Use of Information Technology Facilities and Services Policy (Students)

Approving authority	Governing Board
Purpose	Roles and Responsibilities are as detailed throughout this Policy – applied to all User including Public
Responsible Officer	IT Manager
Next scheduled review	July 2021
Document Location	http://www.ozford.edu.au/higher-education/policies-and-procedures/
Associated documents	SPAM Act 2003 (Commonwealth) Copyright Act 2003 (Commonwealth) Use of Information Technology Facilities and Services Procedure (Student)

1. PRINCIPLES

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. IT facilities and services are provided to users to support the strategic objectives of the Institute

This policy is designed to allow legitimate and optimal use of IT facilities and services and to protect both students and the Institute.

In particular the aims of the policy are to:

- promote the effective use of IT by students to enable them to work effectively in successfully meeting the requirements of their course;
- ensure that the Institute IT resources, networks, printers, equipment and other infrastructure; 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

The policy applies to

2.1 to all students who use of the Institute's IT facilities and services;

2.2 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;

2.3 the use of the remote system, accessed via IT facilities and services, is also covered by this policy;

2.4 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 IT facilities and services.

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

3. DEFINITIONS

The Institute - Ozford Institute of Higher Education Pty Ltd.
The Institute Information Technology (IT) resources - means all computer, telecommunications and IT 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;
Users- includes 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 or its third-party agents.
Use - means use of the Institute IT resources 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.
Personal data storage device – is any device, that is the personal belonging of the user, that when connected to the Institute's IT resources is able to transfer stored data to or from the device.
Cloud services– is where providers deliver services online which are accessed from a web browser, computers and applications

4. POLICY

Users must take responsibility for using IT 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.

4.1. Privacy

4.1.1 While the Institute desires to provide a reasonable level of privacy, users should be aware that the data they create or store on the Institute resources, or while using the Institute resources, is the property of the Institute.

4.1.2 Students are responsible for exercising good judgment regarding personal use of the Institute resources.

4.1.3 The use of the Institute resources for conducting business, which is not the business of the Institute, is strictly prohibited.

4.1.4 The use of personal data storage devices to transfer stored data to or from the Institute's IT resources is strictly prohibited unless undertaken with the full knowledge and approval of member of the IT Services manager and meets the security requirements specified in 4.2

4.1.5 The Institute may monitor users' use of the Institute resources.

4.1.6 The Institute may monitor the equipment, systems and network traffic of users at any time.

4.1.7 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.

4.2. Security

4.2.1 Students are responsible for the security of their passwords and the use of the Institute resources via their accounts.

4.2.2 Passwords must remain secure and students should refrain from disclosing their password to any person and, from sharing accounts.

4.2.3 All PCs, laptops, tablets, mobile devices and workstations should be secured by logging off or locking the workstation when the system is unattended.

4.2.4 Institute email accounts are provided for academic and study related communications

4.2.5 Students may provide their Institute email address to known friends, family and associates.

4.2.6 Students must not copy, duplicate (except for backup purposes), disclose, or allow anyone else to copy or duplicate any confidential information.

4.3. External IT Equipment / Cloud services and solutions

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

4.3.2 The accessing, storing and working on 'Cloud' services must abide by the same legislations and the Institute policies with regards to access, privacy, security and data breach.

4.4. Electronic Mail Guidelines

4.4.1 A signature should be present on all email correspondence.

4.4.2 The contents and size of student email accounts will be defined by the Institute's IT services division.

4.4.3 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.

4.5. Personal Mobile Phone, Handheld Devices and Computers

Personal mobile phone, handheld devices and computers are the personal belongings of students. It is the student's responsibility to ensure they are kept secured and safe. Students 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.

4.6. Prohibited Activities

Under no circumstances is a student authorised to engage in any activity that is illegal under local, state, federal or international law while using the Institute resources.

4.6.1 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 name 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).

4.7. ICT Resources Loss/Damage

4.7.1 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.

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

4.8. Breach of ICT Use Policy

4.8.1 Students are expected to report any wilful damage, suspected breaches of legislation, regulations and any actions specified in 4.6

4.8.2 Non-adherence with this policy will be regarded as a serious matter and appropriate action may be taken.

4.8.3 The Head of IT is responsible in the first instance for handling potential breaches.

4.8.4 The Institute will report any suspected illegal activities to appropriate authorities.

5 QUALITITY 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 listed responsible officers of the Institute.

7 ACKNOWLEDGEMENTS

This policy was initially developed with reference to the following policy;
Ozford College of Business, 2014

8 VERSION CONTROL

Version	Date approved	Description	Approved by
4.0	30 June 2018	Initial issue	CEO
5.0	30 July 2018	Several grammatical and editorial amendments	
Related legislation/ regulation/standard	HES Threshold Standards 2015, HES Threshold Standards 2015- Representation, Information and Information Management		