OZFORD
Institute of Higher Education

USE OF INFORMATION TECHNOLOGY FACILITIES AND SERVICES POLICY (STAFF)

Approving authority	Governing Board
Purpose	This policy provides all users (including the public) with guidelines for the appropriate use of Use of Information and Communication Technology Facilities and Services
Responsible Officer	President and CEO
Next scheduled review	September 2026
Document Location	http://www.ozford.edu.au/higher-education/policies-and-procedures/
Associated documents	Use of Information Technology Facilities and Services Procedure (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 students when they are being used to access or are connected to the Institute's ICT facilities and services.

This policy 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 IT by staff to enable them to work effectively in supporting students and the Institute more broadly;
- ensure that the Institute IT 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 policy applies to all users, including staff, contractors and other persons, who use of the Institute's ICT facilities and services.

This policy 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

Commercial Electronic Message:
An Electronic message which has a commercial purpose that includes an offer to supply or sell goods or services or to advertise or promote goods and includes for example and email sent offering to supply or promote educational services or business opportunities.

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 accountholder 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 accountholder is, or has been, enrolled as a student at the Institute;
    - a member or former member of the household of the relevant electronic accountholder 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. POLICY

Use of ICT facilities and services

4.1 Users must take responsibility for using ICT facilities and services in an ethical secure and legal manner; having regard for the objectives of the Institute and the privacy, rights and sensitivities of other people.

4.2 Staff must use the Institute's ICT facilities and services in an ethical, secure and legal manner; having regard for the privacy, rights and sensitivities of other users.

4.3 It is the responsibility of staff to make themselves aware of the policies, procedures and guidelines related to Information Technology Services and conduct their activities accordingly.

4.4 Staff must comply with this Use of Information Technology Facilities and Services Policy, the associated Procedure and the following policies:

- ***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***
- ***Human Resources Policy and Procedure (Manual)***

- ***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***

4.5 The Institute ICT facilities and services including the email accounts are provided for Institute academic and business related communications. Any personal use of ICT facilities and services should be incidental and not interfere with the work of others or the operation of the Institute.

4.6 Users may provide their Institute email address to known friends, family and associates.

4.7 Users are responsible for exercising good judgment regarding personal use of the Institute resources.

4.8 The use of the Institute resources for unreasonable or excessive personal use or conducting any activities, which are not academic, or Institute business related, is strictly prohibited. All ICT use must be undertaken with the full knowledge and approval of Head of Department and the ITS services team. In approving use, the ITS services team requires that the activity meets the security requirements set out in this policy.

4.9 Personal profile images uploaded to Institute systems must be professional, appropriate and respectful.

4.10 Institute resources provided to or accessed by users may contain proprietary and other confidential information about the Institute, its clients, students, users and suppliers, such confidential information remains the property of the Institute at all times.

4.11 Users must not copy, duplicate (except for backup purposes), disclose, or allow anyone else to copy or duplicate any confidential information. The use of personal data storage devices to transfer stored data to or from the Institute's ICT facilities and services is strictly prohibited.

4.12 Costs incurred by the Institute due to excessive personal use may be recovered directly from the individual concerned and may lead to further disciplinary/legal actions.

4.13 If an employee leaves the employ of the Institute for any reason, all confidential information (including copies) and any Institute ICT equipment or data files in the employee's possession or control must be immediately returned to the Institute.

4.14 Staff who are alleged to have misused Institute ICT facilities and services are subject to investigation and, if misuse is established, action will be taken, as detailed in this policy.

Monitoring

4.1 While the Institute desires to provide a reasonable level of privacy, users should be aware of the Institute's ***Privacy Policy and Procedure*** and that the data they create or store on the Institute resources, or while using the Institute resources, is the property of the Institute. This includes but is not limited to emails sent and received from staff and student email accounts, emails retained in central archive, voicemail, text messages and instant messages.

4.15 The use of personal data storage devices to transfer stored data to or from the Institute's ICT resources is strictly prohibited unless undertaken with the full knowledge and approval of member of the Executive Management Team and meets the security requirements specified in this policy.

4.16 The Institute will monitor users' use of the Institute ICT facilities and services. The Institute has systems to monitor the Institute's ICT equipment, systems and network traffic of users.

4.17 The Institute can access and audit networks and systems (including electronic mail systems and information stored in the network) on a periodic basis for any business purpose including but not limited to:

- security, network and maintenance purposes;
- assessing the level of personal use;
- accessing or retrieving email or data that may have been deleted;
- ensuring that there is no illegal or improper use of email or the internet;
- monitoring potential breaches of confidential information;
- assessing any violations that may constitute harassment or discrimination;
- investigating complaints of users, clients or suppliers;
- obtaining all data about the use of email and the internet for strategic purposes; and,
- assessing whether this policy is being adhered to and identifying any possible breaches.

Information Security

4.18 Users must take all reasonable precautions for the safety and protection of Institute data and information assets from unauthorised access or disclosure in order to minimise risk by adhering to the handling requirements and security controls.

4.19 Users are responsible for the security of their passwords and the use of the Institute ICT facilities and services via their accounts.

- Passwords chosen by staff must not be easily be guessed or predicted
- Passwords must remain secure, and users should refrain from disclosing their password to any person and, from sharing accounts.

- Users must change their password regularly (and immediately if it becomes known by another person)
- All PCs, laptops, tablets, mobile devices and workstations should be secured by logging off or locking the workstation when the system is unattended.
- Users must protect the security of data held on mobile systems (eg phones, laptops, memory sticks and other storage mediums), including by maintaining reasonable virus control measures where possible.

4.20 Users will be held responsible for all actions including any infringement carried out by a third-party given access to their accounts. To the extent allowed by law, the Institute is not liable for loss, damage, or consequential loss or damage, arising directly or indirectly from:

- use or misuse of any facilities;
- loss of data or interference with data stored on any facilities;
- interference with or damage to equipment used in conjunction with any facilities; or
- any acts taken or decisions made not in accordance with this or any other policy.

4.21 All computers and devices connected to the Institute network including computers and devices not owned or managed by the Institute, must have the current operating system patches applied to them and be equipped with the latest antivirus software, either by automated download or manual update.

External IT Equipment / Cloud services and solutions

4.22 Any external or personal equipment that users wish to be connected to the Institute's networks 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.

Electronic Mail Guidelines

4.23 Institute email accounts are provided for academic and business-related communications of the Institute.

4.24 Email is an official method of communication for staff and students. Mass electronic communications are moderated.

4.25 A signature and disclaimer (as defined at the sole discretion of the Institute) should be present on all external email correspondence.

4.26 The contents and size of employee email accounts will be defined by the Institute's ITS services team.

4.27 Some types of emails and attachments will be blocked by the Institute's systems to help secure the environment from spam, viruses, worms or other harmful software.

4.28 The Institute will comply with the *SPAM Act 2003*. Where any commercial electronic messages are sent, there will be a functioning Unsubscribe Facility at the end of each message. The messages will also have clear and accurate sender information.

Personal Mobile Phone, Handheld Devices and Computers

4.29 Personal mobile phone, handheld devices and computers are the personal belongings of staff. It is the owner's responsibility to ensure they are kept secured and safe. Staff are expected to use them in a safe, responsible and ethical manner at all times. This includes:

- keeping the device on silent during class times; only making or answering calls or messages outside of lesson times (except for approved learning purposes);
- respecting others and communicating with others in a supportive manner, never verbally or in writing or participating in bullying (for example, harassing phone calls/text messages, forwarding messages and supporting others in harmful, inappropriate or hurtful online behaviours);
- protecting own privacy; not giving out any personal details, including name, telephone number, address, passwords and images;
- protecting the privacy of others; never posting or forwarding their personal details or images without their consent - Carefully considering the content before uploading or posting online;
- investigating the terms and conditions (e.g. age restrictions, parental consent requirements). If unclear seek further explanation from a teacher/manager;
- not bringing to the Institute or downloading unauthorised programs, including games;
- respecting the privacy of others; only taking photos or recording sound or video when formal consent has been given or when recording is part of an approved lesson; and
- obtaining appropriate (written) consent from individuals who appear in images or sound and video recordings before forwarding them to other people or posting/ uploading them to online spaces.

Prohibited Activities

4.30 Under no circumstances is a user authorised to engage in any activity that is illegal under local, state, federal or international law while using the Institute ICT services and facilities.

4.31 The following activities are expressly prohibited:

- violations of the rights of any person or the Institute protected by confidentiality, copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to the installation or distribution of "pirated" or other software products that are not appropriately licensed for use, or the duplication or transmission of copyrighted or otherwise protected materials. This prohibition also applies to materials that are considered "Confidential";
- sending spam using the Institute resources;
- the use of any peer-to-peer file sharing software or websites, including but not limited to BitTorrent, eMule, LimeWire or Ares;

- the use of any IRC or messenger software or websites, including but not limited to Facebook Messenger or other "Messengers", IRC or "chat" clients (except that, for the avoidance of doubt, Voice Over IP products are allowed for the Institute business purposes only, where the employee has first registered the username and service with the Institute's IT services division and obtained his or her consent to such use);
- unless specifically for the Institute academic or business purposes, posting or subscribing to newsgroups, online discussion boards or email list groups;
- using the Institute resources to actively engage in procuring or transmitting material that is in violation of sexual harassment, privacy, discrimination or workplace laws including but not limited material which is offensive, obscene, threatening, pornographic, defamatory, discriminatory, insulting, inappropriate, disruptive, intimidating or in violation of a person's privacy;
- effecting disruptions to, or interfering with, any other computer or network;
- using any form of network monitoring which will intercept data not specifically intended for the employee, unless this activity is a part of the employee's normal job responsibilities;
- circumventing user authentication or security of any host, network or account;
- providing information about, or lists of, the Institute's users, customers or potential customers to any third party; or outside the Institute;
- activities which discredit the Institute or its users;
- using electronic mail or the internet for political, religious, private commercial, personal profit making, gambling or personal advertising purposes;
- unauthorised use, or forging, of email header information;
- connecting to the internet, or sending email through, an anonymous proxy server or similar conveyance designed to obfuscate the user's identity;
- creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type;
- installing any software that is not approved by the IT department;
- unauthorised accessing, copying of the Institute information to a personal USB memory stick, hard disk or removable storage device/cloud (whether it is a to mobile phone, tablet, music player, cloud storage or otherwise);
- the 'ripping', copying or storage of music for any purpose; and,
- the use of third party email accounts for carrying on the Institute business (with the exception of the use of a third-party email server to send an email, where the return address is the Institute provided email address).

Termination of Access

4.32 User access will be removed at close of business of the last day of employment or engagement or when a contract is terminated by the Institute.

ICT Resources Loss/Damage

4.33 All ICT infrastructures are covered by a manufacturer's warranty. The warranty covers manufacturer's defects and normal use of the device. It does not cover negligence, abuse or malicious damage.

4.34 The Institute may require users to pay for any loss or damage to the Institute's IT resources caused by their negligence, abuse or malicious actions.

Breach of ICT Use Policy

4.35 All breaches of this Policy will be treated seriously.

4.36 Staff are expected to report any wilful damage, suspected breaches of legislation, regulations and any actions specified in this policy. Staff must also report any lost or stolen Institute owned or managed computing devices immediately.

4.37 Staff who becomes aware any misconduct by any student or staff member that infringes the rights of another person, or that the effect of any use of any facilities is to infringe such rights, must notify the Institute's Executive Management team.

4.38 The outcome of a substantiated breach of this Policy may include, is not limited to the following:

- Counsel 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 users 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 for staff will be in accordance with the ***Human Resources Policy and Procedure (Manual)***.
- Disciplinary actions for other users will be as set out in their contract with the Institute.

4.39 The ITS services team is responsible for managing any disruption to or impact on ICT services and facilities caused by an ICT breach.

4.40 The Head of Department is responsible for dealing with any breach of this policy by a user.

4.41 Staff can access the ***Human Resources Policy and Procedure (Manual)*** or the process set out in their Employment agreement if they are aggrieved by an Institute decision.

4.42 In addition to any disciplinary action by the Institute, a breach of this policy this may lead to civil or criminal proceedings and penalties, which the Institute may report to relevant law enforcement bodies and for which the staff will be held personally accountable.

Reporting

4.43 All incidents involving non-compliance with legislative requirements and serious misconduct incidents will be reported to the Audit and Risk Committee and the Governing Board.

5. QUALITY ASSURANCE

To ensure that this policy 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 policy is welcomed by the Executive Management Team of the Institute.

7. ACKNOWLEDGEMENT

This policy 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
4.0	June 2018	Initial issue	GB
5.0	July 2018	Internal review with Several grammatical and editorial amendments	GB
6.0	September 2023	Internal Review	GB

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)

Notes:

GB = Governing Board

EMT = Executive Management team (minor changes only)