Computer, Internet, Email and Telecommunications Policy

1. INTRODUCTION

The purpose of this policy is to provide employees/ volunteers with information regarding:

- The use of internet technology
- Controls in accessing unauthorised and unacceptable websites
- The receipt and distribution of inappropriate email
- Downloading illegal and/or copyright material, and
- The use of telecommunication equipment.

2. SCOPE

This policy applies to all permanent, fixed term, part-time and casual employees and volunteers of the UQU.

3. RESPONSIBILITY

It is the responsibility of all employees/volunteers to ensure they are aware of the restrictions and ethical conduct round the use of technologies including email, access to unsuitable websites, downloading data, and telecommunication usage.

4. RISK

Fines for illegal copyright breaches by both individuals and UQU.

5. APPLICATION

1. Under no circumstances will UQU computer or telecommunication facilities be utilised for:
   - Accessing/transmission of unethical material such as but not limited to pornography
   - Active participation in any material other than for the purpose of UQU commercial advantage
   - Harassment
   - Defamation/vilification
   - Breach of copyright
   - Breach of confidentiality
   - Illegal activity of any kind, or
   - Any activity that would bring the organisation into disrepute.

   Note: UQU conducts routine surveillance of technology usage to ensure there are no breaches of this provision. Any wilful breach of these prohibitions may result in disciplinary action up to and including termination of employment.

2. UQU does not engage in monitoring or surveillance of employee/volunteer personal correspondence. Should surveillance of correspondence become necessary for legal purposes UQU shall warn, in writing, of any intended surveillance of personal correspondence, except in circumstances where the organisation has obtained legal authorisation.

3. No software program or data other than UQU's intellectual property or other devices will be installed or run without the authorisation of the appropriate manager or authorised person. (Legislation prescribes heavy fines for illegal copyright breaches by both individuals and UQU).

4. Only UQU's purchased software and hardware are to be used on the network. External trainers, suppliers or other individuals using third party equipment are not to have access to UQU's network without express authorisation of the appropriate manager.

5. Downloading of material on UQU mobile phones is prohibited. If downloads are performed that incur a charge, this will be forwarded to the employee/volunteer for payment.

6. UQU computers and equipment are not to be modified or interfered with in any way by unauthorised employee/s.

7. Screen savers will either be windows standard settings, as installed, or personal messages deemed not to offend.

8. Screen background will remain windows standard settings, as installed, a background accessible from the installed operating system, or personal photos which are deemed not to offend.

9. Equipment configurations will remain as installed by the authorised Information Technology consultant or authorised staff. If configuration needs altering, the alteration shall be approved by management prior to alteration.

10. Computers are to remain in a state that will allow other employees/volunteers to the equipment by logging on using their user name and password at any time. If the password is changed you must inform your manager of the change.
    - Maintaining security of files is the responsibility of every employee
    - The use of outlook is for the intent of business nature, however, there may be occasions when messages are of a personal nature both incoming and outgoing.

11. All correspondence remains the property of UQU and as such is subject to examination by authorised personnel at any time. Emails may be viewed by another employee/volunteer in their absence to ensure stakeholders are service accordingly.
    - Offensive material in any form is not to be stored on any of UQU's technical equipment.
    - Offensive material is not to be transmitted (including using telecommunication equipment and systems for transmission), copied, or executed in form from UQU equipment or systems.
    - The internet is to be used primarily for business purposes only. Some private use is acceptable during breaks or before and after hours.
    - Computers are to be used in a professional manner. They are considered a business tool to improve business efficiency, and not for the use of accessing games or inappropriate websites.

- No food or beverage is to be placed near hardware, software, or data storage media.
- Monitors are to be turned off in shutdown mode. This is to reduce risk of fire after hours.
- Data storage media is not to be placed where physical or magnetic damage (where applicable) may occur.
- All employees/volunteers are obligated to report to management any action or materials which may be deemed offensive, and/or the inappropriate use of technology.
- Employee/s or volunteer emails should be redirected to another employee/volunteer if they are absent for an extended period of time. If employees/volunteers do not do so UQU reserves the right to redirect their emails to another employee/s or volunteers address during their absence.

For further information regarding this policy please contact the Human Resources and/or Information Technology Departments.