Provision and Acceptable Use of Information Technology Resources Policy

1. Purpose

1.1 The Provision and Acceptable Use of Information Technology Resources Policy (the policy) outlines requirements for:

- acquiring information technology (IT) resources for the university
- providing IT resources to staff and students, and
- rights and responsibilities in relation to the use of IT resources.

2. Scope

2.1 This policy applies to all staff, students, affiliates and visitors (hereafter users) as well as any other person provided with access to UTS information, corporate data and UTS IT resources.

2.2 This policy applies to the acquisition, management, maintenance, provision and use of the university's IT resources.

2.3 UTS controlled entities may use this policy or develop their own. The policies and practices of controlled entities must be equivalent to the standards and expectations outlined in this policy and the Information Security Policy.

3. Principles

3.1 IT resources are critical to the university's core business, supporting the initiatives under the UTS 2027 strategy.

3.2 UTS will apply appropriate security measures and protections to its IT resources in line with the Information Security Policy.

3.3 UTS will seek to streamline the acquisition and roll out of IT capabilities and resources to support the university in responding to emerging and evolving needs, while optimising cost and minimising the risk from cybersecurity threats. Where appropriate, this will be aligned with business continuity planning and disaster recovery processes.

3.4 The acquisition, provision and use of IT resources should comply with and enable the provisions of the Sustainability Policy. UTS and individual users should seek to minimise waste and the wasteful use of resources, both digital and physical.

3.5 UTS requires users to act with integrity and respect at all times in line with the Code of Conduct, Equity, Inclusion and Respect Policy and Student Rights and Responsibilities Policy.

3.6 UTS acknowledges that IT resources may be unavailable from time to time for either planned or unforeseen circumstances.

3.7 IT resource requirements vary across the university. This policy does not seek to put unnecessary limits on IT usage but aims to ensure that use and access is managed relative to need.

4. Policy statements

Acquisition and provision

4.1 The Information and Technology Unit (ITU) under the Chief Information Officer (CIO) is responsible for:

- acquiring IT resources directly
- setting IT architecture standards, procedures and guidelines that must be adhered to for all IT services, and
- providing advice and due diligence of university-level IT agreements as appropriate.

4.2 All faculties, units and other business areas must seek advice from ITU when acquiring or building new IT for local use. All acquisitions must be undertaken in line with the Delegations and Procurement Policy. All proposed new technologies must pass through the UTS IT solution design framework, managed by ITU. This framework ensures that proposed solutions meet architectural and cybersecurity standards.

4.3 Users will be provided access to UTS IT resources for the purposes of work, study and, where appropriate, incidental personal use, noting that:

- provision and access will reflect the level, budget, work and access requirements of the user, and
- resources will be allocated by the university as appropriate.

4.4 Staff and students are provided with the following, however these remain the property of UTS:

- UTS email accounts (automatically issued on appointment or enrolment)
- access to collaborative technologies, shared mailboxes, specialised programs and other resources, and
- access to necessary and appropriate information (through storage systems, databases and other IT resources).

4.5 ITU will develop procedures, guidelines and training as necessary to ensure effective implementation and use of centrally managed IT resources. ITU may also support development of local-level guidance and specific application or business process procedures as appropriate, although these are typically the responsibility of the relevant business unit or faculty.

Acceptable use

4.6 Users must adopt responsible approaches to the use of UTS IT resources, ensuring that their use complies with UTS policies, and state and federal legislation requirements, addressing, for example:

- intentional damage of physical property or deletion and destruction of original digital information (outside the normal retention and destruction requirements outlined in the Records Management Policy)
- violation of licencing agreements or any unauthorised use of software or hardware
- violation of commercial email (and other types of commercial messaging such as instant messaging or SMS)
- hacking and unauthorised access
- theft of equipment, information, data or software
- creation, possession or distribution of illegal content (for example child pornography)
- breach of intellectual property or copyright requirements (refer Intellectual Property Policy), and
- discrimination, harassment and the provision of a fair working environment (for example cyberbullying).

4.7 UTS IT resources must be used only for UTS work and activities and incidental personal use, not for non-UTS business activities or personal gain.

4.8 Users have a collective responsibility to ensure that UTS's cyber risks are minimised. This is a mandatory requirement of IT resources usage. Users must familiarise themselves with and operate under the requirements of the Information Security Policy and its associated procedures and guidelines. Any issues or concerns should be immediately reported as follows:

- For staff: in line with the procedures for reporting IT security incidents at Beyond the firewall: UTS cybersecurity (SharePoint)
- For students: by contacting IT support
- For all other IT users: via Facilities and campus security: Campus security who will make a report in line with internal procedures.

4.9 Users must manage information and data security in line with the Records Management Policy, Data Governance Policy and Privacy Policy. This applies when accessing corporate data externally or via personal devices.

4.10 UTS expects users to make use of help and training provided by UTS to improve skills and knowledge needed for their work as required.

4.11 Users must follow procedures, guidelines and conditions of use approved by the CIO (in consultation with the Chief Data Officer (CDO) as appropriate) and published by ITU (refer Using technology (Staff Connect)). This includes but is not limited to:

- access and passwords
- conduct and behaviour (refer principle 3.5)
- data sharing and confidentiality (with the CDO)
- downloading, storing and processing of large data files (with the CDO)

- email account ownership and management (including shared and secure mailbox email addresses)
- provision and use of UTS mobile devices
- software management and updates
- use of personal computers and other devices for UTS activities
- virus protection.

4.12 Users must manage their UTS email accounts responsibly (including their security) in line with guidelines and procedures approved by the CIO and published by ITU from time to time. Access to email records or email addresses may be blocked without the consent of the user in line with the Delegations.

4.13 UTS outlines its expectations of ethical behaviour and standards in the Equity, Inclusion and Respect Policy. Users must comply with the provisions of this policy when using IT resources including but not limited to:

- online lectures, classes, meetings and examinations
- communication via email or other collaboration tools (for example Microsoft Teams or Canvas), and
- use of internet browsers.

Conditions of use

4.14 UTS is not responsible for any inaccuracies in results or output when using IT resources. This precludes obligations relating to accuracy of personal information under the Privacy Policy.

4.15 To protect the university and all its users UTS reserves the right to install and operate filtering and/or network monitoring equipment, software or procedures to prevent unauthorised or unlawful emails or other content that is contrary to legislation, that is incompatible with the objectives of the university or that presents a potential cybersecurity threat.

4.16 UTS may retain backup copies of emails and communication via other tools (for example Microsoft Teams) for its business needs and legislated purposes and/or may authorise access to emails or other records held in staff allocated accounts where required for the business needs of the university in line with this policy, the Delegations, Privacy Policy and Records Management Policy and in accordance with any other procedures or guidelines approved by the CIO.

4.17 Broadcast emails should be used minimally and are only used for official university business. Broadcast emails may only be sent by:

- the Chancellor, Vice-Chancellor and members of the Senior Executive (or appropriate delegates (for example the Marketing and Communications Unit))
- deans and heads of division.

4.18 When a user's affiliation with UTS ends, access to all IT resources will be terminated in line with the guidelines approved by the CIO. Alternative agreements must be negotiated on a case-by-case basis in line with the Delegations.

4.19 UTS reserves the right to undertake periodic audits to ensure compliance with this policy.

Policy breaches

4.20 Breaches of this policy should be reported to the CIO for management and escalation as appropriate. Reports can be made via a line manager, the Student Complaints Policy or the Staff Complaints Policy as appropriate.

4.21 Users who are found to be in breach of this policy will be managed in line with one or more of the following as appropriate:

- Code of Conduct
- Student Rights and Responsibilities Policy
- Concerning Behaviour Intervention Policy
- Child Protection Policy
- Enterprise agreements
- individual contract of employment
- section 16, Student Rules
- state or federal legislation.

4.22 Breaches of this policy that relate to incidents of fraud or maladministration may be reported to the CIO or in line with the provisions of the Fraud and Corruption Prevention and Public Interest Disclosures Policy.

4.23 Data breaches must be managed in line with the Privacy Policy and Data breach response procedures (Staff Connect).

5. Policy ownership and support

5.1 **Policy owner:** The Chief Information Officer (CIO) is responsible for enforcement and compliance of this policy, ensuring that its principles and statements are observed. The CIO is also responsible for the approval of any associated university-level procedures.

5.2 **Policy contact**: The Deputy Chief Information Officer (CIO), Strategic Planning and Architecture is responsible for the day-to-day implementation of this policy and acts as a primary point of contact for advice on fulfilling its provisions.

The Chief Data Officer (CDO) is responsible for university data in line with the Data Governance Policy.

The Deputy CIO, Strategic Planning and Architecture and CDO are jointly responsible for the development of procedures and user guidance in relation to the use and management of UTS data.

5.3 **Others**: Users are responsible for the use of UTS IT resources in line with this policy.

6. Definitions

The following definitions apply for this policy and all associated procedures. These are in addition to the definitions outlined in Schedule 1, Student Rules. Definitions in the singular also include the plural meaning of the word.

Acquisition means the purchase, lease or other attainment of IT resources for university purposes in line with this policy and the Procurement Policy.

Affiliate is defined in the Code of Conduct.

Corporate data is defined in the Data Governance Policy.

Hacking means obtaining or attempting to obtain a higher level of access or privilege to university IT resources without appropriate authorisation.

Incidental personal use means the incidental and unofficial use of UTS IT resources for personal requirements that are aligned to the primary purpose of these resources (that is to help staff and students in undertaking their university work). Incidental use must come at no additional cost to UTS, should be otherwise in line with normal use requirements and should not interfere with any UTS business. Examples of incidental personal use include:

- contacting a family member about schedule changes because of a work activity or obligation
- making or changing childcare or educational arrangements
- contacting health care professionals, particularly where it relates to UTS work or absence
- other personal business that has a direct association with or impact on UTS work or activities (for example UTS club memberships), and
- activities in line with the relevant travel policies (refer Staff Travel, Expenses and Credit Card Policy and Student Travel and Expenses Policy and Procedures).

IT resources (also **IT services** and **resources**) means all information technology hardware, software, cloud services, devices, workstations, servers, storage, equipment, wi-fi, mobile networks, packages, accounts and platforms, either owned, leased or used under licence by UTS.

7. Approval information

Policy contact	Deputy CIO, Strategic Planning and Architecture
Approval authority	Vice-Chancellor
Review date	2022
File number	UR21/821
Superseded documents	Acceptable Use of Information Technology Facilities 2001 (UR06/357) UTS Email Policy 2004 (UR98/76) Guidelines for the Responsible Use of Email 2004 (UR16/1189)

Version history

Version	Approved by	Approval date	Effective date	Sections modified
1.0	Vice-Chancellor	26/07/2021	12/08/2021	New policy.
1.1	Vice-Chancellor	28/04/2022	28/04/2022	Changes and updates to reflect new ownership under portfolio realignment under Fit for 2027 project.

Web version

Provision and Acceptable Use of Information Technology Resources Policy

References

Procedures

Beyond the firewall: UTS cybersecurity (SharePoint)

Policies and rules

Child Protection Policy

Code of Conduct

Concerning Behaviour Intervention Policy

Data Governance Policy

Equity, Inclusion and Respect Policy

Enterprise agreements

Facilities and campus security

Fraud and Corruption Prevention and Public Interest Disclosures Policy

Information Security Policy

Intellectual Property Policy

Privacy Policy

Procurement Policy

Records Management Policy

Student Rights and Responsibilities Policy

Student Rules

UTS Delegations