GRIFFITH UNIVERSITY

Policy

Information Technology Code of Practice

1.0 Purpose

Information technology resources are essential for accomplishing the University's mission of pursuing excellence in teaching and learning, research and community service. Members of the University community are granted shared access to these resources, which must be used and managed responsibly to ensure their confidentiality, integrity, and availability for appropriate business, educational and research activities.

Successful use of University IT resources depends upon mutual respect and co-operation to ensure that everyone has equitable privileges, privacy and protection from interference or harassment.

This policy outlines the obligations of all authorised users of University Information Technology (IT) resources and information to protect the University and to protect the confidentiality, integrity, and availability of the University's information, from threats, whether internal or external, accidental, or deliberate, and to satisfy legal, regulatory, contractual and stakeholder requirements related to information security and cyber resilience.

2.0 Scope

This policy covers all University IT resources and information, irrespective of device, service or location, and applies to all authorised users, including:

- Griffith University employees, students and alumni.
- Contractors and third parties providing services to the University.
- Any affiliates authorised to access or use University IT resources.

3.0 Policy Statement

This policy mandates the acceptable use and management of the University's IT resources.

3.0.1 Authorised users shall:

a) Exercise responsibility.
b) Uphold the University's values.
c) Use resources appropriately, ethically, efficiently and for their intended purpose.
d) Respect the rights, privacy, safety and wellbeing of others.
e) Employ all reasonable efforts to protect the confidentiality, integrity and availability of University IT resources.
f) Report incidents that could adversely impact University information or IT resources.
g) Operate in accordance with the law and comply with other University policies and procedures.

h) Where possible, exchange information through University-supported channels only and in line with the Information Security Policy and Privacy Management Policy.

i) Understand and formally acknowledging the rules governing the use of University IT resources as set out in this policy and keeping current with any material changes to these rules.

j) Immediately notify an appropriate University officer (for example, Head of Element, supervisor, lecturer, Digital Solutions staff) of any violation of this policy of which they become aware.

k) Limited personal use, as defined in section 5.0 of this policy, is acceptable if it is in accordance with this policy and all other University policies, including conduct policies, and avoids conflicts of interest.

l) The University cannot guarantee the confidentiality of users' personal information or non-Griffith University information, stored, or transmitted on or over University IT resources.

3.1 Information Security

All users are responsible for information security, including:

a) Completing cyber security awareness training activities on time.

b) All activities that originate from their account.

c) Backing up information that is stored locally on your device.

d) Ensuring passwords, accounts, and data are adequately protected.

e) Not disclosing account details or passwords.

f) Only using accounts, systems and information you are authorised to use.

g) Take appropriate steps to ensure that data under their custodianship used in any sharing circumstance is adequately protected from unauthorised access, modification or destruction.

h) Logging out, or locking systems connected to the university network when not in use, including when unattended.

i) Immediately notifying the IT Service Centre if a user knows or suspects that another person has gained access to their account.

j) Reporting any information security incidents (which may commonly include lost or stolen University owned or managed devices, account compromises, accidentally sending information to the wrong person, data leakage or theft or other insecure observed practice), immediately to their supervisor and to the IT Service Centre.

3.2 Approved Software and Services

Users shall only use software or cloud-based services to store or process Griffith University information approved by the Chief Digital Officer (CDO) or delegate. For example:

a) Only software that has been approved by the CDO or their delegate, including commercial and open-source software, can be installed on University IT resource.

b) Only cloud-based services that have been approved by the CDO or delegate, including generative AI, social media, storage services, can be used to store or process University Information.

3.3 Email Use

Authorised users of University IT resources must:

a) Use University provided email accounts and systems for University related activity.

b) Not use personal or private email accounts and systems, for University-related business.

c) Forward any University-related emails received in a personal or private email account to the appropriate University provided email address and ensure the sender is notified that they should send future communications to the University provided email address.

d) Not set up automatic forwarding of University related emails to external, personal or non-University email accounts, unless an exception to this rule has been approved by your supervisor and in writing by the CDO.

3.4 Unacceptable Use

The University's IT resources or information must not be used for any activity (inclusive of work, study, research and personal use) that:

a) Is illegal or malicious.

b) Is for private business or commercial activities unless specifically authorised.

c) Supports or promotes political campaigns, candidates, legislation or ballot issues, or use e-mail for mass distribution of commercial or political content; or irrelevant or personal messages including petitions and chain mails.

d) A user is not specifically authorised.

e) Undermines the security, protection and privacy of University information or IT resources.

f) Attempts to connect any network device to the University wired network without prior permission from the Chief Digital Officer (CDO).

g) Has the potential to bring the University into disrepute.

h) Misrepresents a personal view or group discussion as the view of, or an official part of, the University, including unauthorised use of the University logo, trademarks or branding. This also applies to the naming or labelling of groups, sites or online pages outside of the University's own communications channels with Griffith University associated nomenclature when this is not an approved University forum (e.g., the establishment of social media groups labelled as "Griffith Students' Forums").

i) Involves the creation, downloading, distribution, storage or display of illegal, pornographic or inappropriate material (whether sexual or otherwise) or material that advocates hate or violence (see section 3.10 Exception for use).

j) Acts to defame, discriminate, vilify, bully, cyberbully, threaten or harass individuals or groups, including via accessing sites that violate conduct and safety expectations outlined in University policy, including sites that advocate on issues in a way that encourages unlawful discrimination on the basis of a protected attribute.

k) Breaches copyright law and licences.

3.5 Communication and Official Representation of the University

When communicating via University IT resources and on publicly accessible sites and networks, authorised users must:

a) Act in accordance with this policy and all other applicable University policies and procedures.

b) Only express views on behalf of the University with official authorisation to do so.

c) Identify their position within the University together with the appropriate authorisations in any communication that officially represents the University and/or its view.

d) When expressing personal views, clearly state that the opinion expressed is that of the writer, and not necessarily that of the University, or words to that effect.

e) Only use the Griffith University logo and trademarks for approved University documents.

f) Only use the Griffith University logo or branding on social media accounts, pages or networks with formal, written permission from the Vice President, Marketing and Communication.

3.6 Records Management

a) All electronic and digital information relevant to University business are official documents. They are subject to statutory recordkeeping requirements and can be subpoenaed during legal processes.

b) All emails relevant to University business are considered University records having the same status as other written communications and must be treated in accordance with the Information Management Policy, regardless of whether the device or facility used to create or store the email record is university-owned or not.

3.7 Monitoring

a) All information, metadata, data or files created, downloaded or stored by users while employed or enrolled at the University may be monitored and subject to investigation.

b) The University may monitor and audit equipment, systems and network traffic at any time to ensure compliance with University policies.

c) The University reserves the right to copy and examine files or information resident on or transmitted via University IT resources.

3.8 Privacy

a) The University uses approved hosted services and system that may involve the storage of data outside of Australia. Authorised users will acknowledge that data, including emails that may contain confidential or personal information (as that term is defined in the Information Privacy Act 2009) may be stored overseas. The Cloud Hosting policy is in place to ensure that a governance approval process occurs for the protection of information stored overseas, including security protection equivalence or great to Australian law.

b) While the University has entered into confidentiality arrangements to protect the privacy of such data (including adherence to the EU-US Privacy Shield), authorised users' data stored outside Australia may be subject to compulsory access through process of law, under the relevant jurisdiction in which it is stored.

3.9 Consequence of Misuse or Abuse

a) Digital Solutions may temporarily remove material from web sites, or disable any account, that is endangering the running of the system, or is suspected of unauthorised, inappropriate, or illegal use.

Failure to comply with this policy may result in sanctions relating to:

b) the individual's use of IT resources (such as suspension or termination of access, removal of online material or closure of website services),

c) the individual's employment (up to and including immediate termination of employment in accordance with the applicable University policy),

d) the individual's studies within the University (such as student discipline in accordance with the applicable University policy),

e) prosecution under State, Commonwealth and/or international laws.

3.10 Exception for Use

Material that has the potential to cause offence or would normally be regarded as inappropriate should not be used unless a genuine reason exists, which may be to support teaching, learning or research activities. Such use must be in accordance with the principles of the Academic Freedom and Freedom of Speech Policy, see specifically section 3.2. In such cases, the reason for the use must be documented and approval sought in writing from the relevant supervisor.

4.0 Roles, Responsibilities and Delegations

ROLE	RESPONSIBILTY
Chief Operating Officer	Is accountable for information security within the University and promoting a culture of strong information security.
Chief Digital Officer (CDO) or nominated delegate	Is responsible for information security risk management and security assurance activities within the University, as delegated by the Chief Operating Officer. Approving software and cloud services.
Director Cyber Security	Is responsible for providing advice, risk management, overseeing the day-to-day operations and the implementation, maintenance and improvement of relevant frameworks, policies, standards, procedures, guidelines and controls related to information and cyber security, and approving exceptions to the information security policy and associated standards and procedures. Temporarily disable accounts suspected of unauthorised activity.
Chief Marketing Officer	Approval of use of the Griffith University logo or branding on any social media accounts, pages or networks.
Managers / Supervisors	Are responsible for the implementation and oversight of this policy and promoting a culture of strong information security within their area of responsibility.

5.0 Definitions

For the purposes of this policy and related policy documents, the following definitions apply:

Authorised user includes staff and students of the University, and any person who has been provided with authorisation by the University to access University information technology resources and services.

Electronic and digital information are often used interchangeably, but in this policy context refers to all forms of information including communication created, transmitted, used, and stored using some form of electrical energy over mediums like internet, radio waves, local area and wide area networks. Some examples include documents, music, videos, podcast, emails, social media, chat and system logs.

Information technology (IT) resources are the capture and collection of any Griffith University data, information systems, applications, technology resources and infrastructure, including but not limited to desktop computers, laptops, tablets, notebooks, smartphones, intranet, internet access, wired and wireless networks, voice and video systems, servers, storage devices and systems, cloud based services, all web services, all messaging and collaboration services including instant messaging, social media and email services, as well as all user credentials for accessing data and systems. The definition includes the use of

privately owned devices (eg. smartphones, tablets) to access Griffith University networks, platforms, data, or services, or engage in online discussion or activities with other members of the Griffith community.

Limited personal use covers the use of University information technology resources to support activities that do not directly relate to University employment or studies and do not require substantial expenditure of time, adversely affect University information technology resources or breach the University's Code of Conduct. Limited personal use **does not** include private business or commercial activities. Examples of limited personal use include conducting personal life administration tasks, checking personal emails, or social media.

Offensive material is any published or broadcast content that is likely to be upsetting, insulting, or objectionable to a significant number of people. Material is not deemed offensive simply by virtue of expressing contrary opinions on a topic or providing factual coverage of distressing events, although graphic material dealing with upsetting subjects may still be unsuitable for some audiences.

6.0 Information

Title	Information Technology Code of Practice
Document number	2024/0001088
Purpose	This policy outlines the acceptable use of University Information Technology (IT) resources and information.
Audience	Public
Category	Operational
Subcategory	Information Security
UN Sustainable Development Goals (SDGs)	This document aligns with Sustainable Development Goal: 16: Peace, Justice and Strong Institutions
Approval date	9 April 2024
Effective date	9 April 2024
Review date	2025
Policy advisor	Director of Cyber Security
Approving authority	Chief Operating Officer

7.0 Related Policy Documents and Supporting Documents

Legislation	Information Privacy Act 2009 Privacy Act 1988
Policy	Academic Freedom and Freedom of Speech Policy Code of Conduct Information Security Policy Information Management Policy Privacy Statement Risk and Resilience Management Policy
Guidelines	Social Media Guidelines
Local Protocol	N/A
Forms	N/A