

USE OF COMPUTING FACILITIES

401.03

POLICY AUTHORISED BY <i>Sue A Slavin, Managing Director</i>	POLICY AUTHOR/OWNER <i>Manager Information Systems</i>	POLICY REVIEW RESPONSIBILITY <i>Manager Information Systems</i>
CURRENT VERSION DATE <i>December 2004</i>	POLICY REPLACES <i>Use Of Computing Facilities (1 Aug 1997)</i>	DATE OF NEXT REVIEW <i>January 2006</i>

1 Policy

1.1 Policy Statement

All staff and students accessing College computer networks, equipment or systems are responsible for use according to the following policies and the College Code of Conduct, regardless of whether the use is on or off site.

Acceptance of a Login to the West Coast TAFE computing network, or utilising College computing facilities in any way, implies acceptance of these policies.

This policy document is to be accessible to staff via the Staff Intranet – within both the resources and online induction components, and to students via the Student Portal and the main Student Intranet webpage, which is displayed at network login time.

1. Users must keep the password(s) associated with a College login(s) private, and not divulge it to any person, have easily accessible or allow any other person to use their personal login.
2. Use only your College login, and do not attempt to gain access to another user's login or account, in any other way. Use of other users' accounts, a false identity or another person's identity to gain access to any aspect of College facilities is prohibited.
3. Users will not load, store, copy, disclose, transfer or use any computer software or software application on the computing and communications facilities provided by the College in such a way as to breach any right of any person (including copyright) without the express written permission of the Information Systems Manager or Director, Business Support Services.
4. Users may utilise only those facilities to which they have been given specific access, or which have been advertised for general usage, and to the extent and in the manner that they are authorised to use them.
5. Users will not copy, disclose of, transfer, delete, examine, rename, change or add to software, data or information belonging to the College or another person

unless permission has been granted or the software, data or information is clearly intended to be public.

6. College computing facilities must not be used for any commercial purpose, other than that approved by the College.
7. The College wishes to maintain a secure, efficient computing and communications environment. It has the right to examine all computer files and to monitor computer usage to ensure compliance with these rules.
8. If necessary computer processes that are actively causing a problem will be terminated, or access to any files related to a breach of the rules removed.
9. Users will not change any software or hardware configuration of any computing equipment. If changes are required contact the College IT Help Desk.
10. The College reserves the right to withdraw the availability of any computing or communications facility without notice.
11. Tampering with other users' accounts in any way, including attempting to thwart the system security, setting password traps, and any other behaviour designed to interfere with other users' access to the facilities is prohibited.
12. Circumventing, or attempting to circumvent security or obtaining or attempting to obtain information that would allow security to be circumvented, is prohibited.
13. Users must comply with any directions from authorised IT staff of West Coast TAFE.
14. All items of computing equipment are the property of the College and may be relocated if required to enhance the overall deployment of IT services within the College. All computing equipment relocations must be arranged via the IT Help Desk and Finance provided with the asset number and new location. This includes any authorised borrowing or offsite usage.
15. Storage media of any form, not provided by the College or last accessed outside the College's computing environment, must not be introduced into the College computing environment without first checking for viruses.
16. Users must not deliberately or negligently interfere with the operation or performance of a system by:
 - Generating excessive load, use of storage capacity, network traffic, etc.
 - Physically damaging or adjusting the equipment. Any such tampering, vandalism, theft or wilful and/or reckless damage may be referred to the police.
 - Introducing viruses or other software components designed to interfere with the normal operation of a system.
 - Deleting, adding or modifying information relevant to the system's operation.
 - Obtaining extra resources without authorisation.
 - Excessive printing. Use of printers is limited to output of material related to academic programs (students) or related to normal job functions (staff).
 - Creating excessive network links.

- Playing games, running non-course (student) or non-work (staff) specific applications.
- Using the Internet to download non-course related (students) or non-work related (staff) files, including but not limited to music, movie and picture files.
- Using the Internet to access non-course related (students) or non-work related (staff) chat-rooms, radio broadcasts or similar.

17. College facilities are not to be used for:

- The deliberate or negligent accessing, preparing, storing, displaying of racist, pornographic or other offensive material,
- The deliberate receiving or transmitting of racist, pornographic or other offensive material unless it is a requisite component of a course of study and has the approval of the relevant lecturer (student) or manager (staff).
- The deliberate receiving or transmitting of material (whatever form) protected by copyright, prohibited by legislation, or of an obscene or threatening nature.

18. Students are not to assist persons who do not normally have access to a resource or unauthorised information to obtain such access.

19. Smoking, eating or drinking in computer laboratories or while using College student computing facilities, is prohibited. Likewise behaviour that impacts adversely on other users in shared spaces, such as making unreasonable noise.

20. Users must operate within the disk storage, file size and file age limits set by the College.

21. Non College devices must not be connected to the College network, except where prior (written) approval has been provided by the Information Systems Branch.

22. Users found in breach of these policies are liable to disciplinary action. Disciplinary action could result in a warning, a reprimand, suspension of computing facilities access, or exclusion from the College or course of study (students), and / or Police notified.

1.2 Objective/s

The objective of West Coast TAFE's policy is to facilitate the use of information resources by the provision of appropriate and timely technology solutions and technical assistance, and a key strategy of the College Business Plan is to use information technology in support of the educational, research and administrative activities of the College.

Making information technology more readily available contributes significantly to improving academic quality and student access.

While at West Coast TAFE, staff and students are responsible for ensuring that their use of computing and communications facilities is ethical and lawful. They are responsible for ensuring that their actions are not detrimental to the property of the College and the rights of others.

The aim of this policy is to ensure responsible use by all staff and students of all computing facilities owned and managed by the College.

1.3 Definitions, Terms and Acronyms

1.3.1 "account" refers to any computing or electronic communication resource allocated for sole or shared usage by a staff member or student and protected from general usage by a security system. Such a resource might include, but is not limited to, storage space; access to a computer terminal; processor time; printed output or dial-up access time. A security system might include, but is not limited to, password protection.

1.3.2 "computing facilities" refers to: (a) all networked services and computer hardware (and including fax machines and telephones) and software, owned, leased or used under licence by the College including the College's student, academic and administrative systems; (b) computing facilities maintained by other bodies but available for use through an agreement or agreements with the College; and (c) all other computing facilities, wherever situated, where access is by means of College-provided services.

1.3.3 "user" means any person or persons (eg staff / students / third-parties) utilising, accessing or attempting to gain access to computing facilities owned and / or managed by the College.

1.3.4 "College" means West Coast TAFE.

1.3.5 "communications" refers to the use of any of the College's computing and/or electronic communications facilities, including, but not limited to, the College network, Department of Education and Training network, the modem pool, telecommunications, PABX and facsimile equipment to access or transmit information.

1.4 Related Legislation/Standards/Frameworks/Policies/Procedures

Users of computing and communications facilities must be aware that use of these facilities is subject to the full range of State and Federal laws that apply to communications and to the use of computers, as well as any other relevant laws. This includes copyright, breach of confidence, defamation, privacy, contempt of court, harassment, vilification and anti-discrimination legislation, the creation of contractual obligations, and criminal laws.

1.5 Supporting/Related Documents

1.5.1 Student Handbook.

1.5.2 College Privacy Statement.

1.5.3 College Code of Conduct.

1.5.4 College Policy no. 408.03 – Spam Policy (staff only).

1.5.5 College Policy no. 408.02 – Email Policy (staff only).

1.5.6 College Use of Computing Facilities Guidelines and Procedures (Appendix A).

Appendix A: Use of Computing Facilities Guidelines and Procedures

1. Users should log out of computing systems when leaving the workstation for any lengthy time to ensure the security of the network.
2. Report any faults to the College IT Help Desk, and not to attempt to rectify equipment or network faults by connecting or disconnecting cables etc, tampering with, powering off equipment (unless instructed to) or changing configuration files.