Information Technology Acceptable Use Policy

Information systems and computer networks are an integral part of the Company's business. The Company has made a substantial investment to create and protect these systems. As such, access to these systems cannot be provided unconditionally or without limits. The Company reserves the right to add a future user-pay cost component for internet and printing as deemed appropriate.

The purpose of this policy is to outline the acceptable use by Employees of Company Resources. This policy is in place to protect both Employees and the Company. The aims of the policy are:

1. To protect Company Resources, networks, printers, equipment and other infrastructure and to safeguard the information contained within the Company's systems;

2. To reduce unsolicited commercial email ("Spam");

3. To promote the use of Company Resources to achieve the Company's commercial aims; and

4. To protect the Company and its Employees from activities that might expose the Company or its Employees to liability.

5. To expressly inform Employees that everything that you do while connected to the network canbe monitored and viewed by authorized personnel.

A. Definitions

"**Company**" means, Ozford Institute of Higher Education Pty Ltd

"**Company 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 Company or its affiliates and all Company networks, servers and off-site services that the Company subscribes to;

"**Employees**" includes all full-time and part-time employees of the Company as well as all temporary and contract staff engaged by the Company or its third party agents; and
"**use**" means use of Company Resources by Employees including but not limited to internet and email (both Company and external email) access. This includes the connection of any device, regardless of ownership or purpose, to any Company Resources and the connection of a device to a mobile network (GSM, Wifi, WiMAX, 3G or other mobile network), where the number, service, SIM or bill is paid for or provided by the Company.

B. Privacy

While the Company desires to provide a reasonable level of privacy, Employees should be aware that the data they create on Company Resources, or while using Company Resources, is the property of the Company. The Company cannot guarantee the confidentiality of information stored on any computer device belonging to the Company or connected to Company Resources. Employees are responsible for exercising good judgment regarding the reasonableness of personal use of Company Resources. The use of Company Resources for the carrying on of any business which is not the business of the Company is strictly prohibited. Should personal use by

an Employee of Company Resources become excessive (such determination to be made at the Company's sole discretion), then the Company may restrict that Employee's access to Company Resources or take such other action as the Company deems appropriate in the circumstances.
The Company may monitor Employee use of Company Resources. Authorised individuals within the Company may monitor the equipment, systems and network traffic of Employees at any time. The Company reserves the right to 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 Employees, 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.

C. Security
Employees are responsible for the security of their passwords and the use of Company Resources via their accounts. Passwords must remain secure and Employees are expressly prohibited from disclosing their password to any person and from sharing accounts.

All PCs, laptops and workstations should be secured by logging off or locking the workstation when the system is unattended.
Company email accounts are provided for business related communications of the Company only. Employees may provide their Company email address to known friends, family and associates.

Company Resources provided to or accessed by Employees may contain proprietary and other confidential information about the Company, its clients, students, Employees and suppliers ("**Confidential Information**"). Such information remains the property of the Company at all times. Employees must not copy, duplicate (except for backup purposes), disclose, or allow anyone else to copy or duplicate any Confidential Information. If an Employee leaves the employ of the Company for any reason, all Confidential Information (including copies) and any Company Resources in the Employee's possession or control must be immediately returned to the Company.

D. External IT Equipment
Any equipment that is connected to Company's networks by an Employee must first be approved by the Company's IT Services Division. Approval will be withheld unless there is an active anti-virus program running on the equipment within current anti-virus definitions. Antivirus software is available from the Company's IT Services Division.

E. Electronic Mail Guidelines
A signature and disclaimer (as defined at the sole discretion of the Company) should be present on all external email correspondence.
The contents and size of Employee email accounts must be appropriately maintained by Employees to occupy no more than size limit notified by the Company's IT Services Division from time to time. The Company's servers may enforce size restrictions automatically and notify Employees when the limit is exceeded.

Some types of emails and attachments are blocked by the Company's systems to help secure the environment from spam, viruses, worms or other harmful software. This list may change at any time without notice.

F: Reporting breaches
Employees are expected to report any willful damage, suspected breaches of legislation, regulations and Company policies. All such reports will be treated in a confidential and responsible manner. The Company will protect the interests of such Employees reporting any breaches or suspected breaches in good faith and in a responsible way.

G. Prohibited Activities
Under no circumstances is an Employee authorised to engage in any activity that is illegal under local, State, Federal or international law while using Company Resources.
In addition, the following activities are expressly prohibited:

- Violations of the rights of any person or company 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 Company Resources;

- The use of any peer-to-peer file sharing software or websites, including but not limited to BitTorrent, KaZAA, Grokster or Morpheus;

- The use of any IRC or messenger software or websites, including but not limited to AOL Messenger or other "Messengers", IRC or "chat" clients (except that, for the avoidance of doubt, Voice Over IP products are allowed for Company business purposes only, where the Employee has first registered the username and service with the Company's IT Services Division and obtained his or her consent to such use) ;

- Unless specifically for Company business purposes, posting or subscribing to newsgroups, online discussion boards or email list groups;

- Using Company 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 Company's Employees, customers or potential customers to any third party;
- Activities which discredit the Company or its Employees;
- 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 copying of Company information to a personal USB memory stick, hard disk or removable storage player (whether it is a music player or otherwise);
- The 'ripping', copying or storage of music for any purpose;
- The use of third party email accounts for carrying on Company business (with the exception of the use of a third party email server to send an email, where the return address is the Company provided email address).

H. General

This policy may be changed at any time, without prior notice, at the sole discretion of the Company. Any changes will be provided Employees in writing (or by email) and shall have full force and effect as if originally incorporated herein. The latest version of this policy will be displayed on the IT Services webpage on the Company Intranet.

Important Notice: An Employee's breach of this policy shall be grounds for disciplinary action and may result in termination of employment.
The Company's failure to enforce any provision of this policy shall not operate to invalidate the Company's rights to enforce any of the provisions of this policy, including subsequent changes. Should any provision of this policy be deemed invalid, it shall not effect nor invalidate any other provision.

Acknowledgement of IT Acceptable Use Policy

This form is used to acknowledge receipt of, and compliance with, the Company's IT Acceptable Use Policy.

By signing below, I acknowledge and agree that:

1. I have read and understood the Company's IT Acceptable Use Policy; and
2. In consideration of the Company continuing to allow me access to Company Resources, I agree to comply with, and be bound by, the terms of the Company's IT Acceptable Use Policy.

Employee Signature:……..

Employee Name:……..

Date: