LCI Melbourne
+613 9676 9000
info@lcimelbourne.edu.au
www.lcimelbourne.edu.au
PO Box 1219 Collingwood VIC 3066
150 Oxford Street Collingwood VIC 3066
ABN 97 585 592 579 CRICOS No. 02201G

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

Revision Number		**Accountability**	Dean and Principal
Policy Number		**Operational Responsibility**	General Manager
Date of Approval	Q2 2018	**Last Reviewed**	Q2 2018
Approval Authority	Board of Directors	**Next Review**	Q2 2019

OBJECTIVES

LCI Melbourne is committed to maintaining documented procedures for all activities related to the use of the school's computer and telecommunication resources, including the Internet. LCI Melbourne's technology resources assist in the progress of learning by means of teaching and knowledge sharing.

SCOPE

This policy applies to any activity related to the use of computer and telecommunications resources and has an impact on the quality of the functioning and operations of LCI Melbourne. Furthermore, this policy applies to all users of the Institutes information and communications technology and supporting infrastructure. Users include employees, students and all other parties that have been granted access.

EXCLUSIONS

There are no exclusions to this policy.

PROVISIONS

Responsibility

- It is the General Manager's responsibility to establish, update and enforce this policy;
- Each Coordinator has the responsibility to enforce this policy to the student community of LCI Melbourne;
- It is the Facilities Manager's responsibility to ensure that the most appropriate and innovative forms of telecommunication services are operating in order to meet the needs of the Institute;
- It is the Facilities Manager's responsibility to supervise the security of the internal and external telecommunications traffic with the intention of protecting the Institutes systems.

DEFINITION

The term "user" refers to any person (regardless of status as a student or an employee) using LCI Melbourne computer and telecommunication resources.

Rights of Access and Conditions

Existing IT infrastructure is in place to support the work of Academic staff and staff members as well as increase access to information for students. Pursuant to this, the right of access is limited to activities corresponding with the mission of the Institution (research, education, administration and communication). Access may be denied or restricted by the Facilities Manager upon request of the user's immediate supervisor or an Academic staff member in case of improper use.

Usage Responsibilities

Each user is responsible for the utilisation of computer and telecommunications resources to which they have access. The immediate supervisors will safeguard sensitive information in the interests of LCI Melbourne and IT users.

Any email received by LCI Melbourne employees must be responded to in a timely manner.

SUPPORTING PROCEDURES

Use of IT Resources

LCI Melbourne's IT resources (particularly the Internet, email, phone and fax) are provided solely to facilitate professional business and enhance studies. Usage of this equipment for other purposes – especially those related to personal, commercial or entertainment activities – is prohibited.

LCI Melbourne recognizes that these resources might be used during incidental personal situations. However, such incidental situations shall not interfere with the Institute's operations or interfere with the user's employment or other obligations. Reasonable private use – such as during the lunch hour – is permitted outside scheduled working hours.

Forwarding of Chain Letters

The transmission of messages to all users, courtesy copies (cc) and blind courtesy copies (bcc) should be done only when necessary. The recipients of messages should also be carefully chosen.

Messages of an Offensive Nature

Any messages of an offensive nature should be reported to the Facilities Manager, who will block the respective sources.

Any messages that make reference to viruses (e.g. *"A colleague from ... has asked me to let you know that a super-virus from the Internet*…") should be forwarded with comments to the Facilities Manager, and not to all users, for analysis and response.

Downloading Data from the Internet

Access for downloading is controlled by the IT Services, who will give permission to download only to those who have been granted this privilege by the manager of their department or service.

The following activities are strictly forbidden:

- Downloading of files (e.g. music files) other than the document files that are necessary for daily work / studies;

- Usage of alternative non-work-related communication and social media (e.g. Hotmail, Facebook, Skype, Instagram, etc.) other than those necessary for daily work / studies;
- Sharing sensitive information found in workstations, including files and directories;
- Sharing files that are not necessary for daily work / studies, using the personal network file services or shared directories;
- Use of MP3 players, cell phones or tablets, during working hours, unless the use is for Institute usage purpose.

Given the high volume of users, it is vital to conserve bandwidth by using the internet in an economical and efficient manner.

Confidentiality

Workstations are a component of the IT system belonging to LCI Melbourne. User files are considered institutional records, whether or not they are accessible to other users. They can therefore, be viewed at any time by the immediate supervisor or the latter’s supervisor.

The administration may also appoint a person or persons responsible for quality control in services dealing directly with students and employees. Such a person has access to the global means of communication (telephone and electronic) of specific employees. The same conditions apply for the records of said individuals.

Users are required to safeguard any information on the internal functioning of the institution.

IT Services may be called upon (with the permission of the head of their department or service) to examine the content of files and mailboxes to obtain sufficient information to correct software problems, system overloads or, if necessary, to engage in investigations related to user compliance with the policies listed in this document.

Workstations should not be used without permission from the user to whom they are assigned, except at the request of the head of the department or service.

User Computer and Telecommunications Records

LCI Melbourne will keep a record of the usage of computers and telecommunications. Users who use the Internet for unauthorized purposes will be subject to disciplinary measures.

Rules to Follow

Each user is accountable for his or her use of computer resources. Users must show commitment to avoiding activities that adversely affect the regular functioning of the network, the integrity of computers and the internal and external relations of LCI Melbourne.

Unattended computers must be locked after all applications have been closed. In addition, users

should strictly refrain from:

• Undermining the integrity or infringing on the sensitivity of another user through messages, texts or images in bad taste;
• Hiding their true identities, particularly by logging in under other user names;
• Tarnishing the image of the establishment through the improper use of network tools;

• Interrupting the regular operation of the network or systems connected to the network for example: abnormal handling of technology or data through careless use, willful damage, breach of security, compromise of privacy, theft or the introduction of viruses;
• Accessing the account of another user without permission, in particular, the account of immediate supervisors;
• Accessing information belonging to other network users without their permission or that of their immediate supervisor (except in the cases specified above);
Information and Communications Technology Policy
• Modifying or destroying information – especially accounting or other sensitive information – belonging to other users without their permission or that of their immediate supervisor.

Any deviation from these principles can lead to disciplinary measures or criminal charges depending on the severity of the offence.

Security

All users of the LCI Melbourne computer network must contribute to the best of their ability and apply rules of common sense and the recommendations provided by the Institute and computer systems management to ensure security. Any communication that is threatening or offensive shall be immediately reported to the Institute's management.

All users are asked to adhere to the following guidelines:

- Reasonably and intelligently use shared resources (disk space, software and bandwidth on
- the network);
- Never leave the computer when confidential information is displayed on the screen;
- Protect all corporate files deemed confidential.
- Choose secure passwords and follow the subsequent recommendations:
  a) Never disclose Active Directory (i.e. Outlook, Intranet, ACCPAC, Clara, Taleo) passwords
  or login as another person
  b) Never disclose passwords to anybody unless doing so is necessary to perform tasks on
  behalf of the institution;
  c) Save files regularly and manage backups and storage of files in compliance with organizational requirements;
  d) Control and manage access to the computer equipment individually assigned to them.

There are default security systems in place for all users whereby the screen saver is set to ten (10) minutes and the password expiration is set to one-hundred and twenty (120) days.

Student data and personal information must be stored on Canadian servers (not outsourced to the USA subject to the rules and regulations of the patriotic act).

Immediate supervisors have full access to employee files such as email accounts.

Employee Access to Records

Employee access to Institute records is limited. To obtain approval to view a file on a shared server, an email must be sent to their immediate supervisor requesting authorisation. Once approved, in writing, another email must be sent to the IT Services requesting access to the server. However, access to documents is always limited.

Bring your own device

The following section includes detailed guidelines on the proper use of personal devices at the college. Academic staff are highly encouraged to read this section to reinforce the good use of personal devices by their students. It also informs Academic staff about BYOD best practices for themselves and their students.

Acceptable Use

- Students may be blocked from accessing certain websites during class hours/while connected to the school network at the discretion of the college. Such websites include, but are not limited to…
  - Pornographic content
  - Streaming of video (Netflix or other)
- Devices may not be used at any time to:
  - Store or transmit illicit or illegal materials
  - Harass others
  - Engage outside business activities
- Students may use their personal and mobile devices to:
  - Browse any content related to their classes.
  - Use the school learning management system (LMS), in this case LÉA.
- LCI Melbourne has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

Devices and Support

- Connectivity issues (e.g., Wi-Fi) are supported by IT Services. Students can send a MIO to 3777 to report a problem with Wi-Fi. Academic staff can send a message on Outlook to 3777. Everyone can also call 03 9676 9000, ext. 8106 to report a technical problem.
- Students and Academic staff should contact the device manufacturer or their carrier for operating systems or hardware-related issues. The Institute is not responsible for such issues.
- Academic staff should contact the Facilities Manager for any issues related to the use of their PC or MAC devices
- Students' personal devices must be configured with standard apps, such as browsers, office productivity software and security tools, before they can access the network. Failure to do so puts the student at risk of malware (e.g., viruses) and academic failure (e.g., need required software to complete projects).

Reimbursement

- LCI Melbourne will not reimburse the students or Academic staff for the cost of the device they had bought nor will they replace the device if it has been damaged or stolen.
- LCI Melbourne will not reimburse the students or the Academic staff for the following charges: roaming, plan overages, etc.

Security

- In order to prevent unauthorised access, devices must be password protected using the features of the device and a strong password is required to access the Institute's network. LCI Melbourne's strong password policy is:
  - At least six characters
  - A combination of upper- and lower-case letters
  - Numbers and symbols.
- The device must lock itself with a password or PIN if it's idle for five minutes.
- Students are automatically prevented from downloading, installing and using any app that is not related to the class.
- Smartphones and tablets belonging to students and/or Academic staff that are for personal use only are allowed to connect to the network. However, the Institute is not responsible for any harm caused to these devices, as it is at the student's and teacher's discretion to bring them to school.

Risks/Liabilities/Disclaimers

- While IT will take every precaution to secure the Institute's network, it is the student's and Academic staff responsibility to take additional precautions, such as backing up files, projects, emails, contacts or other on cloud-based websites (e.g., Omnivox, One drive, Google Drive).
- LCI Melbourne reserves the right to disconnect devices or disable services without notification, in case of threat or misuse of the network.
- Students and Academic staff are not automatically covered by providers (e.g., Apple, DELL, etc.) in case of lost or stolen devices. Students and Academic staff are responsible for notifying their mobile carrier and/or provider immediately upon the loss of a device. LCI Melbourne is not held responsible for such losses.
- Students and Academic staff are expected to use his or her devices in an ethical manner at all times and adhere to the Institute's acceptable use policy as outlined above.
- Students, Academics and staff members are personally liable for all costs associated with his or her device.
- The students, Academics and staff members assume full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- LCI Melbourne reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

Terms of Use for Technical Devices in the Classroom

Personal technological devices can be used only for the purpose of educational activities. It is forbidden to use them for other activities, including for personal, commercial, or entertainment purposes. Therefore, LCI Melbourne requires students to respect the following terms and conditions of use:

1. Only authorised persons may use the Institute's technological devices.
2. All technological devices must be used generally and habitually for purposes related to Institute activities: teaching, learning, research, organization, and information.
3. Any use of technological devices for commercial purposes other than those related to LCI Melbourne activities is prohibited.
4. Those who use or communicate with their technological devices must ensure that they respect the rules of netiquette. The term "netiquette" is used to refer to "online etiquette over

networks, such as online communities, forums, and even online learning environments," and includes email messages. "Following the rules of netiquette improves the readability of your messages, lays the groundwork for making trustworthy connections and helps other people to better understand you."

5. Please respect individual privacy. Do not capture and/or distribute visual or sound recordings without the written consent of the person(s) represented

6. No person shall broadcast material produced by another without having written permission.
7. No person may consult websites carrying information of a violent, racist, hateful, homophobic, or pornographic nature or sites of gambling, contests or lotteries.
8. No person may distribute repetitive messages that are targeted or have the effect of cluttering or otherwise encumbering a site facilitating the activities of LCI Melbourne.
9. No person is allowed to participate in chain letters or send mass mailings for personal purposes (ex. solicitations for political purposes) or without explicit permission from the direction of the school.
10. No person may use the Information and Communication Technologies (ICT) so as to cause defects or failures in the systems or networks to which they have access or to block access to others. To this end, identity theft, phishing, and theft of data or personal information are prohibited activities and subject to severe disciplinary actions.
11. In the case of inappropriate behaviour, the school reserves the right to intervene.
12. Information Technology services (IT) is not required to provide technical support for equipment that does not belong to the Institute.
13. Given the high number of student users, an economy of bandwidth is required. Therefore, the Internet must be used in strict compliance to educational needs. All massive downloads for personal purposes (applications, videos, music, live broadcasts, etc.) are prohibited.
14. The use of ICT must be in compliance with Institute policies, laws, and license agreements.
15. The failure to respect one or more of these conditions could lead to a warning, the suspension of a course, or expulsion from the Institute, according to the recurrence or severity of the misconduct, in compliance with LCI Melbourne's Student Conduct Policy.

Accountable Officers

The accountable officers for the implementation and relevant training of this policy are listed below.

<table>
<tr><td colspan="3">Policy Category</td><td colspan="2">IT</td></tr>
<tr><td colspan="3">Responsible Officer</td><td colspan="2">General Manger</td></tr>
<tr><td colspan="3">Review Date</td><td colspan="2"></td></tr>
<tr><td colspan="5">Approved by</td></tr>
<tr><td colspan="5"></td></tr>
<tr><td colspan="5">Change and Version Control</td></tr>
<tr><td>Version</td><td>Authored by</td><td>Brief Description of the changes</td><td>Date Approved</td><td>Effective Date</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table>