# Information Technology Conditions of Use

## GENERAL

1. Users of the College's IT facilities must ensure that they:

   - use computing resources ethically;
   - show restraint in the consumption of resources;
   - observe academic and professional integrity;
   - respect intellectual property and the ownership of data and software; and
   - respect other users' rights to privacy, and freedom from intimidation, harassment and annoyance.

2. An account holder is responsible for:
   - all activities that originate from his or her account;
   - all information sent from, requested, solicited or viewed from the account;
   - publicly accessible information placed on a computer using the account; and
   - users are required to take precautions to prevent and detect the introduction of malicious software such as any computer viruses.

3. All users of College IT facilities shall:
   - only use an account personally;
   - only use an IT facilities account for the purpose for which it was allocated;
   - keep access codes or passwords associated with an account confidential;
   - prevent the use of an account by others; and
   - ensure equipment is physically protected from security threats and environmental hazards.
4. A user must not harass or annoy another person using IT facilities.

5. A user must not copy software or data without the permission of the copyright owner (by way of licence or otherwise).

6. A user must not examine, disclose, copy, rename, delete or modify software or data without the express or implied permission of its owner.

7. A user must not monopolize IT facilities. Specifically prohibited examples of monopolization include:
   - overloading IT facilities with excessive quantities of information; and
   - playing games not prescribed as part of College work or study.

8. A user must not waste consumable resources, damage resources or behave in a manner that inconveniences other users of the facilities.

9. A user must not attempt to circumvent system security, network security or any protection or resource restrictions placed on an account.

10. A user must not attempt to capture or decode passwords or access codes, read or capture any data without authority.

11. A user must not attempt to create or install any form of malicious software (for example worms, viruses, sniffers) which may affect computing or network equipment, software or data.

12. A user must not attach any unauthorised device or signal to College IT facilities.

13. A user must not connect any equipment providing off-campus access to College IT facilities (for example, a modem) without the prior certification of the Director Information, Systems, and Technology that such connection meets College security standards.

14. A user must not tamper with or move installed IT facilities without the authorisation of the IT Manager.

15. Permission to use College IT facilities and to access College information is personal and non-transferable.

16. When using mobile computers (laptops, palmtops etc.) users must take special care to ensure that College business and other information is not compromised.

17. Users must take appropriate measures to physically secure and protect, use access controls, cryptographic techniques, undertake backups and provide virus protection.

18. Users must at all times provide adequate protection for mobile computers that are very attractive items for theft.

19. Mobile users who use College IT assets must ensure that this practice is authorised and that the College provided equipment has the same security controls as an on-site machine.

20. Users must report all incidents affecting security through appropriate channels as quickly as possible.

21. All IT facilities identified for disposal or sale must be checked to ensure all resident data is copied and deleted prior to disposal or sale.

## ELECTRONIC MAIL

22. E-mail messages should be kept as short and specific as practicable in the circumstances. Material which may be transmitted by e-mail includes:

- confirmation of arrangements;
- circulation of draft documents for comment or review;
- records and minutes of sectional or ad hoc meetings and working parties;
- confirmation of procedural or administrative information;
- substitutes for written memoranda or telephone conversations; and
- circulation of information received in digital form from external parties.

23. Subject to any standard specified by the College, material that must not be transmitted by email includes;

- sensitive data; inappropriate personal observation about the College, its employees or students;
- advertising material (other than advertisements by the College);
- material of a private nature including private, commercial, political or religious material;
- solicitation of donations or subscriptions to political causes;
- content used to promote discrimination on the basis of race, colour, national origin, age, marital status, sex, political affiliation, religion, disability or sexual preference;
- offensive text or pictures (e.g. pornography, racism, sexism, obscenities, insults, sarcasm); content that may reasonably be considered offensive, threatening or intimidating; defamatory statements, rumours, and gossip, about individuals or organisations;
- users should not respond to irritating e-mail or junk mail just to retaliate. Responding to junk e-mail confirms your e-mail address for future junk e-mail.

24. E-mail is provided primarily for College business use and may be used in legal proceedings.

25. Responsible personal use of the College provided e-mail account is permitted, provided it is reasonable and is not detrimental to the College image.

26. The College may be liable for the acts of an employee that are done in the course of employment, even if the act is unauthorised and contrary to College's policies regarding discrimination and harassment.

27. The general laws of copyright, privacy and freedom of information apply to e-mail communications and all users are responsible for compliance with those laws.