Computer acceptable use policy

Introduction

AECC provides its staff and students with Network (data storage), internet access and electronic communications services as required to aid the learning experience across the College campus and/or for the performance and fulfilment of job responsibilities.

All computer users must understand that this access is for the purpose of increasing learning and not for non-learning activities.

All computer users must also understand that any connection to the Internet offers an opportunity for non-authorised users to view or access corporate information. Therefore, it is important that all connections be secure, controlled, and monitored.
To this end, users in AECC should have no expectation of privacy while using College-owned or College-leased equipment. Information passing through or stored on College equipment can and will be monitored. Users should also understand that AECC maintains the right to monitor and review network data, Internet use and e-mail communications sent or received by users as necessary.

Permitted Use

The Network, Internet connection and e-mail system of is primarily for College use. Occasional and reasonable personal use is permitted, provided that this does not interfere with the performance of learning and responsibilities.

Users may use Internet services for personal improvement and learning, provided that such use is consistent with professional conduct and is not for personal financial gain or breaches the law.
Users may send and receive e-mail attachments that do not exceed 10 MB in size, provided that all attachments are scanned before they are opened using chosen anti-virus software.

Users may NOT send or receive chat messages via any chat room, unless supervised or requested to do so as part of a lesson supervised by teaching staff.

Prohibited Use

Users shall NOT use the College's network, Internet or e-mail services to view, download, save, receive, or send material related to or including:

- Offensive content of any kind, including pornographic material
- Promoting discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion, or disability
- Threatening or violent behaviour
- Illegal activities
- Commercial messages
- Gambling
- Sports and/or entertainment sites (except as required under the curriculum)
- Personal financial gain
- Forwarding e-mail chain letters
- Sending of unsolicited e-mail (known as spamming) from College's e-mail services or company machines
- Material protected under copyright laws
- Sending College-sensitive information by e-mail or over the Internet
- Dispersing corporate data without authorisation
- Opening files received from the Internet without performing a virus scan
- Use of the College system in order to misrepresent yourself and the College to others
- Saving or playing games or unauthorised executable files on the network
- Sending broadcast network messages unless directed to do so by a member of the teaching staff

- Connecting any unauthorised computer to the College network without prior permission from the IT manager
- The use of computer hacking tools may lead to instant dismissal and possible prosecution
- Any interference with the standard “look” of the computer system (portal). This may also lead to disciplinary action to the offender.

Only IT Department staff may install or authorise the installation of software to any computer system. Any breach of this instruction will breach licensing agreements and can be dealt with by FAST (Federation Against Software Theft).

Responsibilities

Users are responsible for:

- Honouring acceptable use policies of networks accessed through the College’s network, Internet and e-mail services
- Abiding by existing government, local telecommunications and networking laws and regulations
- Following copyright laws regarding protected commercial software or intellectual property
- Minimising unnecessary network traffic that may interfere with the ability of others to make effective use of the College’s network resources.
- Ensuring confidentiality in relation to patient data covered by the Access to Medical Records Act and in all matters relating to the Data Protection Act.

Computer Monitoring and Policing

The IT Department’s staff at the College are authorised by the Principal to monitor the storage of files on the computer network, monitor and log internet site access and also scrutinise any misuse of e-mail activity from the network.

IT Department staff will also randomly remotely view students’ computer screens and record any misuse (which in turn will be presented to the tutor) and make steps to seek potential disciplinary action.

Any interference with the computer set-up on any computer will be treated accordingly and disciplinary action may be taken. The computer equipment is the property of AECC and any interference with these computer systems could be seen as criminal damage.

Violations

Violations will be reviewed on a case-by-case basis. If it is determined that a user has violated one or more of the above use regulations, that user will receive a reprimand from his or her tutor/supervisor/ manager and his or her future use will be closely monitored.

If a gross violation has occurred, management will take immediate action. Such action may result in losing network, Internet and/or e-mail privileges, severe reprimand, or termination of employment or study at AECC.

Student/Staff Acceptance

The policy will be published in the Staff Handbook and in the Student Handbook.

Review

This policy will be reviewed annually.