IT ACCEPTABLE USE PROCEDURES

OVERVIEW

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

- Clarifying the responsibilities of Users of University IT. For the avoidance of doubt, any reference to 'University IT Users' and/or 'Users' in these procedures, includes users of Bring Your Own Device (BYOD) unless the context otherwise provides;
- Defining additional User responsibilities for BYOD when accessing the University applications, systems, and networks; and
- Prescribing how breaches of the Policy and this Procedure will be managed.

Scope

These Procedures apply to all Users of University IT.
By connecting an unmanaged/self-managed device (BYOD) to the University network, Users acknowledge that they have read, understood and agree to comply with these Procedures.

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) Use University IT in a lawful, ethical, and responsible manner for the purpose of supporting their learning, research, and administrative objectives.
b) Comply with all relevant laws and regulations including, but not limited to:
   i. Criminal Code Act 1995 (Cth)
   ii. Tertiary Education Quality and Standards Agency Act 2011 (Cth) (TEQSA Act) ss 114A and 114B
   iii. The Privacy Act 1988 (Cth)
   iv. The Spam Act 2003 (Cth)
   v. The State Records Act 1997 (SA)
c) Comply with all relevant University Policies including, but not limited to:
   i. Academic Integrity Policy
   ii. Behaviour and Conduct Policy (staff and titleholders)
   iii. Code of Conduct (staff and titleholders)
   iv. Information Management Policy
   v. Privacy Policy & Management Plan
   vi. Risk Management Policy
   vii. Sexual Misconduct Policy
   viii. Student Misconduct Policy (students)
d) Comply with the terms of use that apply to particular software or services.
e) Undertake security awareness training and education commensurate with the User's responsibilities as determined by the University. Continued non-compliance with this

requirement will constitute a breach of this policy.

f) Maintain the confidentiality of any personal or confidential information accessed via University IT.

1.2 Users must not use University IT (whether via University owned, leased or supported devices or a BYOD);

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, trojan horses, worms, or address-harvesting software etc.
   vi. Providers or websites that provide, arrange, enable, encourage, or promote academic integrity breaches.

b) To gain any inappropriate personal, academic, or other advantage.

c) To manipulate University data without authorisation.

d) To engage in any conduct that constitutes sexual misconduct in accordance with the University's Sexual Misconduct Policy.

e) To conduct excessive or inappropriate personal business or commercial use in contravention of employment or other agreements.

f) For any illegal activity such as cyberstalking, identity theft or attacking other computer systems.

g) In a manner that would cause the University to be in breach of its legal or contractual obligations.

h) To forward electronic materials without the express or implied permission of the material's creator.

i) To access peer-to-peer file sharing software for unlawful purposes.

1.3 The following must be observed concerning use of University IT:

a) Staff are expected to utilise only approved University IT (Centralised, Specialist or Distributed IT) that have undergone an IT due diligence assessment process conducted by ITDS and have been certified for use according to the classification of data that is to be stored and processed, or a formal exemption has been granted.

b) Development and acquisition of new University IT, including purchase of software and cloud-based systems, is only permitted in accordance with rules set out by ITDS to ensure:
   i. They align to architectural principles.
   ii. They do not duplicate existing University IT.
   iii. Risks, including information security risks, have been assessed, mitigated, or accepted and documented.
   iv. Contracts have been reviewed and approved in accordance with the Contract and Agreement Policy.
   v. Suppliers are selected in accordance with the University Procurement Procedures.
   vi. Clear support arrangements, business owner and IT custodian are identified.

c) The only mode of remote access to the University network is using one of the modes authorised by the University that use multi-factor authentication (MFA). Use of desktop remote access software to gain remote access to University IT connected to the University network is strictly prohibited.

2. Device Security

Responsibility: All Users

a) Staff are expected to use a standard operating environment (SOE) endpoint device for conducting University business unless an exemption has been granted by the Area Managers, Head of School, Branch Heads, or their delegates and ITDS.

b) SOE devices must have the following restrictions in place:
   i. Users do not have local administrative privileges unless required for work and authorised by ITDS and Area Managers, Head of School, Branch Heads, or their delegates.
   ii. Users must not circumvent security controls and configurations on SOE.
   iii. Users must not install unauthorised and/or unlicensed software.
   iv. Users must restart their SOE device when prompted to do so in a timely fashion in order to complete installation of updates.

c) BYOD Users are responsible for ensuring the security of any University data accessed or stored on personal or non-SOE managed devices.
   i. Confidential University data may not be stored on a non-SOE device unless encrypted and access-controlled.

d) All BYOD including University-funded devices that are not SOE devices managed by ITDS that connect to the University network and/or store University data must be configured to mitigate the risks of compromise and data loss as follows:
   i. Passcode or password must be configured on the device with automatic screen lock enabled after a period of inactivity.
   ii. Anti-virus and anti-malware software must be installed, configured, and updated. Only operating system versions that are supported and maintained by the manufacturer must be used.
   iii. The operating system and applications should be kept up to date with the latest updates and security patches.
   iv. Only digitally signed software with appropriate licenses from trusted sources is to be used. All software on which University data is stored or uploaded must be reviewed by ITDS.
   v. Any BYOD that does not meet the above security criteria or is otherwise deemed to pose a threat to the security of the University may be restricted from connecting to the University network.

e) To reduce risk of unauthorised use of their device, account holders are strongly encouraged to either log off or lock their devices when leaving them unattended.

f) Devices that are compromised by malware or determined to pose a 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.

g) Devices containing University data, including computers, smart devices, and mobile storage devices must be erased in a secure manner as determined by ITDS to render any University data previously stored on the hardware illegible and irretrievable before being sold or otherwise disposed of.

h) Users of BYOD consent to provide limited authority over their personal device for the purpose of protecting University data, and investigation of policy breaches.
   i. By choosing to BYOD, the User consents to the University interrogating their personal device to ensure appropriate use and compliance with this procedure and any related policies and procedures.
   ii. The University reserves the right to monitor network traffic and access to University systems of a BYOD device while it is connected to the University network, to ensure compliance with this procedure and to protect University resources.
   iii. Monitoring will be conducted in accordance with applicable laws and University policies.

iv. While the University respects the privacy of Users of BYOD, it may inspect, monitor, and record network traffic and device activities connected to its network to ensure compliance with University policies and for security purposes.
v. The University is not responsible for any damage or loss that occurs to any personal device of a User.

3. Account and Password Security

Responsibility: All Users

a) Users are accountable for ensuring the security of their University login and protect against unauthorised use. In particular:
   i. A strong and complex password that complies with the current password policy (refer to IT Security Procedures for the current policy) that is not used with other online services must be chosen.
   ii. Multi-factor authentication must be configured on the user's account.
   iii. Password must never be disclosed to or shared with others.
   iv. Password must be changed when there is a chance that it has been compromised or become known to others.
b) Users must prove their identity by showing a valid photo ID (either in person, or over a video call) when asking an IT support staff to perform one or more of the following actions:
   i. Reset the password to a temporary password.
   ii. Modify the secondary email used for password recovery.
   iii. Reset (erase) all existing multi-factor authentication factors for the purpose of enrolling a new factor.
c) Users must not use other people's accounts or otherwise impersonate other users to gain access to University IT.
d) When access to University IT is no longer required by the User or their direct reports, the User or their supervisor should contact ITDS to ensure redundant access is removed in a timely fashion.
e) Line managers are responsible for ensuring that where their direct reports access becomes redundant (for example after changing roles and responsibilities), it is removed as soon as possible.
f) Business owners are accountable for performing periodic reviews (at least annually) of access to University IT that they own to ensure that access granted to users remains current, and any excessive access is removed.
g) 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 Information Management and Governance Policy.
h) Where an account holder is unable to comply with Procedure 3g 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 (CIO) or Chief Information Security 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.

4. 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.
i) All electronically held University data should be captured, stored and disposed of in

accordance with the Information Management and Governance Policy and Research Data and Primary Materials Policy (in the case of research data).

d) Users of BYOD must remove or transfer University data from their personal device or associated storage when no longer required or when the device is decommissioned.
e) The University may remove University data from a personal device either locally or remotely in order to protect University data and information assets.

5. Reporting IT Security 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 the ITDS Service Desk 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 ITDS 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 Services.
c) Cooperate with the University's IT and security teams during incident investigations and remediation efforts, including allowing access to the device (including a BYOD device) for forensics if a malware is suspected to have infected the device.

6. Procedure for handling breaches

Responsibility: ITDS

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 ITDS, ITDS 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 Area Manager, Heads of Schools or Branch Head
Student	Executive Director, Student Experience
Visitor account holder	Person who authorised the visitor account
Staff of Controlled Entity	General Manager (or equivalent) of the Controlled Entity
Staff / student or 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, ITDS may implement immediate technological measures to mitigate the risks.
c) Any unauthorised access to University systems, misuse of University resources, or other violations by a User may result in prosecution under applicable laws.