Raffles
COLLEGE OF DESIGN

Raffles College Pty Ltd, trading as Raffles College of Design & Commerce
ABN 86 108 888 900 I TEQSA 12039 I RTO 91240 I CRICOS 02761J
1 Fitzwilliam Street, Parramatta NSW 2150, Australia
T +61 2 9633 3800 I **F** +61 2 9633 3399
E contact@raffles.edu.au I **W** www.raffles.edu.au

Information Technology Policy and Procedure

RSY-MGT-PY-v1.0-Information Technology Policy and Procedure

Document History

Version	Date of Review	Date of Approval	Change(s)
1.0		**20 June 2017**	-

Approved by: **Academic Board** on **20 June 2017**

Distribution List

To: All RCDC Staff
All RCDC Students

Cc: Chair, Council

Table of Contents

1 Purpose

This Policy sets out the obligations and expectations of students and staff of the Raffles College of Design and Commerce (RCDC) who use RCDCs IT facilities for Internet and email purposes.

2 Scope

This Policy applies to all students and staff of RCDC.

3 Definition of Terms

IT: Information Technology.

IT facilities or resources: these include systems, software, hardware and services and may include computers, modems, printers, terminals, networks, telecommunication devices, storage and related equipment, data files, information systems, and services such as internet access and email.

Passwords: the secure entry point for personal access to IT resources such as email.

User: an individual who uses any IT system, hardware or service owned or leased by RCDC.

4 Policy Principles

The Policy recognises:

- that IT facilities are provided in order to assist with day to day work and studies, and must be used lawfully, responsibly and ethically;
- that no person is allowed to use RCDC's IT facilities who has not previously been authorised to do so by the IT support services staff;
- that all users are expected to act in a manner that will not cause damage to IT facilities or disrupt IT services; and
- that all users are expected to use IT facilities in a way that does not bring the Institute into disrepute.

5 Policy Details

5.1 Unauthorised access

Under the *Cybercrime Act 2001,* it an offence to try and access any computer system for which authorisation has not been given. RCDC's IT resources may only be used by authorised users, and only to discharge the responsibilities of their positions as employees, to further their studies as students, to conduct official business with RCDC, or in other sanctioned activities. Unauthorised access to IT facilities is prohibited by law and may result in disciplinary action and/or criminal prosecution.

5.2 Email

Under the *Telecommunications (Interception and Access) Act 1979*, and the *Freedom of Information Act 1982*, any information which RCDC holds may potentially be disclosed to a requester. This includes emails.

Users need to be sure that they are not breaching any data protection when they write and send emails. This could include but is not limited to:

- passing on personal information about an individual or third party without their consent;
- keeping personal information longer than necessary; and
- sending personal information to a country outside of Australia.

Email should where possible be avoided when transmitting personal data about a third party. Any email containing personal information about an individual may be liable to disclosure to that individual. This includes comment and opinion, as well as factual information. Therefore this should be borne in mind when writing emails, and when keeping them.

5.3 Other Offences

Other offences against State and Federal legislation include:

- copying software without the permission of the owner of the copyright;
- publishing untrue statements which adversely affect the reputation of a person or group of persons; and
- encouraging terrorism and/or disseminating terrorist publications in any form.

5.4 Monitoring

Staff and students should note that the *Workplace Surveillance Act 2005* allows for an organisation to monitor or record communications (telephone, Internet, email and fax) for defined business related purposes.

6 Actions and Responsibilities

6.1 Authorisation

RCDC's IT resources may only be used by authorized users. Unauthorised access to IT facilities is prohibited and may result in either disciplinary action or criminal prosecution.

6.2 Responsibilities

6.2.1 General

Users may only use RCDC's IT facilities in order to discharge the responsibilities of their positions as employees, to further their studies as students, to conduct official business with the Institute, or in other sanctioned activities. Users are responsible for any IT activity which is initiated under their username.

6.2.2 Damage or Disruption

Any accidental damage or disruption must be reported to IT support services as soon as possible after the incident has occurred.

6.2.3 Use of the Internet

Use of the Internet is encouraged where such use is consistent with the work of students/staff, and with the objectives of RCDC in mind. At all times, users must not:

- participate in any online activities or create or transmit material that might be defamatory, bring RCDC into disrepute, or incur liability on the part of RCDC;

- visit, view, download or transmit any material from an Internet site which contains illegal or inappropriate material. This includes, but is not limited to, pornography, obscene matter, race hate material, violence condoning messages, criminal skills, terrorism, cults, gambling, and illegal drugs;

- use the internet for illegal or criminal activities;
- use the internet to send offensive or discriminatory material to others; or
- knowingly or maliciously interfere with IT services. This includes knowingly introducing any form of a computer virus into RCDC's network, and hacking into unauthorized areas.

Reasonable personal use is permissible, provided that the above restrictions are adhered to, and subject to the following:

- Personal use of the Internet must not cause an increase for significant resource demand (such as storage, capacity, or speed) or degrade system performance.
- Users must not download commercial software or any copyrighted materials belonging to third parties, unless such downloads are covered or permitted under a commercial agreement or other such licence.
- Users must not use the Internet for personal financial gain.
- Personal use (such as online banking, shopping, information surfing) must be limited, and done only during non-class time.
- Use of gambling sites, online auction sites and social networking sites such as, but not limited to, Facebook, LinkedIn, YouTube, Twitter, Instagram etc. must be limited, and only used when relevant to the learning activities or during non-class time.
- Users may face disciplinary action or other sanctions (see below) if they breach this Policy and/or cause RCDC embarrassment or compromise its reputation.

6.2.4 Use of Email

Staff and students are responsible for all actions relating to their email account/pc username, and should therefore make every effort to ensure no other person has access to their account.
When using RCDC email, users must:

- follow and abide by the relevant instructions;
- ensure they do not disrupt RCDC's wider IT systems or cause an undue increase for significant resource demand in storage, capacity, speed or system performance;
- ensure they do not harm RCDC's reputation, bring it into disrepute, or incur liability on the part of RCDC;
- not seek to gain access to restricted areas of the network;
- must not use disruptive or offensive messages, images, materials or software that include offensive or abusive comments about ethnicity or nationality, gender, disabilities, age, sexual orientation, appearance, religious beliefs and practices, political beliefs or social background. Students who receive emails with this content from other students of the Institute should report the matter to IT support staff.
- not send email messages that might reasonably be considered by recipients to be bullying, harassing, abusive, malicious, discriminatory, defamatory, and libelous or contain illegal or offensive material, or foul language.
- not upload, download, use, retain, distribute, or disseminate any images, text, materials, or software which might reasonably be considered indecent, obscene, pornographic, or illegal.
- not engage in any activity that is likely to:
  - corrupt or destroy other users' data or disrupt the work of other users;
  - waste staff effort or RCDC resources, or engage in activities that serve to deny service to other users;
  - fall outside of the scope of normal study-related activities;

- affect or potentially affect the performance, damage, or overload, RCDC's system, network, and/or external communications in any way;
- be a breach of copyright or license provision with respect to both programs and data, including intellectual property rights; and

- not send chain letters or joke emails from a RCDC account.

- Students and staff who receive improper email from individuals inside or outside RCDC should discuss the matter in the first instance with IT support staff.

6.3 Good Practice

6.3.1 Confidentiality

Where sensitive and confidential information needs to be sent via email for practical reasons, please be aware that email is essentially a non-confidential means of communication. Emails can easily be forwarded or archived without the original sender's knowledge. They may be read by persons other than those for whom they are intended.

6.3.2 Content and Tone

Users must exercise due care when writing emails to avoid being rude or unnecessarily terse. Emails sent from the College domain may be interpreted by others as RCDC statements. Users are responsible for ensuring that their content and tone is appropriate.

6.3.3 Deletion, Archiving and Junk Mail

Users should delete all personal emails and attachments when they have been read and should also delete all unsolicited junk mail. Users should take care not to archive inappropriate material.

6.3.4 Sources

Caution should be used when opening any attachments or emails from unknown senders. Users must endeavour to ensure that any file downloaded from the Internet is done so from a reliable source. Any concerns about external emails, including files containing attachments, should be discussed with IT support staff.

6.3.5 Use of Antivirus Software

Antivirus software will be automatically enabled on stand-alone PC's, and run regularly on networked computers to minimize as far as possible the Institute's IT systems being compromised by malware.

6.3.6 Security for Passwords

All users are expected to take responsibility for protecting their passwords, and to change them regularly in order to maintain their security. Passwords must include a variety of characters and numbers, must not consist of names, birthdays, whole words, or other predictable terms, and must not be disclosed to any other person.

6.4 Remote Users

Users may sometimes need to use RCDC's equipment and access the Institute network while working remotely. The standards set out in this document apply whether or not RCDC equipment and resources are being used.

6.5 Monitoring

All resources of RCDC, including computers, email and the internet, are provided for legitimate use. If there are occasions where it is deemed necessary to examine data beyond that of the normal business activity of RCDC then, at any time and without prior notice, RCDC maintains the right, subject and in accordance with current legislation in Australia, to examine any systems and inspect and review all data recorded in those systems. This will be undertaken by authorised staff only and in accordance with RCDC's Personal Information and Privacy Policy. Any information stored on a

computer, whether the information is contained on a hard drive or in any other manner, may be subject to scrutiny in order to ensure compliance with internal policies and the law.

6.6 Penalties for Improper Use

Users in breach of these regulations may:

- have access to RCDC's IT facilities restricted or withdrawn;
- be subject to RCDC's disciplinary procedures;
- have their enrolment or employment terminated;
- be reported to relevant law enforcement agencies; and/or
- be subject to prosecution.

7 Legislation

All users shall comply with the relevant legislation. This includes the following:

- Telecommunications (Interception and Access) Act 1979/ Freedom of Information Act 1982
- Cybercrime Act 2001
- Copyright Act 1968
- Defamation Act 2005
- Anti-Terrorism Act 2005
- Workplace Surveillance Act 2005