Macquarie College

Policy and Procedure

Policy and Procedure Information

Name	**Acceptable Use of ICT Facilities**
Version	2.0
Approved By	AdCom
Date Approved	23 June 2016
Last Reviewed	June 2016

Responsibility

Policy Owner	ICT Manager

Policy & Procedure Directory Requirements

Category	5.2 Staff Management, 5.7 Student Management
Sub-Category	5.2.3 ICT, 5.7.3 Technology/Social Media

1. Introduction

The purpose of this policy is to detail the acceptable use for Information and Communication Technology facilities (ICT facilities) at Macquarie College (College) by staff, students and third parties.

2. Audience

The intended audience for this policy is all staff, students and third parties that use the ICT facilities of Macquarie College.

3. Scope

This Policy applies to users with authorised accounts (as defined below) with access to the College's ICT facilities.

4. Policy

The College provides ICT facilities to support its teaching and learning, administrative and business activities. ICT facilities includes all computing and communication equipment, software, services, data and dedicated building space used in connection with information and communication technology, which is owned by, leased by or used under licence or agreement by the College. The College recognises its responsibility to ensure the appropriate use of its ICT facilities and that it must be protected from damage or liability resulting from the unlawful or inappropriate use of its ICT facilities.

This policy also acknowledges that the College is working towards eSmart accreditation as well as promoting cyber safety to our community. This policy has been revised in consultation with the College's eSmart representatives.

4.1 Users with Authorised Accounts

4.1.1 It is a requirement that every person who accesses the College's ICT facilities must have an authorised user account for their exclusive use

4.1.2 Authorised accounts will only be issued to staff employed by the College, currently enrolled students, visiting academics, contractors or consultants engaged by the College, or other recognised affiliates of the College. In addition, access to particular systems and types of use may require authorisation by the ICT Manager, Business Manager or Principal

4.1.3 All users with an authorised account must comply with this policy when using the College's ICT facilities.

4.2 Other Users

4.2.1 This policy recognises that some College ICT facilities are provided for the use of members of the general public who do not have any formal relationship with the

College. An example of such facilities are College web sites that are not subject to some form of access control.

4.2.2 These users will not be issued with user accounts, and will only be subject to sections 4.3.3 and 4.3.4 of this policy. In addition, their use of College ICT facilities must comply with State and Commonwealth laws and any additional Guidelines issued by the College in relation to their use of the facilities.

4.3 Acceptable Use

4.3.1 ICT facilities are provided to support the College's teaching and learning, administrative and business activities

4.3.2 ICT facilities are not provided for recreational or personal use unless specifically stated otherwise in the guidelines listed under Supporting Documentation

4.3.3 ICT facilities must not be used for conducting any business for financial gain of any party other that the College

4.3.4 Users of College ICT facilities must comply with the College's requirements for acceptable use. Specific activities that constitute unacceptable use include but are not limited to:

- 4.3.4.1 deliberate, unauthorised corruption or destruction of ICT facilities (including deliberate introduction or propagation of computer viruses)
- 4.3.4.2 deliberate, unauthorised access to ICT facilities
- 4.3.4.3 unauthorised use of data or information obtained from the use of ICT facilities
- 4.3.4.4 use of ICT facilities to access, create, transmit or solicit material which is obscene, defamatory, discriminatory in nature, or likely to cause distress to some individuals or cultures, where such material is not a legitimate part of teaching and learning or research (if the material is a legitimate part of teaching and learning or research, an appropriate warning should be given)
- 4.3.4.5 transmission or use of material which infringes copyright held by another person or the College
- 4.3.4.6 violation of software licensing agreements
- 4.3.4.7 use of ICT facilities to transmit unsolicited commercial or advertising material
- 4.3.4.8 deliberate impersonation of another individual by the use of their login credentials, email address or other means
- 4.3.4.9 violation of the privacy of personal information relating to other individuals
- 4.3.4.10 unauthorised disclosure of confidential information
- 4.3.4.11 use of ICT facilities to harass or threaten other individuals
- 4.3.4.12 unauthorised attempts to identify or exploit weaknesses in ICT facilities
- 4.3.4.13 unauthorised attempts to make College ICT facilities unavailable
- 4.3.4.14 use of College ICT facilities to gain unauthorised access to third party ICT facilities
- 4.3.4.15 use of College ICT facilities in unauthorised attempts to make third party ICT facilities unavailable

4.3.4.16 use which deliberately and significantly degrades the performance of ICT facilities for other users (including the downloading of files not related to teaching and learning and research)

4.3.5 Users must also comply with the College's other policies and procedures and other guidelines as released by ICT

4.3.6 If any unacceptable use of College's ICT systems is detected, it must be reported to ICT

4.3.7 Behaviour which breaches this policy may also breach Commonwealth and State law.

4.4 User Accounts and Passwords

4.4.1 All user accounts must have one person nominated as the person responsible for that account

4.4.2 Users are responsible for all activity initiated from their accounts, unless it is established that the activity was done by another person who gained access to the user's account through no fault of the user

4.4.3 Users must select passwords that cannot be easily guessed and they must not divulge passwords to others, including other staff and students

4.4.4 Users must not attempt to determine another user's password

4.4.5 If the security of a password is compromised, it must be changed immediately

4.4.6 Users are not permitted to authorise others to login using their account

4.4.7 Passwords should be changed regularly

4.4.8 Users are prohibited from using another user's account.

4.5 College Responsibility

The College will take reasonable steps to protect its ICT facilities from unauthorised and unacceptable use.

4.6 Monitoring Use

The College reserves the right to monitor any and all aspects of its ICT facilities to determine if a user is acting unlawfully or violating this policy, the associated documents listed under the support documents section, or any other College policy or rule. Such monitoring may include, but is not limited to, individual login sessions, the internet sites visited by users and the content of electronic communications. Monitoring may be done with or without prior notice to the user.

4.7 Compliance

4.7.1 Users of College ICT facilities are responsible for adhering to the provisions of this policy

4.7.2 The College may take remedial action and suspend user access with or without prior notice in response to suspected breaches of this policy

4.7.3 Breaches by staff or students that constitute misconduct will be addressed by the relevant staff or student disciplinary procedures

4.7.4 Sanctions for failing to comply with this policy or the associated documents listed in supporting documents section, may include:

4.7.4.1 immediate withdrawal of access to ICT facilities, with or without prior notice
4.7.4.2 action taken under the College's relevant performance management scheme and/or disciplinary procedures for staff or for students
4.7.4.3 criminal or other penalties imposed by State or Commonwealth legislation
4.7.4.4 financial compensation sought by the College.

4.8 Exceptions

Requests for exceptions to this policy must be authorised by the ICT Manager. Such requests must be made in writing and will be evaluated based on the case presented to support it.

4.9 Implementation and review

4.9.1 All Managers, Heads of School or equivalent will be responsible for the implementation of this policy in their respective areas of responsibility
4.9.2 The ICT Manager is responsible for regularly reviewing this policy
4.9.3 The ICT Manager has authority to issue from time to time the guidelines referred to in the supporting documents section due to changes in the law or changes in the practices of the College
4.9.4 The ICT Manager has authority to amend the supporting documents section and any guidelines issued
4.9.5 The guidelines referred to in the supporting documents section and any additional guidelines are afforded the status of policy.

4.10 Communication

4.10.1 The Principal, Heads of School, Managers and Student Services are responsible for ensuring that all students and all staff members are aware of this policy. The policy is also available policy section of Moodle and the ICT department website.
4.10.2 This policy will be included in the information package provided to all new members of staff.

5. Supporting Documentation

- Guidelines for Students on Use of ICT Facilities
- Guidelines for Junior School Students on Use of ICT Facilities
- Guidelines for Staff on the Use of ICT Facilities

References

This policy and its guidelines have been based on the University of South Australia's Acceptable Use Policy.

Version Control and Change History

Version Number	Approval Date	Approved by	Amendment
1.0	12 March 2012	AdGroup	New Policy
2.0	23 June 2015	AdCom	Review of Policy Changed policy to new format Changes made as requested by eSmart initiative