



Internet Acceptable Use Policy

Student Use

Students may use the Internet to participate in distance learning activities, to ask questions of and consult with experts, to communicate with other students and individuals, and to locate material to meet their educational and personal information needs.

College staff acknowledge the need to help students develop the intellectual skills needed to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use information to meet their educational goals.

With worldwide access to computers and people also comes the availability of material that may not be considered of educational value. On a global network, it is impossible to control all materials, and a user may discover inappropriate material. Southern Cross Catholic College believes the educational value of the information and interaction available on this worldwide network outweighs the risks users may procure material that is not consistent with the educational goals of the College.

Student network users have been granted the privilege of accessing the Internet to facilitate educational growth in technology, information gathering skills, and communication skills.

Acceptable Use:

The purpose of the network connection to the Internet is to support research and education in and among academic institutions in Australia and the world by providing access to unique resources and the opportunity for collaborative work. The use of an Internet account must be in support of education and research and consistent with the educational objectives of the College. Transmission of any material in violation of any Australian Federal or State regulation is prohibited. This includes, but is not limited to:

- copyrighted material
- threatening or obscene material
- material protected by trade secret.

Privileges:

The use of the Internet is a privilege, not a right, and inappropriate use will result in cancellation of those privileges. The Administration will deem what is inappropriate use and that decision is final. Also, the Information Technology Coordinator may close an account any time as required while any breach of this policy is investigated. Administrators, faculty, and staff may request the Information Technology Coordinator to deny, revoke, or suspend user accounts.

Student Responsibilities

The use of a student account must be in support of their education and consistent with the educational objectives of the College.

While exercising their privileges to use the Internet as an educational resource, they shall also monitor and accept the responsibility for all material received. Student users are not to use the network for wasteful or frivolous purposes.

Student users:

- have the responsibility of keeping all pornographic material, inappropriate text files, or files dangerous to the integrity of the network from entering the school via the Internet, and to report all violations
- are responsible for maintaining the integrity of the electronic mail system
- are to be responsible for all mail received
- are to make only those contacts leading to some justifiable educational growth
- are to not knowingly receive electronic mail containing pornographic material, inappropriate information, or text-encoded files that are potentially dangerous to the integrity of the hardware on school premises
- are to report all inappropriate materials (solicited or unsolicited) to the supervising staff member.

Student users may not:

- copy, change, or transfer any software provided by the school, faculty, or another student without permission from the originator
- copy copyrighted software owned by Southern Cross Catholic College. It is generally illegal to copy any software which has a copyright. The use of illegally copied software is considered a criminal offence and is subject to criminal prosecution
- intentionally introduce a computer virus
- deliberately use the computer to annoy or harass others, eg making accessible any obscene, abusive, or threatening messages or sending offensive, racist or sexist messages
- intentionally damage the system, damage information not belonging to you, misuse system sources, or allow others to misuse system sources
- tamper with equipment except as directed by the teacher
- use the network for financial or commercial gain
- attempt to bypass network security
- disclose their home address, telephone number, credit card or PIN number
- allow anyone else to use their account or give their password to anyone else
- use another student's account or tamper with their account
- bring Southern Cross Catholic College into disrepute
- use the Internet for political purposes

All files and programs on the computer belong to someone. Student users may not erase, modify, rename, or make unusable anyone else's files or programs.

Student users are expected to abide by the generally accepted rules of network etiquette. These include the following:

- being polite, ie not writing or sending abusive messages to others
- using appropriate language, ie not swearing, using vulgarities or any other inappropriate language
- not revealing personal address or phone number or those of students or colleagues
- accepting that electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to all mail and messages relating to or in support of illegal activities may be reported to the authorities.

Misuse of Privileges and Consequences

All users are held responsible for their actions and activity, as outlined in the Responsibilities Section. Unacceptable use of the network in any instance will result in the suspension of all user privileges while the matter is investigated by the Administration, Information Technology Coordinator and the Network Manager. Reinstatement of privileges will be made at the discretion of the Administration.

Security on any computer is a high priority, especially when the system involves many users. If any user feels he/she can identify a security problem on the Internet, the Information Technology Coordinator or Network Manager must be notified. Users should not demonstrate the problem to other users. Users should not use another individual's account without written permission from that individual. Attempts to logon to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history or problems with other computer systems may be denied access to the Internet.

Vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet, or any of the other networks that are connected to the internet backbone. This includes, but is not limited to, the uploading or creation of computer viruses, and also includes the unauthorised deletion of computer system or application software.

All instances of breeches of security and vandalism will be strictly dealt with. This initially will mean loss of Student Privileges and other action as deemed necessary by the Administration.

Students are advised the E-Mail and/or Internet correspondence is not privileged or confidential. From time to time, communications may be monitored by the Information Technology Coordinator and Network Manager to assure that Internet use is in support of the College's goals.