

Acceptable Use Policy

INFORMATION AND COMMUNICATIONS TECHNOLOGY USE

St. Colmcille's Community School
Administrative Policy

1. **PURPOSE**

St. Colmcille's Community School owns and operates a variety of computing systems, which are provided for the use of St. Colmcille's Community School students, faculty, life long learners and staff in support of the programs of the school and are to be used for education, research, academic development, and public service only. All users of these systems are responsible for seeing that these computing facilities are used in an effective, efficient, ethical, and lawful manner.

This document establishes rules and prohibitions that define acceptable use of these systems. Unacceptable use is prohibited, and is grounds for loss of computing privileges, as well as discipline or legal sanctions.

This document establishes the need for an ICT Development Officer and an ICT Coordinating Committee. The task of this committee is to:

- Set hardware and software purchasing plans, secure an annual budget and provide an annual budget breakdown
- Ensure that there is an ongoing program of staff development and support.
- Regularly review hardware, software and ICT training needs.
- Co-ordinate where necessary with resource leaders in other curriculum areas, particularly in respect to software purchases.

The position of ICT Development Officer may be established and filled in line with the scheme of school needs. If not, the position of ICT Development Officer will be filled by agreement amongst the ICT Coordinating committee at the beginning of the academic year. Preferably all members of said committee will be teaching ICT at any level in the academic year. The Principal or other staff member designated by him / her will be a member of the committee. The Adult Education Officer, or the Deputy Officer due to the nature of his or her involvement in providing access to ICT evening classes, will also be part of the ICT Coordinating Committee. The ICT technician will have the option of attending meetings if s/he should so wish.

2. **AUDIENCE AND AGREEMENT**

All users of St. Colmcille's Community School computing systems must read, understand, and comply with the policies outlined in this document, as well as any additional guidelines established by the Information Technology Department. Such guidelines will be reviewed by the ICT Development Officer and may become subject to Board approval as a policy or procedure to be included in the school plan. BY USING ANY OF THESE SYSTEMS, USERS AGREE THAT THEY WILL COMPLY WITH THESE POLICIES.

3. **RIGHTS**

These computer systems, facilities, and accounts are owned and operated by St. Colmcille's Community School. St. Colmcille's Community School reserves all rights, including termination of service without notice, to the computing resources that it owns

and operates. These procedures shall not be construed as a waiver of any rights of the school, nor shall they conflict with applicable acts of law.

4. **PRIVILEGES**

Access and privileges on St. Colmcille's Community School computing systems are assigned and managed by the ICT Development Officer. Eligible individuals may become authorized users of a system and be granted appropriate access and privileges by following the approval steps prescribed for that system by the ICT coordinating committee.

The ICT Development Officer must approve all access to the School's computer resources, including the issuing of accounts and related passwords.

Users may not, under any circumstances, transfer or confer these privileges to other individuals. Others shall not use any account assigned to an individual without express permission from the ICT Development Officer. The authorized user is responsible for the proper use of the system, including any password protection.

5. **RESPONSIBILITIES**

Users are responsible for maintaining the following:

a) An environment in which access to all School computing resources are shared equitably between users. The ICT Development Officer along with the ICT coordinating committee sets minimum guidelines within which users must conduct their activities.

b) An environment conducive to learning:

A user who brings food or drink into the computer rooms will be asked to leave and privileges may be removed.

Disruptive behaviour will not be tolerated in any form. If any arises, the user responsible will be asked to close down their terminal and will be given alternative written work to complete at that time.

A user who harasses, or makes defamatory remarks, shall bear full responsibility for his or her actions. Further, by using these systems, users agree that individuals who transmit such remarks, to or from the school, shall bear sole responsibility for their actions. Users agree that St. Colmcille's Community School's role in managing these systems is only as an information carrier, and that they will never consider transmission through these systems as an endorsement of said transmission by St. Colmcille's Community School.

Some of the St. Colmcille's Community School computing systems provide access to outside networks, both public and private, which furnish electronic mail, information services, bulletin boards, conferences, etc. Users are advised that they may encounter material that may be considered offensive or objectionable in nature or content. Users are further advised that St. Colmcille's Community School does not assume responsibility for the contents of any of these outside networks.

The user agrees to comply with the acceptable use guidelines for whichever outside networks or services they may access through St. Colmcille's Community School systems.

Further, the user agrees to follow proper etiquette on outside networks. Documents regarding etiquette are available through the ICT Development Officer.

The user agrees never to attempt to transmit, or cause to be transmitted, any message in which the origination is deliberately misleading (except for those outside services which may conceal identities as part of the service). The user agrees that, in the unlikely event that someone does transmit, or cause to be transmitted, a message that is inconsistent with an environment conducive to learning or with a misleading origination, the person who performed the transmission will be solely accountable for the message, not St. Colmcille's Community School, which is acting solely as the information carrier.

c) An environment free of illegal or malicious acts:

The user agrees never to use a system to perform an illegal or malicious act. Any attempt to increase the level of access to which (s) he is authorized, or any attempt to deprive other authorized users of resources or access to any St. Colmcille's Community School computer system shall be regarded as malicious, and may be treated as an illegal act.

The user agrees to be bound by the terms and conditions laid down in the **Data Protection Act of 1988** and the **Freedom of Information Act of 1997** and to inform themselves of their rights as citizens and their responsibilities under said acts.

Other legal / sector specific requirements need to be satisfied under the list of applicable Irish Laws as laid down in Appendix A of this document. All users agree to abide by the terms and conditions of these applicable Irish Laws.

d) A secure environment;

When not in use the doors to the computer rooms must be kept locked.

No user is permitted to use removable storage media that have originated outside of St. Colmcille's Community School. Storage solutions will be issued by the School, if needed.

Any user who finds a possible security lapse, or technical difficulty, on any system is obliged to report it to the ICT Development Officer. The system must not be used until the ICT Development Officer has investigated the problem.

Knowledge of passwords or of loopholes in computer security systems shall not be used to damage computing resources, obtain extra resources, take resources from another user, gain unauthorized access to resources or otherwise make use of computing resources for which proper authorization has not been given.

Users are responsible for backup of their own data. The ICT Development Officer may from time to time schedule an overhaul and clean up of the network. File owners will be notified of this necessary maintenance, in advance, if such notice is practical.

All users must become familiar with logging off the system and must do so at the end of every session. If so asked by their teacher, users must ensure that all systems are shut down, though the proper means, when they are finished using them.

6. **ACCOUNTS**

Accounts will be issued and revoked solely by the ICT Development Officer. Others must not use an account assigned to an individual without express permission from the ICT Development Officer. The individual is responsible for the proper use of the account, including proper password protection.

The user is responsible for all work carried out through and transmitted to and from the account issued and for maintenance of files and folders created within said account.

7. **CONFIDENTIALITY**

Programs and files are confidential unless they have been made available, with written permission, to other authorized individuals. The ICT Development Officer reserves the right to access all information stored on computers other than those used by senior management. File owners will be notified of file access and/or maintenance, in advance, if such notice is practical. When performing maintenance, every effort is made to insure the privacy of a user's files. However, if policy violations are discovered, they will be reported immediately.

8. **SYSTEM USAGE**

Users must be aware that all their computer activity is tracked and logged for reference purposes. These individual user logs may be accessed at any time by the ICT Development Officer. If policy violations are discovered they will be reported immediately.

Electronic communications facilities (such as E-MAIL) are for school related activities only. Fraudulent, harassing or obscene messages and/or materials are not to be sent or stored.

The computer facilities may be used during out of class times by any student who has been deemed competent in computer usage by a member of the ICT coordinating committee.

Staff may use either of the Computer Rooms with their class group(s) during class time provided the appropriate class period(s) are recorded via the booking procedures in force at that time. Scheduled and timetabled ICT classes take precedence over all other sessions.

9. **SYSTEM PERFORMANCE**

No one should deliberately attempt to degrade the performance of a computer system or to deprive authorized personnel of resources or access to any school computer system.

10. **UNAUTHORIZED ACCESS**

Loopholes in computer security systems or knowledge of a special password should not be used to damage computer systems, obtain extra resources, take resources from another user, gain access to systems or use systems for which proper authorization has not been given.

11. **COPYRIGHT**

Computer software protected by copyright is not to be copied from, into, or by using St. Colmcille's Community School computing facilities, except as permitted by law or by the contract with the owner of the copyright. This means that such computer and microcomputer software may only be copied in order to make back-up copies, if permitted by the copyright owner. The number of copies and distribution of copies may not be done in such a way that the number of simultaneous users in a department exceeds the number of original copies purchased by that department.

12. **VIRUS PROTECTION**

Computer viruses are items of software that attach themselves to other legitimate items of software or data, without the consent of the computer user, and are programmed to proliferate themselves onto other computers, often to cause disruption or damage. It is essential that all users play a part in protecting the network from the presence of viruses.

It is the policy of the school to run up to date virus protection software on all computers that are attached to the network. This software will automatically report the presence of most known viruses. Any user who receives an on-screen warning from this software (these are very clear and explicit) should stop all use of the computer immediately and report the occurrence to the ICT Development Officer or the ICT Technician.

Viruses can attach themselves easily to removable storage media and this is one of the main ways in which they proliferate. The software used to prevent students from tampering with various computer settings will also, to some extent, prevent them from accessing these removable media. However this is not totally secure. Furthermore there are instances in which students and staff will want to transfer data to and from the network on removable media, e.g. as a means of submitting homework. To allow for this and still ensure system security it is the school's policy that all removable media must be virus scanned before being accessed through any computer on the network. These must be re-scanned again each time they are used in computer outside the network. Please give reasonable notice to system administrators if scanning is needed.

13. VIOLATIONS

An individual's computer use privileges may be suspended immediately upon the discovery of a possible violation of these policies. Such suspected violations will be confidentially reported to the ICT Development Officer.

The Principal may nominate the ICT Development Officer to conduct an examination of computing systems at any time and without prior notice to assure compliance with internal policies, assist with internal investigations, and assist with the management and protection of the schools information resource systems.

Violations of these policies will be dealt with in the same manner as violations of other school policies and may result in disciplinary action. In such a review, the full range of disciplinary sanctions is available including the loss of computer use privileges, dismissal from the school, Garda involvement and legal action. Violations of some of the above policies may constitute a criminal offence.

14. ST. COLMCILLE'S COMMUNITY SCHOOL STRATEGY

The school will employ a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

AUP Forms

All users will be presented with an appropriate acceptable use policy document in line with their role in the school. These forms must be read carefully, signed and returned to the ICT Development Officer where they will be filed securely. Once these forms have been signed returned, the user will have access to the computing systems in operation throughout the school.

General

Internet sessions will always be supervised by a teacher.

Uploading and down loading of non-approved software will not be permitted.

Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material. Filtering software and / or equivalent systems will be fully explained to all users.

The school expects all parents / guardians to engage in teaching their children about responsible use of the Internet.

The school will regularly monitor students' Internet usage.

Students and teachers will be provided with training in the area of Internet safety.

Virus protection software will be used and updated on a regular basis.

The use of personal removable storage media in school requires a teacher's permission.

Users will observe good "netiquette" (i.e., etiquette on the Internet) at all times and will not undertake any actions that may bring the school into disrepute.

World Wide Web

Users will not visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.

Users will use the Internet for educational purposes only.

Users will be familiar with copyright issues relating to online learning.
Users will never disclose or publicise personal or school information especially on sites requiring e-commerce transactions.
Users will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.

Email

Teachers will use approved school email accounts when communicating professionally with other partners in education or other significant bodies regarding school or educational business.

Students will use approved class email accounts under supervision by or permission from a teacher and these school accounts must be used when communicating approved work to or from the school.

Non-school related business should be conducted using a non-school email account.

Students will not send or receive any material that is illegal, obscene, or defamatory or material that is intended to annoy or intimidate another person.

Students will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.

Students will never arrange a face-to-face meeting with someone.

Sending and receiving email attachments is subject to permission from their teacher.

Internet Chat

Students will only have access to chat rooms, discussion forums or other electronic communication forums that have been approved by, or set up by, the school.

Chat rooms, discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised.

Usernames will be used to avoid disclosure of identity.

Face-to-face meetings with someone organised via Internet chat is strictly forbidden.

School Website

We are privileged to have a portal on the World Wide Web that gives interested parties an insight into the life of St. Colmcille's. It will exist at <http://www.stcolmcilles.ie>. It is envisaged that our students will contribute to the site and they will be given the opportunity to publish projects, artwork or school work on the World Wide Web.

The publication of student work will be co-ordinated by a teacher.

Students' work will appear in an educational context on Web pages with a copyright notice prohibiting the copying of such work without express written permission.

Digital photographs, audio or video clips of individual students will not be published on the school website without parental permission. Most photographs, audio and video clips featured on the school website will focus on group activities. Video clips may be password protected.

Personal student information including home address and contact details will be omitted from school web pages.

Students will continue to own the copyright on any work published.

Legislation

The school will provide information on the following legislation relating to use of the Internet which teachers, students and parents should familiarise themselves with:

Child Trafficking and Pornography Bill 1997

1993 Interception Act
Video Recordings Act 1989
The Data Protection Act 1988
Freedom of Information Act 1997

Support Structures

The school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of the Internet.

Sanctions

Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities, to involve the Gardai and other legal bodies should the need arise in the case of a serious breach of this AUP.

Parents may be asked to furnish the school with the IP address of any home internet account that is used in a malicious or offensive manner regarding communications to or from the school. This IP address will be used in order to establish beyond reasonable doubt the origin of said malicious or offensive material.

15. ADDITIONAL GUIDELINES

The ICT Development Officer together with the coordinating committee will establish more detailed guidelines, as needed, for specific computer systems and networks. These guidelines will cover other items related to administration and implementation of a system that offers a first class learning experience to all users.

16. ANNUAL REVIEW

The aim of this Acceptable Use Policy is to ensure that all users will benefit from learning opportunities offered by the school's Internet resources in a safe and effective manner. Internet use and access is considered a school resource and privilege. It is envisaged that school and parent representatives will revise the AUP annually.

This version of the AUP was created on:

and was ratified by the Board of Management of St. Colmcille's Community School on:

Signed:

ICT Development Officer

Principal