
- **must not** have any undue effect on the performance of the computer system; and
- **must not** be for any commercial purpose or gain unless explicitly authorised by the school.

Personal use is permitted at the discretion of the school and can be limited or revoked at any time.

Use of your own Equipment

- Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff, and **must not** be used until approved. This test must be performed at regular intervals as required by school's normal rules on electrical safety testing.
- You **must not** connect personal computer equipment to school computer equipment without prior approval from the IT Network Manager, with the exception of storage devices such as USB memory sticks.
- If you keep files on a personal storage device (such as a USB memory stick), you **must** ensure that other computers you connect this storage device to (such as your own computers at home) have an up-to-date anti-virus system running to protect against the proliferation on harmful software onto the school computer system.

Conduct

- You **must** at all times conduct your computer usage professionally, which includes being polite and using the system in a safe, legal and business appropriate manner. Among uses that are considered unacceptable are the following:
    - Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials;
    - Making ethnic, sexual-preference, or gender-related slurs or jokes.
- You **must** respect, and not attempt to bypass, security or access restrictions in place on the computer system.
- You **must** not intentionally damage, disable, or otherwise harm the operation of computers.
- You **must** make efforts not to intentionally waste resources. Examples of resource wastage include:
    - Excessive downloading of material from the Internet;
    - Excessive storage of unnecessary files on the network storage areas;
    - Use of computer printers to produce class sets of materials, instead of using photocopiers.
- You should avoid eating or drinking around computer equipment.

Internet Use

Use of the Internet should be in accordance with the following guidelines:

- Transmission of any material in violation of any United Kingdom or other national laws is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material or material protected by trade laws
- Do not allow a student access to your account to gain access to websites which are normally blocked to students.
- 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 or abusive is not permitted.
- Respect the work and ownership rights of people outside the School. This includes abiding by copyright laws.
- Do not access Internet chat sites. These represent a significant security threat to the School's network.
- The use of online gaming sites is prohibited. These consume valuable network resources that may adversely affect the performance of the system.
- Do not print out pages directly from a website. Web pages are often not suitably formatted for printing and this may cause significant wastage of paper. If you wish to use content from websites, consider using the copy and paste facility to move it into another application, copyright permitting.

- Do not attempt to download or install software from the Internet. The ICT department assumes responsibility for all software upgrades and installations.

Use of Social Networking websites and online forums

Staff must take care when using social networking websites such as Facebook, even when such use occurs in their own time using their own computer. Social Networking sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children.

You must not allow any student to access personal information you post on a social networking site. In particular:

- You **must not** add a student to your 'friends list'.
- You **must** ensure that personal information is not accessible via a 'Public' setting, but ensure it is set to a 'Friends only' level of visibility.
- You should avoid contacting any student privately via a social networking website, even for school-related purposes.
- You should take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them access to your personal information.

Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.

- Unless authorised to do so, you **must not** post content on websites that may appear as if you are speaking for the school.
- You should not post any material online that can be clearly linked to the school that may damage the school's reputation.
- You should avoid posting any material clearly identifying yourself, another member of staff, or a student, that could potentially be used to embarrass, harass, or defame the subject.

Use of Email

All members of staff with a computer account are provided with an email address for communication both internally and with other email users outside the school. The following considerations must be made when communicating by email:

- E-mail has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of e-mails may therefore have to be made available to third parties. You **must** be cautious when sending both internal and external mails. The professional standards that apply to internal memos and external letters must be observed for e-mail.
- E-mail to outside organisations has the same power to create a binding contract as hardcopy documents. Check e-mail as carefully as written contracts, always use a spell checker and, where appropriate, obtain legal advice before sending. You **must not** purchase goods or services on behalf of the school via e-mail without proper authorisation.

- All school e-mail you send should have a signature containing your name, job title and the name of the school.
- E-mail is not a secure method of communication, and can be easily copied, forwarded and archived. Unless explicitly authorised to do so, you **must not** send, transmit, or otherwise distribute proprietary information, copyrighted material, trade secrets, or other confidential information belonging to the school.
- Having an external e-mail address may lead to receipt of unsolicited e-mail containing offensive and/or sexually explicit content. The school will take measures to minimise the receipt and impact of such content, but cannot be held responsible for material viewed or received by users from the Internet.
- You must not send chain letters or unsolicited commercial e-mail (also known as SPAM).

Supervision of Student Use

- Students **must** be supervised at **all** times when using school computer equipment. When arranging use of computer facilities for students, you must ensure supervision is available.
- Supervising staff are responsible for ensuring that the separate Acceptable Use Policy for students is enforced.
- Supervising staff **must** ensure they have read and understand the separate guidelines on e-safety, which pertains to the child protection issues of computer use by students.

Privacy

- Use of the school computer system, including your email account and storage areas provided for your use, may be subject to monitoring by the school to ensure compliance with this Acceptable Use Policy and applicable laws. This may include remote monitoring of an interactive logon session. In particular, the school does keep a complete record of sites visited on the Internet by both students and staff, however, usernames and passwords used on those sites are NOT monitored or recorded.
- You should avoid storing sensitive personal information on the school computer system that is unrelated to school activities (such as personal passwords, photographs, or financial information).
- The school may also use measures to audit use of computer systems for performance and diagnostic purposes.
- **Use of the school computer system indicates your consent to the above described monitoring taking place.**

Confidentiality and Copyright

- Respect the work and ownership rights of people outside the school, as well as other staff or students.
- You are responsible for complying with copyright law and licenses that may apply to software, files, graphics, documents, messages, and other material you wish to use, download or copy. Even if materials on the school computer system or the Internet are not marked with the copyright symbol (©), you should assume that they are protected under copyright laws unless there is an explicit permission on the materials to use them.
- You **must** consult a member of IT Network staff before placing any order of computer hardware or software, or obtaining and using any software you believe to be free. This is to check that the intended use by the school is permitted under copyright law (as well as to check compatibility and discuss any other implications that the purchase may have). Do not rely on the claims of suppliers, who do not have specific knowledge of the school's systems.
- As per the standard staff contract, any invention, improvement, design, process, information, copyright work, trade mark or trade name made, created or discovered by you during the course of your employment in any way affecting or relating to the business

of the School or capable of being used or adapted for use within the School shall be immediately disclosed to the School and shall to the extent permitted by law belong to and be the absolute property of the School.
- By storing or creating any personal documents or files on the school computer system, you grant the school a non-exclusive, universal, perpetual, irrevocable, and royalty-free license to use, copy, and distribute those documents or files in any way the school sees fit.

Reporting Problems with the Computer System

It is the job of the IT Network Manager to ensure that the school computer system is working optimally at all times and that any faults are rectified as soon as possible. To this end:

- You should report any problems that need attention to a member of IT support staff as soon as is feasible. Problems that seriously hinder your job or teaching and require immediate attention should be reported by telephone; any other problem **must** be reported via email.
- If you suspect your computer has been affected by a virus or other malware, you **must** report this to a member of IT Network staff **immediately**.
- If you have lost documents or files, you should report this as soon as possible. The longer a data loss problem goes unreported, the lesser the chances of your data being recoverable (mere minutes can count).

Reporting Breaches of this Policy

All members of staff have a duty to ensure this Acceptable Use Policy is followed. You **must** immediately inform the Network Manager, or the Principal, of abuse of any part of the computer system. In particular, you should report:

- any websites accessible from within school that you feel are unsuitable for staff or student consumption;
- any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc;
- any breaches, or attempted breaches, of computer security; or
- any instance of bullying or harassment suffered by you, another member of staff, or a student via the school computer system.

Reports should be made either via email or phone call. All reports will be treated confidentially.

Review and Evaluation

This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff.

Notes

1. "Sensitive personal information" is defined as information about an individual that is protected by law under the Data Protection Act 1998. Examples of such data include addresses and contact details of individuals, dates of birth, and student SEN data. This list is not exhaustive. Further information can be found in the school's Data Protection Policy.