Use of Information Technology Facilities and Services Procedure (Students)

Approving authority	Executive Management Team
Purpose	To provide implementation guidelines for the Use of Information Technology Facilities and Services Policy
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 Policy (Students)

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 procedure 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 procedure;

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 procedure 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 students 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. PROCEDURE

4.1 Authorise of Access to IT facilities and services

4.1.1 Students are informed to read IT Acceptance Use Policy and IT Acceptance Use Procedure during orientation.
4.1.2 The relevant Manager or Head of Department authorises IT facilities and service access to students. User accounts are created and deactivated upon request from the relevant manager.

4.2 Access and Monitor IT facilities and services

The IT Manager
4.2.1 Arranges for students to access basic network drives and folders relevant to their work functions. Additional network drive and folder access requires approval from the relevant manager.
4.2.2 Creates a unique username and password for each student to access IT facilities and service at the Institute.
4.2.3 Monitors the Institute IT network infrastructure and address any concerns to CEO.
4.2.4 Ensures that the centralised authentication system is implemented and that only currently authorised students have access.
4.2.5 Ensures that students are trained to use IT facilities and services.

4.3 Availability of IT facilities and services

IT 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 relevant manager. Students can also access online facilities including webmail and Moodle out of business hours.

4.4 Spam

If spam is detected – it is normally automatically quarantined by firewall, sends a notification email to the recipient to with a link to release the email if it is legitimate. If it is not filtered, students are trained to either delete or contact IT for support.

4.5 **Security of IT facilities and services**

The IT Manager

4.5.1 Monitors all logins onto computer systems

4.5.2 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

4.6 Breaches / Prohibited Activities

4.6.1 The IT manager will in the first instance notify the students member of any suspected breaches of the Use of IT Facilities and Services policy.

4.6.2 The IT manager will immediately deny/restrict access to IT services if ongoing or subsequent breaches of the Use of IT Facilities and Services policy are detected and advise the relevant Head of department or Vice president.

4.6.3 The IT Manager may restrict access to IT services after being instructed by a relevant HoD.

4.6.4 Reinstatement of IT services to a student member will be on the authorisation of the relevant HoD or Vice President.

4.7 Backup/Currency of Information Systems

IT Manager

4.7.1 Compiles a list of all students accounts and send to the Institute administration officer/managers for review every 3-6 months

4.7.2 Removes all deactivated students accounts from the systems every 12 months.

4.7.3 Ensures the ongoing backup of Information Systems, as well as the testing of backups and the offsite storage of backup media.

4.7.4 Ensures library system - users/patron from the system will be removed from system after 3 years of inactivity.

4.8 **Secure IT assets**

4.8.1 Physical security, floor access and room access are locked off and secured out of working hours and are limited to people with keys and access card, which is controlled.

4.9 External IT Equipment / Cloud services and solutions

4.9.1 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.

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

4.9.3 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.

4.9.4 The terms and condition of using such service(s) must be forwarded and reviewed by the Institute's IT services division before use commences.

4.9.5 Access to the service(s) if storing or processing the Institute information must be secured and restricted only to appropriate users. All data (including copies/backups electronic or otherwise) needs to be irretrievably erased if no longer used.

4.10IT facilities and services assistance

Students who require assistance with IT facilities and services should contact IT Manager : itservicedesk@ozford.edu.au

5. QUALITY ASSURANCE

To ensure that this procedure is fit for purpose and meet the requirements of the HES Threshold Standards the procedure will be:

5.1 internally approved by the Executive Management Team on development or review
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 listed responsible officers of the Institute.

7. VERSION CONTROL

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