IT 1.0 Information Technology Acceptable Use Policy

Policy Category: Management
Document Owner: Vice-Chancellor and President
Responsible Officer: Director, Operations and Services
Review Date: 2 October 2014
File Number:

<table>
<thead>
<tr>
<th>Related Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud Control Policy</td>
</tr>
<tr>
<td>Research Misconduct Policy</td>
</tr>
<tr>
<td>Staff Code of Conduct</td>
</tr>
<tr>
<td>Staff Misconduct Policy</td>
</tr>
<tr>
<td>Student Charter</td>
</tr>
<tr>
<td>Student Misconduct Policy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Version</th>
<th>Endorsed by</th>
<th>Authorised by</th>
<th>Approved</th>
<th>Effective Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Executive Committee</td>
<td>Vice-Chancellor and President</td>
<td>2 October 2013</td>
<td>2 October 2013</td>
</tr>
</tbody>
</table>

1. **Context**
Torrens University Australia’s information technology (IT) systems play a pivotal role in realising the objectives of the University’s Strategic Plan. The University aims to provide all members of the University community with secure and timely access to the University’s IT systems appropriate to their needs, and in a manner consistent with University policies and community expectations. The University is committed to ensuring that the use of electronic communications:

- protects personal privacy;
- does not breach applicable laws; and
- does not adversely affect the University’s commercial interests.

The purpose of this policy is to ensure that users of the University’s IT systems are aware of their rights and responsibilities.

2. **Definitions**
**University community:** students, staff, agents, affiliates, alumni, officers, contractors, volunteers and other people who are formally involved in a University-related activity, regardless of the location of that activity.

3. **Scope**
This policy will apply to all members of the University community who access Torrens University Australia IT systems.

4. **Principles**
The following principles govern the use of Torrens University Australia IT systems:

- Access is provided to IT systems in order for members of the University community to carry out University-related activities.
- IT systems must not be used to undertake antisocial, intrusive or unlawful activities.
- Security of IT systems and data is of paramount importance and security protocols must be observed at all times.
- The privacy of individuals must be respected at all times.
5. **General restrictions**
The University’s IT systems must not be used by members of the University community:
- for the purposes of creating, accessing or transmitting or otherwise dealing with content which may reasonably be regarded as objectionable or offensive (bearing in mind the cultural diversity of the environment in which the University operates), or content which is illegal;
- for the purposes of unauthorised streaming of video, music or internet radio, online games, file-sharing, sending chain letters, or gambling/gaming;
- for personal commercial purposes without explicit permission from the appropriate University authority;
- in a manner for the purposes contrary to University policies; or
- in a manner which may otherwise expose the University to legal liability.

Prohibited activities include (but are not limited to) activities which relate to:
- content which would reasonably be regarded as being pornographic;
- content which contains racial vilification, cruelty or violence;
- content which is defamatory.

5.1 **Personal use**
IT systems are provided for use in University-related activities. Limited use of the University’s IT systems for private, social or recreational purposes may be allowed, but as a privilege not a right. Staff are allowed reasonable use for such purposes outside of work hours, but such use must at all times comply with this policy. The University regards a total period of less than half an hour per day as reasonable use, subject to access cost incurred by the University.

6. **Email**
Email users must comply with any operational restrictions of the University which may be in place from time to time.

6.1 **Internal information**
The transmission to non-University persons of any internal message or other data prepared for in-house use is not allowed.

6.2 **Confidential information**
Where email contains sensitive or confidential information, a notice must accompany the email to advice of that status. A suggested notice is as follows:

“NOTICE – this message contains privileged and confidential information intended for the use only of the addressee named above. If you are not the intended recipient of this message you are hereby notified that you must not disseminate, copy or take any action in relation to it. If you have received this message in error, please immediately notify the sender at the above address.”

6.3 **Email lists**
Unsolicited group email messages must not be sent without explicit approval from the appropriate University authority. Student lists must only be used for direct academic purposes and only by authorised staff.

6.4 **Acceptable use of email**
Members of the University community must observe appropriate etiquette in formulating email messages. Impolite or inflammatory language must not be used. Nor should members of the University community respond to emails received, which are inappropriate or contain impolite or inflammatory language. Such emails should be deleted immediately.
Deliberately changing the ‘sender’ field of email is prohibited.

6.5 Legal implications
Email messages which are sent from a University email address may be construed as representing the University’s position. Where a user does not have authority, is not aware of the University’s position or where his or her personal view may differ from that of the University, the message should state that the opinion expressed is that of the writer and does not necessarily reflect the views of the University. Be aware that if a court subpoenas email records, the University must comply. Note that deleted files can often be recovered and used in litigation or criminal proceedings.

7. Internet access
In accessing the Internet, members of the University community must:
- comply with the relevant provisions of the Telecommunications Act 1997;
- take precautions not to propagate viruses contracted from the internet; and
- ensure that software downloaded from the Internet can be used legally by the University.

7.1 Quotas
The University reserves the right to impose quotas on internet use on any member of the University community.

8. Electronic commerce
All electronic communications which relate to the University’s products or services must comply with the University’s advertising and marketing guidelines.

Persons using the University’s information systems must comply with any applicable laws which regulate electronic commerce. Users should also be aware of trade practices and fair trading obligations which apply to the University.

Users must comply with the University’s requirements and limitations issued from time to time with respect to on-line transactions.

All electronic commerce should conform with the University’s operating procedures relating to delegation of authority.

9. Surveillance and security
The University has the capability to monitor the use of the University’s IT systems. While the University is committed to maintaining the privacy of personal information, it may be necessary to monitor electronic communications (including email records) in order to comply with applicable laws, to investigate suspected breaches of this policy, or to determine ownership or the recipient of lost or misdirected files.

To ensure the integrity and security of the University’s IT systems, users must:
- comply with University’s security protocols as issued and amended from time to time, including password security procedures;
- not allow access to a site on a University intranet or extranet to a third party if access is blocked to such third parties;
- not take any action which would or could lead to circumventing or compromising security of any of the University’s IT systems; and
- comply with the University’s requirements with respect to the use of encryption or secure transmission channels for particular categories of content.
10. **Data retention**  
Data files stored on University file servers will be backed up in accordance with the procedure for the particular server. Users are responsible for taking appropriate action in regard to retaining backup copies of other files.

11. **Privacy**  
The University’s IT systems must not be used to interfere with the privacy of others. The University and users are required to comply with federal and state legislation which may apply from time to time with respect to privacy of personal information.

12. **Intellectual property**  
Users of the University’s IT systems should respect the intellectual property rights of others. In particular, users must comply with the provisions of the Australian Copyright Act which in general terms (and subject to some exceptions) prevents a person from copying, reproducing, making public, adapting, broadcasting or transmitting copyright material owned by another person without that person’s permission.

13. **Report of suspected breaches**  
Suspected breaches of this policy should be reported as follows:  
- In the case of suspected breach by a student – to the Academic Director.  
- In the case of a suspected breach by an employee or other member of the University community – to the line supervisor of the employee or the Director, Operations and Services.

14. **Consequences if this policy is breached**  
Disciplinary action may be taken against users who breach this policy under the Student Misconduct Policy, the Research Misconduct Policy or the Staff Misconduct Policy, as appropriate. Any use of the University’s information technology systems contrary to this policy may result in a withdrawal of access.

15. **References**  
Spam Act 2003 (Cth)  
Privacy Act 1988 (Cth)  
Copyright Act 1968 (Cth)