

### Policy and Procedure Information

<b>Name</b>	Guidelines for Students on Use of ICT Facilities
<b>Version</b>	2.0
<b>Approved By</b>	ICT Manager
<b>Date Approved</b>	23 June 2015
<b>Last Reviewed</b>	June 2015

### Responsibility

<b>Policy Owner</b>	ICT Manager
---------------------	-------------

### Policy & Procedure Directory Requirements

<b>Category</b>	5.7 Student Management
<b>Sub-Category</b>	5.7.3 Technology/Social Media

1. Introduction.....	2
2. Audience.....	2
3. Scope.....	2
4. Policy.....	2
4.1 Acceptable Use of IT facilities.....	2
4.2 Copyright Law.....	2
4.3 Software.....	2
4.4 Email and Copyright .....	3
4.5 Honesty in representation and identity.....	3
4.6 Security.....	3
4.7 Non - Interference .....	3
4.8 Unacceptable or prohibited use of ICT facilities.....	4
4.9 Privacy.....	5
4.10 Monitoring use of ICT facilities.....	6
5. Supporting Documentation .....	6
Version Control and Change History.....	6

### 1. Introduction

These Guidelines are issued by the ICT Manager under authority of ICT Executive Committee.

These guidelines provide clarification for students on the practical application of the Macquarie College's (College) Policy on Acceptable Use of ICT facilities and they should be read in conjunction with it.

### 2. Audience

The intended audience for this policy is all students and staff members at Macquarie College

### 3. Scope

These guidelines apply to students at Macquarie College who use College ICT facilities.

### 4. Policy

The following sections set out requirements that are particularly significant and provide relevant information about some of the legislation that governs the use of ICT facilities. All students who use College ICT facilities must comply with the policy, legislation and principles that are referred to here as well as to other directives issued by the ICT Manager.

#### 4.1 Acceptable Use of IT facilities

ICT facilities may be used only as set out in the College's Policy on Acceptable Use of ICT Facilities.

Students must not use ICT facilities for the purpose of personal profit making or for commercial activities other than those of the College. Student use of College ICT facilities including email and the internet is conditional upon compliance with all College policies procedures and guidelines, as well as with State and Commonwealth law.

A list of relevant documents and Government legislation with which students must comply is set out in Appendix A of the Policy on College's Acceptable Use of ICT Facilities.

#### 4.2 Copyright Law

Copyright law restricts the copying of software and other material subject to copyright (documents, music, broadcasts, videos etc.) except with the express permission of the copyright owner. More information about copyright is available from the College's web site.

#### 4.3 Software

Students may not make use of, or copy, software contrary to the provisions of any agreement entered into by the College. The onus is on students to consult with ICT to clarify the permitted terms of use if they wish to use any software for purposes other than those for which the College has a licence.

### 4.4 Email and Copyright

The copyright of an email message is owned by the sender, or the sender's employer. Consider the expectations of the originator; did that person set any conditions on the further communication of their email, or expect that it would not be forwarded to anyone else, or would not be forwarded to a particular recipient?

#### Spam Act 2003

All email messages sent from a College email account must comply with the Spam Act 2003. This Act sets up a scheme for regulating commercial e-mail and other types of commercial electronic messages. The Spam Act refers to spam as "unsolicited commercial electronic messaging". "Electronic messaging" includes emails, instant messaging, SMS and other mobile phone messaging. A single message may be spam. The message does not need to be sent in bulk, or received in bulk.

### 4.5 Honesty in representation and identity

#### 4.5.1 User Misrepresentation

Students must not under any circumstance, in messages or otherwise, represent themselves as someone else, fictional or real, without providing their real identity or username.

#### 4.5.2 Public statements on behalf of the College

Under no circumstances should students send communications using College ICT facilities which give the impression that they are representing, giving opinions or making statements on behalf of the College or any part of it.

### 4.6 Security

The following practices should be observed to maintain the security of the College's ICT facilities.

- Students must keep their username and password safe and not make their password available to others or use any account set up for another user or make any attempt to find out the password of a facility or an account for which they do not have authorised access.
- Students must ensure that the confidentiality and privacy of data is maintained.
- Students must not seek access to data that is not required as part of their study.
- Students who inadvertently obtain data to which they are not entitled or who become aware of a breach of security pertaining to data from any information technology facility must immediately report this to the ICT Service Desk. Unauthorised release or use of data inadvertently obtained may lead to legal action.

### 4.7 Non - Interference

#### 4.7.1 Inconvenience and damage

Students must not behave in a manner which, in the opinion of relevant College managers and staff, unduly inconveniences other people or which causes or is likely to cause damage to College ICT facilities.

### 4.7.2 Installation of software

Students must not install software on any College ICT facility.

## 4.8 Unacceptable or prohibited use of ICT facilities

### 4.8.1 Purpose

ICT facilities are provided for use in the College's teaching and learning, administrative and business activities. Some types of unacceptable use, for example transmission of material of an obscene nature, are specifically prohibited by the *College's Policy on Acceptable Use of ICT Facilities* and by State and Commonwealth law.

### 4.8.2 Examples of unacceptable use

Unacceptable use of ICT facilities is set out in section 6.3 of the *Policy on Unacceptable Use*. Further examples of unacceptable use include:

- circumventing system security provisions or usage quotas
- visiting inappropriate internet sites concerned with pornography and downloading materials that are pornographic or storing or transmitting any such material
- sending or soliciting obscene, profane or offensive material
- sending email messages or jokes that contain discriminating or sexually harassing material, or messages that create an intimidating or hostile work environment for others
- sending email messages designed to cause harm to organisations with which the College has commercial relationships
- using College ICT facilities in the conduct of personal businesses or for commercial purposes
- using College email facilities to send chain letters
- unauthorised forwarding of confidential College messages to persons outside the College
- using another person's mailbox without authorisation
- using another's identity or concealing or misrepresenting one's name or affiliations or address
- sending unsolicited personal opinions on social, political, religious or other non-College related matters, where sending such opinions is not a legitimate part of study
- soliciting to buy or sell goods or services, except in electronic forums that have been established specifically for that purpose
- using or transmitting copyrighted information in a way that infringes the owner's copyright

### 4.8.3 Inadvertent inappropriate use

In relation to use of the web, it may not always be possible to tell if a web page is relevant until it has been read and web search engines and links can sometimes lead to irrelevant and inappropriate websites. In these cases usage logs may be used to demonstrate that access to inappropriate sites was inadvertent.

### 4.8.4 Seeking advice on use

Where a student is in doubt concerning their authorisation to use any ICT facility or about whether a particular use is acceptable, they should seek the advice of their teacher or the ICT Service Desk.

### 4.8.5 What to do when misuse is observed

Report the incident directly to the ICT Service Desk.

### 4.8.6 What happens following a report of alleged misuse

Where an alleged misuse has been reported to the ICT Service Desk or brought to the attention of the ICT Manager or staff members responsible for managing any part of the College's information and communication technology facilities, the ICT Manager (or nominee) may:

- a. act immediately to prevent any continuation of the alleged misuse pending an investigation
- b. promptly notify other authorities, including the relevant Head of School
- c. advise the student of the Acceptable Use of ICT Facilities policy and direct the student to discontinue immediately the alleged misuse

If an investigation of alleged misuse requires a student's use of ICT facilities to be examined or monitored they will not necessarily be notified.

Allegations that constitute misconduct or breaches of the law will be referred to the appropriate authority for investigation. The College will give that authority all reasonable assistance requested including disclosing:

- relevant financial and personal data, and
- data which may be limited by contractual obligation including copyrighted software and software that is patented or which contains trade secrets

### 4.8.7 Penalties for misuse of IT facilities

If a student does not abide by College policy when using ICT facilities, access to ICT facilities may be suspended and disciplinary action, and/or civil or criminal legal action may be taken. See the College's Policy on Acceptable Use of ICT Facilities.

## 4.9 Privacy

### 4.9.1 Privacy limitations

The use of individual password may suggest that privacy is ensured. However, privacy is limited in the following ways.

- use of computers, email and the internet can be accessed by ICT administrators.
- ICT systems automatically log the internet sites visited, the downloads made and the time spent at each site as well as information about emails sent and received. This automatically logged information can be accessed by IT administrators.

- while contents of emails and web sites are not routinely recorded, contents may be stored on staff computers or on servers.
- it is possible to retrieve deleted records from backups and archives.

### 4.9.2 Privacy legislation

To ensure fairness, the College has provided these Guidelines to inform students about its practice of monitoring and accessing records relating to use of College ICT facilities, including computers, email and the internet.

### 4.10 Monitoring use of ICT facilities

The College provides ICT facilities for use in relation to the College's teaching and learning, administrative and business activities. Routine monitoring of the use of ICT facilities is conducted to monitor the costs and acceptable use of College resources. The type of information automatically collected includes:

Internet	Email
<ul style="list-style-type: none"><li>• the name of the person who accessed the internet site</li><li>• the date and time the site was accessed</li><li>• the site address (or "URL")</li><li>• the computer the person used to access the internet</li><li>• the size of the site or web page accessed or the amount of material downloaded.</li></ul>	<ul style="list-style-type: none"><li>• the email address of the person who sent the message.</li><li>• the name of the person who received the message.</li><li>• the email addresses of other people who received the message.</li><li>• the date and time at which the message was sent and received.</li><li>• the server(s) from which the message was sent.</li></ul>

## 5. Supporting Documentation

- Acceptable Use of ICT Facilities

## Version Control and Change History

Version Number	Approval Date	Approved by	Amendment
1.0	21 March 2012	ICT Executive Committee	New Policy
2.0	23 June 2015	ICT Manager	Reviewed in light of changes to Acceptable Use of ICT facilities Policy Updated to latest MC policy format