IT ACCEPTABLE USE PROCEDURES

## OVERVIEW

These Procedures support the IT Acceptable Use and Security Policy by;

- Clarifying the responsibilities of users of University IT, and
- Prescribing how breaches of the Policy will be handled.

## Definitions

**Class 3 data** refers to University data that is classified as Class 3 under the University's Information Classification and Handling Guideline (i.e. there would be serious consequences to the University if security of the data were compromised).

University data means data generated by or on behalf of the University or otherwise within the University's custody.

All other defined terms have the same definitions as used in the IT Acceptable Use and Security Policy.

## 1. Acceptable and Unacceptable Use of University IT

*Responsibility: All Users*

1.1 Users of University IT must;

a) Comply with IT security and data protection guidelines (see SecureIT website).
b) Comply with the terms of use that apply to particular software or services.
c) Maintain the confidentiality of any personal or confidential information accessed via University IT.
d) Adhere to the IT best practice guidelines on Technology Services Policies and Guidelines.
e) Comply with the Spam Act 2003 and include the University's recommended signature and disclaimer on emails (only applicable to account holders sending electronic communications on behalf of the University).

1.2 Users must not use University IT;

a) To create, send, store, upload, access, use, solicit, publish or link to;
    i. Offensive, obscene, profane or indecent images or material.
    ii. Material that is threatening, violent, abusive, invasive of another's privacy, hateful, harassing, bullying, discriminatory, defamatory or otherwise objectionable.
    iii. Misrepresentative and/or misleading material.
    iv. Material or copies that infringe the copyright or other intellectual property of another person or organisation.
    v. Malicious software such as viruses, worms or address-harvesting software etc.
b) To gain any inappropriate personal, academic or other advantage.
c) To manipulate University data without authorisation.
d) To conduct personal business or unauthorised commercial activities.
e) For any illegal activity such as cyberstalking, identity theft or attacking other computer systems.
f) In a manner that would cause the University to be in breach of its legal or contractual obligations.

g) To forward electronic materials without the express or implied permission of the material's creator.
h) To access peer-to-peer file sharing software for unlawful purposes.

## 2. Device Security

*Responsibility: All Users*

a) All computing devices, including BYOD, must be configured to comply with the best-practice guidelines as described in the SecureIT website when connecting to the University network. Specifically;
    i. Passcode or password should be configured on device with automatic screen lock after a period of inactivity.
    ii. Security software such as antivirus and personal firewall should be installed.
    iii. Operating system and applications should be kept up to date.
    iv. Only digitally signed software from trusted sources should be used.
    v. Encryption and "remote wipe" features should be enabled for mobile devices when available.
    vi. Avoid storing Class 3 data on mobile devices.
b) To reduce risk of unauthorised use of their account, account holders are strongly encouraged to either log off or leave screensavers locked when leaving their devices unattended.
c) Devices that are compromised by a malware, or determined to pose threat to the security of University IT and other users, may be blocked from connecting to the University network until the sources of threats have been removed.

## 3. Data Security and Quality

*Responsibility: All Users*

a) All electronically held University data should be stored in such a way that it is backed up regularly; usually by saving it on a network drive that is backed up nightly.
b) Handling of sensitive or confidential University data should align with the University's Information Classification and Handling Guideline.
c) All University data should be captured and maintained in a manner that ensures its quality and integrity.
d) All electronically held University data should be captured, stored and disposed of in accordance with the University Records Policy and Research Data and Primary Materials Policy (in the case of research data).
e) University IT hardware must be disposed of through the disposal service facilitated by Technology Services or otherwise in a manner that renders any University data previously stored on the hardware illegible and irretrievable at the time of disposal.

## 4. Reporting IT Incidents

*Responsibility: All Users*

All University IT users must:

a) Report IT security incidents, including weakness or threat to University IT, suspected or actual intrusions, unauthorised access, or other breaches of the IT Acceptable Use and Security Policy or these Procedures to Technology Service Desk on 8313 3000 or via this form.
b) Report lost or stolen IT equipment that could provide access to University IT and/or class 3 data to the Technology Service Desk as soon as possible. Where the potential exposure of University class 3 data may be in breach of privacy or other obligations owed by the University to a third party, this should also be reported to Legal and Risk via heldesklegal@adelaide.edu.au.

## 5. Procedure for handling breaches

*Responsibility: Technology Services*

a) If an alleged breach of the IT Acceptable Use and Security Policy or its associated Procedures by a User is detected by or reported to Technology Services (TS), TS will refer the alleged breach to the following persons for a decision on what further action should be taken in respect of the User:

| Alleged breach by: | Notify to: |
|---|---|
| Staff or titleholder | Relevant Head of School or Branch / Area Manager |
| Student | General Manager, Student Services |
| Visitor account holder | Person who authorised the visitor account |
| Staff of Controlled Entity | General Manager (or equivalent) of the Controlled Entity |
| Staff / student of third party entity (for whom University IT is provided as a service under contract) | University contract manager responsible for that contract |

b) Where the alleged breach presents a risk to the University, Technology Services may implement immediate technological measures to mitigate the risks.

## 6. Expiry of Accounts

*Responsibility: All account holders and their Supervisors*

a) All account holders whose relationship with the University ceases will be notified prior to their accounts being disabled as outlined in the Identity Management procedures.

b) Prior to the account holder's IT account being disabled, it is the account holder's responsibility to ensure that all files and email messages on their account are stored in accordance with the University Records Policy.

c) Where an account holder is unable to comply with Procedure 6b before leaving the University (for instance, due to illness or death), the relevant supervisor of that account holder may request that the Chief Information Officer arrange for a nominated University account holder to be granted access to view and deal with the records associated with the account before it is disabled.