OZFORD
Institute of Higher Education

USE OF INFORMATION TECHNOLOGY FACILITIES AND SERVICES PROCEDURE (STUDENTS)

Approving authority	Executive Management Team
Purpose	This procedure provides the Institute's students with guidelines for the appropriate use of Use of Information and Communication Technology Facilities and Services
Responsible Officer	President and CEO
Next scheduled review	**February 2031**
Document Location	https://www.ozford.edu.au/policies-and-procedures/higher-education/
Associated documents	Use of Information Technology Facilities and Services Policy (Students) Academic Integrity Policy and Procedure Anti-Bullying and Harassment Policy and Procedure Anti-Discrimination Policy and Procedure Diversity and Equity Policy and Procedure Engaging Managing and Monitoring the Performance of Education Agents Policy and Procedure Marketing and Advertising Materials Policy and Procedure Occupational Health and Safety Policy Privacy Policy and Procedure Records Management Policy and Procedure Sexual Assault and Sexual Harassment Policy and Procedure Social Media Policy and Procedure (Students) Student Code of Conduct Policy and Procedure Student Grievance s and Appeals Policy and Procedure

1. PRINCIPLES

Ozford Institute of Higher Education (herein after referred to as 'the Institute') recognises the importance of information technology and communication systems as a study and communication tool that is regularly used by its students to connect with each other, Institute staff and the broader community. In recognition of the rapid growth and application of information technology and communication systems, the Institute has recognised the need for a policy to ensure that those who use information technology and communication systems in a personal capacity, study or association with the Institute do so consistent with Institute guidelines for acceptable use.

Information and communication (ICT) facilities and services are an integral part of the Institute's operations. The Institute's ICT facilities and services include:

- computing, collaboration and communications facilities, examples of which include telephones, facsimiles, mobile telephones, computers, tablets, printers, photocopiers, emails, internet access, network applications, web services and similar resources;
- the use of the remote system, accessed via ICT facilities and services, is also covered by this policy;
- the use of mobile phone, handheld devices, iPads , computers and data storage devices that are the personal belongings of students when they are being used to access or are connected to the Institute's ICT facilities and services.

The Institute has made a substantial investment to create and protect ICT facilities and services that are provided to students to support their studies and where applicable internship work with the Institute.

The Use of Information Technology Facilities and Services policy and this procedure is designed to allow legitimate and optimal use of ICT facilities and services and to protect both students and the Institute. This procedure supports the policy to:

- promote the effective use of ICT by students to enable them to work effectively in successfully meeting the requirements of their course;
- ensure that the Institute ICT facilities and services are protected and available for use by students when required;
- protect and to safeguard the information contained within the Institute's systems;
- reduce unsolicited commercial email ("Spam");
- protect the Institute and its students from activities that might expose the Institute or its students to liability.

2. SCOPE

This Procedure applies to all students who use of the Institute's ICT facilities and services.

This Procedure does not apply to the use of social media by students this is the subject to the ***Social Media Policy and Procedure (Students)***.

3. DEFINITIONS

Cloud services

Where ICT providers deliver services online which are accessed from a web browser, computers and applications.

Head of Department

The Head of Department will be one of the following:

- the President and CEO
- the Head of Marketing (currently the Director of Marketing & Student Recruitment)
- the Academic Dean
- the Director of Operations (Brisbane)

ICT facilities and services

The Information and communication technology (ICT) facilities and Services means all computer, telecommunications and ICT equipment including peripherals (and all other items incidental to computer use) that are owned, used or leased by the Institute or its affiliates and all the Institute networks, servers and subscription or application-based services whether on or offsite.

Personal data storage device

Any device, that is the personal belonging of the user, that when connected to the Institute's ICT facilities and services is able to transfer stored data to or from the device.

Severe misconduct

Severe misconduct includes but not limited to

- acts dishonestly in relation to admission to the Institute;
- knowingly makes any false or misleading representation about things that concern the student as a student of the Institute or breaches any Institute Policies or Procedures;
- harasses or intimidates another student, a member of staff, a visitor to the Institute, or any other person while the student is engaged in study or other activity as an Institute student, because of race, ethnic or national origin, sex, marital status, sexual preference, disability, age, political conviction, religious belief or for any other reason;
- Misuses any facility in a manner which is illegal, or which is or will be detrimental to the rights or property of others. This includes the misuse, in any way, of any computing or communications equipment or capacity to which the student has access at or away from the Institute premises while acting as an Institute student, in a manner which is illegal, or which is or will be detrimental to the rights or property of others;
- steals, destroys or damages a facility or property of the Institute or for which the Institute is responsible.

SPAM

SPAM is defined as irrelevant or unsolicited (Unasked for or sent without prior consent) electronic messages sent typically to a large number of users by email for the purposes of advertising, phishing, spreading malware, etc.

The *SPAM Act 2003* regulates the sending of one or more commercial electronic messages and prohibits the use of address harvesting software and harvested address lists. It is prohibited to send unsolicited commercial electronic messages without consent. This applies to messages with an Australian link, either originating in Australia or with an Australian destination, or if the device used to access the message is in Australia.

Unauthorised Software

Unauthorised Software means any software that has not been reviewed by the ICT Services team prior to installation on an Institute device. This includes, but is not limited to, games and peer-to-peer file sharing programs.

Use

Use of the Institute ICT facilities and services by users including but not limited to internet and email (both the Institute and external email) access. This includes the connection of any device, regardless of ownership or purpose, to any the Institute resource and the connection of a device to a mobile network (Wifi, 4G/5G or other mobile networks), where the number, service, SIM or bill is paid for or provided by the Institute.

Users

Users are all students, full-time, and part-time employees of the Institute as well as external committee and board members, guests, temporary and contract staff engaged by the Institute, its third-party education agents, visitors and any other persons involved with the Institute.

4. PROCEDURE

Access to ICT facilities and services

4.1 Student user accounts are created and deactivated by the ITS services team.

4.2 Prior to orientation, the Student Experience team notify the ITS services team to set up access for new students.

4.3 Students are informed about the ***ICT Acceptable Use Policy and Procedure*** during orientation.

Role and availability of the ITS team

4.4 The ITS services team:

- arranges for students to access network drives and folders relevant to their study. Any additional network drive and folder access requires approval from the Head of Department.
- creates a unique username and password for each student to access ICT facilities and service at the Institute.
- monitors the Institute ICT facilities and services.
- ensures that the centralised authentication system is implemented, and that only currently authorised students have access.
- ensures that students are trained and receive support to enable effective use of ICT facilities and services.

4.5 The Institute's ICT facilities and services are available on campus during business hours: Monday to Friday 8.30 am – 5.00 pm. Additional access may be approved by the Academic Dean or the Head of Marketing and Student Experience.

4.6 Students can access online facilities including webmail and Moodle during and out of business hours.

4.7 Students who require ICT assistance should contact ITS services team: by email: itservicedesk@ozford.edu.au

SPAM

4.8 SPAM email can generally be identified by their Sender, Subject or Content. On SPAM, the sender's name that appears is generally a fake email address and the real sender can tell if the email

is opened, and this may lead to a proliferation of more junk mail. If the Subject includes something that is distasteful, misspelt or is not understandable; it probably is SPAM. Be aware also of no Subject as well. This may be harmless because some people just forget to put a Subject on it.

4.9 If SPAM is detected, the ICT is normally automatically quarantined by the Institute's firewall software.

4.10 The ITS services team will send a notification email to the recipient to with a link to release the email if the ICT is legitimate.

4.11 If the ICT is not filtered and a suspect email appears:

- do not open the email.
- use the Reading Pane to view contents. The Reading Pane does not open the email (regardless of the Icon symbol).
- do not open or run any attachments unless requested, even if they appear to be from someone known. A virus is unlikely to be sent from the person that the email says it is from and if the attachment, particularly an executable attachment, has not been requested then there is a good chance that it did not come from the person.
- do not join a group or newsletter list or the equivalent unless there is certainty that it is safe to do so.
- do not provide your email address unless certain of security.
- delete spam emails completely from of Outlook. Using Shift + Delete will delete the message completely, bypassing the Deleted Items folder.
- create a "Rule" to identify keywords and send them to the Junk Mail Folder. Check this folder periodically with the Reading Pane and delete the Spam from Outlook. This way you don't have to do it so often.

4.12 Students should, as they have been trained in orientation, either immediately delete the SPAM or contact the ITS services team for support to do so.

4.13 If a student believes that they have a virus, the ITS services team should be immediately contacted.

Security of ICT facilities and services

4.14 The ITS services team

- Monitors all logins onto computer systems.
- Monitors internet access, the internet is routed through WatchGuard firewall solutions, which filters some traffic (blocks unauthorised traffic) and monitors and logs all internet traffic. All emails are also filtered using WatchGuard firewall email subscription based on filtration and quarantine service; and suspicious emails require manual intervention to be released.
- Monitors remote access to computer and network system.
- Monitors the Institute student administration system.
- Ensures that there is ongoing backup of Information Systems, as well as the testing of backups and the offsite storage of backup media.

4.15 The physical security, floor access and room access are locked off and secured out of working hours and are limited to users with keys and access card, which is controlled.

4.16 Students cannot access the campus after hours.

Termination of Student access

4.17 The Student Services team will notify the ITS services team that access should be removed after graduation, on notification of withdrawal by a student or when an enrolment is terminated by the Institute.

4.18 The ITS services team will:

- compile a list of all student accounts and send to the Student Experience team for review every 3-6 months.
- Removes all deactivated student accounts from the systems every 12 months.
- Ensures library system users are removed from system after 3 years of inactivity.

External ICT Equipment / Cloud services and solutions

4.19 Any external or personal equipment that students wish to be connected to the Institute's facilities or services must first be approved by the ITS services team. Approval is dependent on there being an active antivirus program running on the equipment within current antivirus definitions.

4.20 The accessing, storing and working on Institute data on 'Cloud' services must comply with the Institute policies including the ***Privacy Policy and Procedure***.

4.21 Students must ensure that all data (including copies/backups electronic or otherwise) needs to be irretrievably erased if no longer used.

Breaches of the Policy and this Procedure

4.22 The ITS services team will for an initial breach of the policy and this procedure may:

- Counsel the student on appropriate use of the ICT services and facilities; and/or
- Deny/restrict access to the email service, system access and/or network services.

4.23 The Student Services team will have responsibility for addressing student conduct as set out in the ***Student Code of Conduct Policy and Procedure***.

4.24 If the ITS services team detect a subsequent breach or the breach is regarded severe misconduct, the Head of Department will be notified. The actions the Institute may take include:

- Counsel the student on appropriate use of the ICT services and facilities;
- Suspend or withdraw access to the email service, system access and/or network services.
- Require the student to indemnify or compensate the Institute or a provider for the reasonable loss and damage occasioned by reason of the misuse;
- If the misuse constitutes a potential breach of privacy, refer to and manage this in accordance with the ***Privacy Policy and Procedure***.

- Disciplinary action in accordance with the ***Student Code of Conduct Policy and Procedure***.

4.25 Reinstatement of ICT services to a student member will be on the authorisation of the relevant Head of Department.

4.26 Students can complain or appeal an Institute decision by accessing the ***Student Grievances and Appeals Policy and Procedure***.

4.27 In addition to any disciplinary action by the Institute, staff must report illegal activities to relevant law enforcement bodies, and the student will be held personally accountable.

Reporting

4.28 The Executive Management team will report incidents involving non-compliance with legislative requirements and severe misconduct incidents to the Audit and Risk Committee and the Governing Board.

5. QUALITY ASSURANCE

To ensure that this procedure is fit for purpose and meets the requirements of the TEQSA Compliance Frameworks the policy will be:

5.1 internally endorsed and approved by the Executive Management Team on development or review or other delegated authority;

5.2 externally reviewed as part of any independent review of the TEQSA Compliance Frameworks approved by the Governing Board;

5.3 internally reviewed by the Responsible Officer every five years from the date of approval (if not earlier).

5.4 referenced to the applicable TEQSA Compliance Frameworks requirement(s) and/or other legislation/regulation.

6. FEEDBACK

Feedback or comments on this procedure is welcomed by the Executive Management Team of the Institute.

7. ACKNOWLEDGEMENT

This procedure was developed with reference to the following:

- Melbourne University, Provision and Acceptable Use of IT Policy, 2021 (Provision and Acceptable Use of IT Policy (unimelb.edu.au))
- Swinburne University, IT Acceptable Use Guidelines (https://www.swinburne.edu.au/about/policies-regulations/it-acceptable-use/)
- Victoria University, IT Appropriate Use Policy, 2021 (IT Appropriate Use Policy / Document / Victoria University Policy Library (vu.edu.au))

- LaTrobe University, SPAM Policy, 2016 (https://policies.latrobe.edu.au/download.php?id=68&version=1)
- Ozford College of Business, Use of IT Technology and Facilities 2014

8. VERSION CONTROL

Version	Date approved	Description	Approved by
5.0	July 2018	Initial issue	EMT
6.0	August 2023	Internal Review	EMT
6.1	February 2026	Internal Review to remove under 18 student obligations after change in policy and minor edits	EMT
Related legislation/ regulation/standard	**Commonwealth** Tertiary Education Quality and Standards Act 2011 (Cth) Higher Education Standards Framework (Threshold Standards) 2021 (Cth) Education Services for Overseas Students Act (ESOS) 2000 (Cth) Education Services for Overseas Students Regulations 2019 (Cth) The National Code of Practice for Providers of Education and Training to Overseas Students 2018 (Cth) Higher Education Support Act 2003 (Cth) FEE-HELP Guidelines 2017 (Cth) Higher Education Provider Guidelines 2012 (Cth) Higher Education Support (HELP Tuition Protection Levy) Act 2020 (Cth) Higher Education (Up-front Payments Tuition Protection Levy) Act 2020 (Cth) Student Identifiers Act 2014 (Clth) Age Discrimination Act 2004 (Cth) Australian Consumer Law (Cth) Australian Human Rights Commission Act 1986 (Cth) Copyright Act 1968 (Cth) Crimes Act 1914 (Cth) Disability Discrimination Act 1992 (Cth) Disability Standards for Education 2005 (Cth) Fair Work Act 2009 (Cth)		

	Fair Work Regulations 2009 (Cth) Privacy Act 1988 (Cth) Racial Discrimination Act 1975 (Cth) Sex Discrimination Act 1984 (Cth) Sexual Offence Crimes Act 1958 (Cth) SPAM Act 2003 (Cth) Workplace Gender Equality Act 2012 (Cth) **Victoria** Accident Compensation (Occupational Health and Safety) Act 1996 (Vic) Australian Consumer Law and Fair Trading Act 2012 (Vic) Charter of Human Rights and Responsibilities Act 2006 Charter of Human Rights and Responsibilities (General) Regulations 2017 Competition and Consumer Act 2010 (Vic) Compliance Code Psychological Health (Vic) Corporations (Victoria) Act 1990 (Vic) Crimes Act 1958 (Vic) Disability Act 2006 (Vic) Equal Opportunity Act 2010 (Vic) Gender Equality Act 2020 Health Records Act 2001 (Vic), Mental Health and Wellbeing Act 2022 (Vic)Occupational Health and Safety Act 2004 (Vic) Occupational Health and Safety Regulations 2017 (Vic) Occupational Health and Safety (Psychological Health) Regulations 2025 (Vic) Privacy and Data Protection Act 2014 (Vic), Public Records Act 1973 (Vic) Racial and Religious Tolerance Act 2001 (Vic) Spent Convictions Act 2021 (Vic) **Queensland** Anti-Discrimination Act 1991 (Qld) Corporations (Administrative Actions) Act 2001 (Qld)

	Crime and Corruption Act 2001 (Qld) Disability Services Act 2006 (Qld) Domestic and Family Violence Protection Regulation 2023 (Qld) Domestic and Family Violence Protection Rules 2014 (Qld) Education (Work Experience) Act 1996 (Qld) Fair Trading Act 1989 (Qld) Fair Work (Commonwealth Powers) and Other Provisions Act 2009 (Qld) Health and Wellbeing Queensland Act 2019 (Qld) Holidays Act 1983 (Qld) Human Rights Act 2019 (Qld) Human Rights Regulation 2020 (Qld) Information Privacy Act 2009 (Qld) Information Privacy Regulation 2025 (Qld) Work Health and Safety Act 2011 (Qld) Work Health and Safety Regulation 2011 (Qld) Work Health and Safety and Other Legislation Amendment Act 2024 (Qld)

Note: EMT = Executive Management Team