OZFORD
Institute of Higher Education

USE OF INFORMATION TECHNOLOGY FACILITIES AND SERVICES PROCEDURE (STAFF)

Approving authority	Executive Management Team
Purpose	To provide implementation guidelines for the Use of Information Technology Facilities and Services Policy
Responsible Officer	President and CEO
Next scheduled review	August 2026
Document Location	http://www.ozford.edu.au/higher-education/policies-and-procedures/
Associated documents	Use of Information Technology Facilities and Services Policy (Staff) Academic Integrity Policy and Procedure Anti-Bullying and Harassment Policy and Procedure Anti-Discrimination Policy and Procedure Child Safety Policy and Procedure Diversity and Equity Policy and Procedure Engaging Managing and Monitoring the Performance of Education Agents Policy and Procedure Human Resources 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 (Staff) Staff Code of Conduct 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 work and communication tool that is regularly used by its staff to connect with each other, Institute students 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, for Institute purposes or in association with the Institute do so consistent with Institute guidelines for acceptable use.

Information systems and computer networks are an integral part of the Ozford Institute of Higher Education's (the Institute) business. The Institute has made a substantial investment to create and protect these systems. ICT facilities and services are provided to users to support the strategic objectives of the Institute. 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 staff when they are being used to access or are connected to the Institute's ICT facilities and services.

This procedure is designed to allow legitimate and optimal use of ICT facilities and services and to protect both users and the Institute. In particular the aims of the policy are to:

- promote the effective use of ICT by staff to enable them to work effectively in supporting students and the Institute more broadly;
- ensure that the Institute ICT resources, networks, printers, equipment and other infrastructure; are protected and available for use by staff when required;
- protect and to safeguard the information contained within the Institute's systems;
- reduce unsolicited commercial email ("Spam");
- protect the Institute and its users from activities that might expose the Institute or its users to liability.

2. SCOPE

This procedure applies to all users, including staff, contractors and other persons, who use of the Institute's ICT facilities and services.

This procedure does not apply to students or to the use of social media by staff which is the subject to the ***Social Media Policy and Procedure (Staff)***.

3. DEFINITIONS

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

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.

Serious misconduct
Serious misconduct includes but not limited to

- Acting dishonestly including any fraud in respect to the Institute, students or stakeholders;

- Knowingly making any false or misleading representation;
- Harassing or intimidating a student, a member of staff, a visitor to the Institute, or any other person, because of race, ethnic or national origin, sex, marital status, sexual preference, disability, age, political conviction, religious belief or for any other reason;
- Misuse of the 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 employee has access at or away from the Institute premises while acting as an Institute employee, in a manner which is illegal, or which is or will be detrimental to the rights or property of others;
- Theft or an action to steal, destroy or damage a facility or property of the Institute or for which the Institute is responsible.
- Any form of violence against a student, staff member or stakeholder of the Institute that is substantiated;
- A child abuse incident where the allegation is substantiated; or
- Being under the influence of alcohol or drug of dependence during working hours.

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.

There is an exemption for educational institutions. Unsolicited commercial messages may only be sent to an electronic account-holder if the following conditions have been met:

- the sending of the message is authorised by an educational institution; and
- either or both of the following subparagraphs applies:
    - the relevant electronic account-holder is, or has been, enrolled as a student at the Institute;
    - a member or former member of the household of the relevant electronic account-holder is, or has been, enrolled as a student at the Institute; and
    - the message relates to goods or services; and
    - the Institute is the supplier, or prospective supplier, of the goods or services concerned."

Where any commercial electronic messages are sent by the Institute, there must be a functioning Unsubscribe Facility at the end of each message. The messages must also have clear and accurate sender information.

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, 3G/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 The relevant Head of Department, their supervisor or the contract manager authorises ICT facilities and service access to staff.

4.2 User accounts are created by the ITS services team.

4.3 Prior to commencement or upon engagement, the Head of Department notify the ITS services team to set up access for new users.

4.4 Users are required to read and sign the ***Use of Information Technology Facilities and Services Policy and Procedure (Staff)*** during their induction.

Role and availability of the ITS team

4.5 The ITS services team

- arranges for users to access basic network drives and folders relevant to their work functions. Additional network drive and folder access requires approval from the Head of Department, their supervisor or the contract manager.
- creates a unique username and password for each user to access ICT facilities and services.
- monitors the Institute ICT facilities and services.
- ensures that the centralised authentication system is implemented, and that only currently authorised users have access.
- ensures that users are trained to use ICT facilities and services and receive support to enable effective use of ICT facilities and services.

4.6 The Institute's ICT facilities and services are available on campus during business hours: Monday to Friday 8.30 am – 5.00 pm.

4.7 Additional access may be approved by relevant Head of Department, their supervisor or the contract manager.

4.8 Users can access online facilities including webmail and Moodle out of business hours.

4.9 Users who require assistance with ICT facilities and services should contact ITS services team : itservicedesk@ozford.edu.au

SPAM

4.10 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.

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

4.12 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.

4.13 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.

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

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

Security of ICT facilities and services

4.16 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. Remote access is authorised by the Head of Department or the President and CEO:
- done via VDI (virtual computer) solution;
- user accesses via remote desktop protocol/software; and,
- request to access the desktop directed to ITS services team, which enable and disable for period required.
- Monitors and maintains the web servers that are hosted independently on external services and not linked to internal systems.
- Monitors the Institute student administration system (ParadigmEMS) - hosted service managed by OIHE administrator

Backup of Information Systems

4.17 The ITS services team

- ensures the ongoing backup of Information Systems, as well as the testing of backups and the offsite storage of backup media.
- ensures that an appropriate Disaster Recovery Plan is developed and in place and that these are aligned with the Business Continuity Plan
- ensures library system users are removed from system after 3 years of inactivity.

4.18 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.

Termination of access

4.19 The relevant Head of Department, their supervisor or the contract manager will notify the ITS services team that access should be removed at close of business of the last day of employment or engagement or when a contract is terminated by the Institute.

4.20 The ITS services team will:

- compile a list of all user accounts and send to the Head of Department for review every 3-6 months.
- Remove all deactivated user 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

4.21 Any external or personal equipment that users 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.

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

4.23 The user is responsible for selecting, using and administering the "Cloud" computing service(s) and for ensuring that the service(s) is "fit for purpose" at the Institute. The terms and condition of using such service(s) must be forwarded and reviewed by the ITS services team before use commences.

4.24 Access to the service(s) if storing or processing the Institute information must be secured and restricted only to appropriate users.

4.25 The ***Records Management Policy and Procedure*** sets out the processes for managing Institute records. All data, including copies/backups electronic or otherwise, needs to be irretrievably erased if no longer required by the Institute.

Breaches of the Policy and this Procedure

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

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

4.27 The Head of Department, supervisor or contract manager will have responsibility for addressing user conduct as set out in the ***Human Resources Policy and Procedure (Manual),*** employment contract or engagement contract.

4.28 If the ITS Services team detect a subsequent breach or the breach is regarded serious misconduct, the Head of Department or president and CEO will be notified. The actions the Institute may take include:

- Counsel the user 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 user 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 ***Human Resources Policy and Procedure (Manual),*** employment contract or engagement contract.

4.29 Reinstatement of ICT services to a staff member will be on the authorisation of the Head of Department or President and CEO.

4.30 Users can complain or appeal an Institute decision by accessing the ***Human Resources Policy and Procedure (Manual)*** or the processes set out in the person's employment contract or engagement contract.

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

Reporting

4.32 The Executive Management team will report incidents involving non-compliance with legislative requirements and serious 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 HES Threshold Standards the policy will be:

5.1 internally endorsed by the Executive Management Team on development or review, prior to approval by Governing Board, or the Academic Board or other delegated authority;

5.2 externally reviewed as part of any independent review of the HES Threshold Standards approved by the Governing Board;

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

5.4 referenced to the applicable HES threshold Standard 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 ICT Policy, 2021 (Provision and Acceptable Use of ICT Policy (unimelb.edu.au))
- Swinburne University, ICT Acceptable Use Guidelines (https://www.swinburne.edu.au/about/policies-regulations/it-acceptable-use/)

- Victoria University, ICT 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 ICT Technology and Facilities 2014

8. VERSION CONTROL

Version	Date approved	Description	Approved by
5.0	June 2018	Initial issue	CEO/EMT
6.0	August 2023	Internal Review	EMT
Related legislation/ regulation/standard	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) Victorian Child Safe Standards Occupational Health and Safety Act 2004 (Vic) Racial Discrimination Act 1975 (Cth) Sex Discrimination Act 1984 (Cth) Disability Discrimination Act 1992 (Cth) Disability Standards for Education 2005 (Cth) Australian Human Rights Commission Act 1986 (Cth) Workplace Gender Equality Act 2012 (Cth) Age Discrimination Act 2004 (Cth) Fair Work Act 2009 (Cth) Equal Opportunity Act 2010 Racial and Religious Tolerance Act 2001 (Vic) Spent Convictions Act 2021 SPAM Act 2003 (Cth) Copyright Act 1968 (Cth) Privacy Act 1988 (Cth) Privacy and Data Protection Act 2014 (Vic), Health Records Act 2001 (Vic), Australian Consumer Law (Cth)		

Note: EMT = Executive Management team