
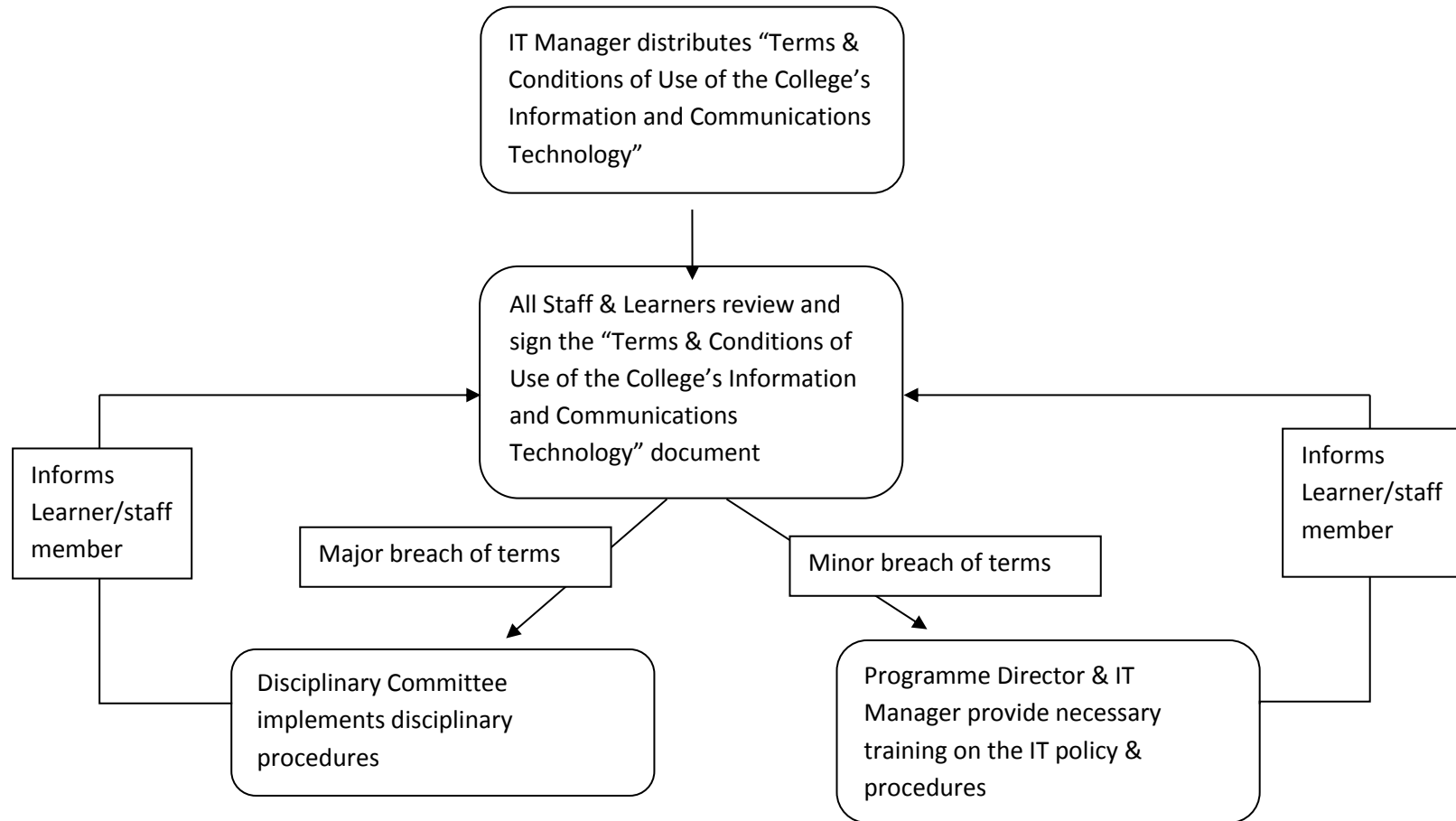


#	POLICY TITLE	POLICY AREA:	VERSION:	DATE ADOPTED:
	8.1 PRINCIPLES, TERMS AND CONDITIONS OF USE OF THE COLLEGE'S INFORMATION AND COMMUNICATIONS TECHNOLOGY	8) INFORMATION AND DATA MANAGEMENT	3.0	AUGUST 2020



Introduction, Context, Scope

- The purpose of this document is to outline principles governing the *Terms & Conditions of Use of the College's Information and*

Communication Technology by which staff and learners are bound.

- The *Terms & Conditions of Use of the College's Information and Communication Technology* and the governing principles outlined below are applicable to all staff, all academic staff (full time and adjunct), all learners and any other parties who use SNMCI it facilities.
- The policy fulfils the requirement of QQI's Statutory QA Guidelines, to have a documented approach to the use of ICT.
- The document takes into consideration European Union (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 in relation to the appropriate use of ICT in online environments.
- The document takes into consideration the Data Protection Act (2018) and the General Data Protection Regulation.

Responsibility:

- The GDPR Officer and IT Manager are responsible for managing and overseeing the implementation of this policy;
- All staff, academic staff (full time and adjunct) and learners are responsible;
- Human Resources and line managers are responsible for managing any suspected breaches of this policy;
- The Director of Quality and Academic Affairs (DQAA) and Head of Registrations are responsible for addressing any suspected breaches of this policy by learners;
- The CEO, in conjunction with the GDPR Officer, is responsible for addressing any suspected breaches of this policy by other parties associated with the College.

Definition of ICT Resources:

Any resource provided to assist learners in their studies and staff in the performance of their duties:

- Internet;
- E-mail;
- Telephone service;
- Virtual Learning Environment (Moodle);
- Video-conferencing (Zoom);
- Social Media;
- File and cloud storage;
- Any and all hardware and software provided by the College.

Policy Statement

- The College fully acknowledges and encourages the use of Information and Communications Technology (ICT) to support teaching and learning and the work of the College;
- The College's Internet connections are intended for activities associated with academic and professional development;
- The College's e-mail should not be used for personal profit/gain, advertising activities outside of the functions of the College or to send information that is the property of the College;
- In order to advance the use of these services in a manner which is beneficial to all and which safeguards the security of the network, it

is necessary for users to be aware of what is considered appropriate and inappropriate usage;

- It is the responsibility of staff and learners to ensure they read and understand the points included in **BFQA 8.1: "Terms & Conditions of Use of the College's Information and Communication Technology"** before signing it and being given access to the College network;
- At induction the Programme Directors and IT Support staff will reinforce the information contained in the "Terms & Conditions of Use of the College's Information and Communication Technology" during any scheduled learner induction / staff induction sessions;
- The College will take an 'educational' approach to unintentional breaches of regulations in the use of the network and offer advice, when beneficial, and further explanations of the seriousness / repercussions of inappropriate use of the network;
- The College will support the implementation of the "Terms & Conditions of Use of the College's Information and Communication Technology" by enforcing related learner and staff disciplinary procedures if required;
- Should an interim change be made to the "Terms & Conditions of Use of the College's Information and Communication Technology" they will be communicated to all staff and learners.
- All individuals will apply a professional attitude towards their work and study environment and demonstrate courtesy and respect at all times when using ICT resources.

Principles of Acceptable Use

Learners and Staff must:

- Use the College's ICT Resources in a responsible, safe and lawful manner;
- Respect the integrity of computer systems, communication devices and networks to which they have access;
- Respect the integrity of the data to which they have access.

Unacceptable Use

Learners and Staff may not:

- Knowingly access, download or distribute illegal or inappropriate material, including material that is in any way pornographic, obscene, abusive, racist, libellous, defamatory or threatening;
- Use social media to degrade, bully or intentionally offend staff members, students or other users or use these tools to bring the reputation of the College into disrepute;
- Gain unauthorised access to the account, systems or equipment of any third party - attempts at 'hacking' may result in criminal prosecution;
- Use another users account;
- Undertake commercial activities or otherwise further commercial objectives which are not a part of their work/studies in the College;
- Infringe the copyright, patent or other intellectual property rights of any person including, by downloading unlicensed software or other unauthorised materials;
- Infringe the data protection or other privacy rights of any person;
- Use the College systems or resources to facilitate plagiarism or cheating in exams or assignments;

- Access, modify, or interfere with computer material, data, displays, or storage media belonging to the College or another user, except with their permission;
- Connect unauthorised equipment to the College network;
- Load or execute unlicensed software or other material on the College's ICT where this is likely to breach the licensing conditions or other Intellectual Property Rights;
- Knowingly introduce any virus, malware or other destructive program or device into the College's systems or network.

Note: System –based controls are in place to prevent inappropriate use, to protect the interests of staff, learners and the College. It is forbidden to intentionally attempt to circumvent these systems.

Passwords and Access Codes

Learners and Staff have a responsibility to safeguard any passwords or access codes granted to them by the College.

- Security measures provided by the College should be respected and no attempt should be made to by-pass them or render them ineffective;
- User ID's and user names should not be shared;
- Passwords should not be shared;
- Staff /learners should not leave computers unattended if they have not 'logged-out';

E-Mail

- Every staff member and learner is provided with an email account to assist with their work and studies;
- This account is the primary way that the College will communicate with learners, graduates and alumni;
- Usage of the email system for academic and professional purposes is encouraged (journals, review papers, professional bodies, etc.);
- Incidental use of an e-mail account for personal purposes is allowed and is subject to the same policies and regulations as official use but systematic use on behalf of individuals or organisations that are not associated with the College **is not allowed**;
- Careless use of e-mail can have very serious consequences. Emails should not contain indecent, obscene, sexist, racist or other inappropriate remarks whether in written form, in cartoon form or otherwise;
- Care must be taken when dealing with suspect e-mails and attachments of unknown origin to prevent computer viruses being transmitted through the network. Suspect e-mails should be deleted immediately and never forwarded to other users;
- Staff members and students **are not authorised** to retrieve or read any e-mail messages that are not sent to them;
- In the unlikely event that an email intended for another person is received the recipient should not forward the message but should contact the GDPR Officer as soon as possible and await further instructions;
- Email messages must not be automatically forwarded (redirected) to external accounts;
- The email account of a staff member, and any information contained in it including content, headers, directories and email system logs, remains the property of the College;
- Care should be taken when attaching documents to ensure the correct information is being released.

Websites/Blogs/Wikis

- The College recognises that learners and/or staff will from time –to- time set up websites, blogs or wikis that, while related to academic or professional activities are nevertheless personal sites and not formal College sites;
- These sites may not display the College name or logo unless they obtain corporate permission;
- Any views expressed on these sites must be accompanied by a disclaimer that indicates that the views are personal and do not represent the College;

Monitoring:

- SNMCI is committed to ensuring security for all and to protecting students, staff members and external parties from illegal and damaging actions carried out by individuals and/or groups whether knowingly or unknowingly;
- SNMCI respects the right to privacy of staff members, learners and external parties and balances this right against the College's own legitimate right to protect itself and its interests from all risk;
- SNMCI reserves the right to monitor such ICT aspects (including but not limited to) as:-
 - Internet access;
 - Network traffic;
 - Social media activity;
 - The VLE Moodle;
 - Server access.
- The SNMCI system is monitored for:-
 - How the system performs;
 - Illegal attempts to access;
 - Unauthorised changes;
 - Compliance with acceptable use.

Students:**Video-conferencing:**

- The integrity of the online environment (intellectual property/copyright etc.) must be upheld and students are **NOT** allowed to individually record any online activities without written permission from the College.
- Students must use full names and identify themselves clearly during online sessions: the use of pseudonyms is **not** permitted;
- When 'in-class', chat sidebars should be used for **ON TOPIC** conversations only. Students must be made aware that 'private' messages can be recovered from the chat manuscript;
- The ICT Facilities related to video meetings, provided by the College, should only be used for legitimate purposes i.e. classes, break-out sessions, student meetings, meetings etc.

Student E-mail:

Disciplinary Committee <ul style="list-style-type: none">- Reviews and makes decisions on any incidents of misuse of the College ICT referred to it.	Disciplinary Committee	
---	------------------------	--

Policy Control Sheet

Policy	QA 8.1: Principles, Terms and Conditions of Use of The College's Information and Communication Technology
Version	3.0
Adopted/Effective	August 2020
Supersedes	2.0
Monitoring/ Next Review Date	Yearly/Aug 2021
Responsible Officer(s) Designated Reviewer(s)	GDPR Officer; IT Manager; CEO; DQAA;
Scope	College Wide

References

SNMCI Policy area	8) Public Information and Communication: QA Vol 3
Developed with reference to	European Union (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. Data Protection Act (2018) Dublin: Stationery Office. Quality and Qualifications Ireland (2016), Core Statutory Quality Assurance (QA) Guidelines
Related SNMCI Policies / Forms	FQA 8.1: Principles and Terms of Use of The College's Information and Communication Technology; FQA 8.2 B: Data Protection Agreement and Information for Learners PQA 8.1: Netiquette Procedures for Learners PQA 8.1: Staff Procedures for interaction with learners in online discussion forums and e-mail

Revision

Revision Number	Revision Description	Originator	Approved By
2.0/Aug 2020	General review for move to Blended Status	Office of DQAA	