Information Technology Code of Practice

Approving authority	Chief Operating Officer
Approval date	9 February 2018
Advisor	Director of Cybersecurity
Next scheduled review	2019
Document URL	http://policies.griffith.edu.au/pdf/Information Technology Code of Practice.pdf
TRIM document	2023/0001174
Description	The Information Technology Code of Practice provides guidance to authorised users, for the appropriate access and use of the University's Information Technology resources, using any device from any location.

Related documents

University Code of Conduct
Copyright Matters
Information Security Policy
Privacy Plan

1. SCOPE

This policy applies to all users of Griffith University Information Technology (IT) resources regardless of their relationship with the University and irrespective of whether those resources are accessed on or off-campus.

2. RATIONALE

Information Technology resources are essential for accomplishing Griffith 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 integrity, security and availability for appropriate educational and business activities. This IT Code of Practice provides guidance to authorised users for the appropriate use of the University's Information Technology resources.

3. STATEMENT

Within this IT Code of Practice, Information Technology resources include but are not limited to all standalone or networked computers, hand held devices, all forms of communication equipment, and software owned or leased by the University, including, but not limited to externally hosted applications, for example, email, blogs and social networking sites.

This IT Code of Practice is intended to operate within, and be consistent with, existing State and Commonwealth Law, and University policies in areas such as sexual harassment, discrimination, equal opportunity, freedom of information, copyright, defamation, discipline and misconduct. It is intended to encourage responsible action and good judgement and to protect privacy.

Sanctions will be enforced if students or staff act irresponsibly and disregard their obligations to other users, or to the University as the provider of Information Technology resources. Inappropriate use of University provided Information Technology resources may also result in suspension, expulsion, termination of employment, legal action, or other disciplinary action.

4. PROCEDURES

4.1 Determination of responsibilities

It is your responsibility to become familiar with the rules governing use of the University's Information Technology resources.

Users who are authorised to permit other persons to use the University's Information Technology resources must ensure that those persons are made aware of the rules governing use of the University's Information Technology resources and have them sign or otherwise acknowledge that they will carry out their responsibilities under these rules.

Users learning of any violation of any of this IT Code of Practice must bring this matter to the attention of an appropriate officer (e.g. head of element, supervisor, lecturer, and Office of Digital Solutions staff) within the University without delay.

4.2 Authorised access

a) Use of equipment, software and access to the Internet via the University IT resources is provisioned conditionally to those with proper authorisation. University staff and authorised associated persons may be provided with Internet Access for University purposes upon authorisation from relevant faculty or Business Unit (e.g., Head of School/Office Director or nominee). Students receive authorisation upon enrolment at Griffith University.

b) Responsibility and accountability for IT security is the shared responsibility of all users. You will be held responsible for all activities which originate from your account. It is your responsibility to ensure that your passwords, accounts, software and data are adequately secured.

c) If you know or suspect that another person has gained unauthorised access to your account, you must immediately notify the Office of Digital Solutions on 3735 5555.

d) You must not use any means, electronic, social engineering or otherwise, to discover others' passwords.

5. APPROPRIATE USE

Griffith University technology resources and infrastructure including, but not limited to, desktop computers, laptops, tablets, smartphones, intranet, internet access, wireless network, telephone system, web services, instant messaging, social media and email services may only be used for University purposes and limited personal use, as outlined below.

5.1 Statutory Requirements

You must not use the University IT resources to violate or breach any Local, State, Commonwealth or International Law. All information, metadata, data or files created, downloaded or stored by users while employed or enrolled at the University can be monitored and subject to investigation. All electronic messages are official documents, subject to the same laws as any other form of correspondence. They are subject to statutory record keeping requirements and can be subpoenaed during legal processes.

5.2 Limited Personal Use

Limited personal use is the use of University IT resources to support activities that do not directly relate to University employment or studies. Examples of limited personal use include researching holidays, checking personal emails, gaming or social media.

Limited personal use must not require substantial expenditure of time, adversely affect University IT resources or breach the University's Code of Conduct.

Griffith IT resources must not be used for private business or commercial activities.

5.3 Prohibited Activities

The University allows its staff to use IT resources for limited extracurricular or non-work-related activities. These activities must not be illegal or potentially bring the University into disrepute, and they must not negatively impact the University's IT infrastructure.

Activities which are prohibited include, but are not limited to, the use of Griffith IT resources to do the following:

a) support or promote political campaigns, candidates, legislation or ballot issues;

b) send mass messages of a commercial, political, lobbying or fundraising nature;

c) send mass messages where the content is not relevant or appropriate for the majority of recipients or is of a personal or private nature;

d) forward electronic "petitions", or to ask recipients to forward messages;

e) send anonymous messages;

f) solicit support (financial or otherwise) for charity, or special causes not connected with a Griffith University effort;

g) send unverified public service announcements (such as virus alerts, unsafe products, lost and found, etc.);

h) use University IT resources to send/upload or access/receive/download or store any copyright infringing works;

i) any action that may infringe our statutory and commercial licenses for works. This may include unauthorised data mining, some types of digitisation, and unauthorised bulk downloads of proprietary database content;

j) any activities for private business, personal gain or profit.

5.4 Offensive and Illegal Material

You should not use the University IT resources to create, download, distribute, store or display any offensive or illegal material.

Material that has the potential to cause offence or would normally be regarded as inappropriate should not be used unless a genuine reason exists (i.e. to support teaching, learning or research activities) and the reason for the use must be documented and approved by the relevant supervisor. Such access should not occur on publicly accessible terminals.

Inappropriate Internet sites include but are not limited to:

a) sites that are illegal or hold illegal content;

b) sites that are pornographic or contain inappropriate sexual material;

c) sites that advocate hate or violence;

The University regularly audits such sites and reserves the right to remove / remove access to, such material from its resources without notice.

5.5 Discrimination, Harassment, Bullying and Defamation

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

You must not use communication systems including, but not limited to e-mail, instant messaging, discussion forums (including wikis, blogs or social media such as Facebook or Twitter) or web pages under your control, to provide or communicate obscene materials, or that threatens, harasses, intimidates or singles out individuals or groups for degradation or harassment in violation of Commonwealth or State Laws, and other University policies and regulations.

You must not display images or wording, nor play audio which could create an atmosphere of harassment to others.

5.6 Malicious Activities

You must not use University resources to engage in attempts to subvert University or external security provisions. This includes but is not limited to:

a) intentionally seeking information on / obtaining copies of /viewing / corrupting or modifying files, data storage media, passwords or any type of data belonging to other users unless specifically authorised to do so;

b) intentionally disrupting or damaging the academic, research, administrative, or related pursuits of others;

c) knowingly creating or propagating a virus, worm or any other form of malicious software;

d) attempting to email "spoof" i.e., construct electronic communication so it appears to be from someone else;

e) altering, or disrupting the operations of any other information system; attempting to capture to otherwise obtain user credentials, encryption keys, or any other token or access control mechanism that could permit unauthorised access;

f) tampering with hardware components or hardware configurations without the express permission of the person/s responsible for that particular item of equipment. This includes: workstation, monitor, keyboard and mouse;

g) printers and other peripherals;

h) network outlets, cabling and other components;

i) phones;

j) any part of a lab or other installation used by the general population of the University.

Under no circumstance are you allowed to connect any network device to the Griffith wired network unless prior permission is obtained from the Chief Digital Officer or designate. Network devices include but are not limited to; hubs, switches, routers, wireless access points, network appliances of any function and any devices performing network monitoring.

Wireless network connections must not be made with the intention of malicious activity.

5.7 **Official Representation of the University**

Where you are representing the views of the University, the communication must identify your position within the University. Where the view expressed is the official University view, the authorised source and author of that view should be identified.

You must not express views on behalf of the University without official authorisation to do so, or to allow another person to reasonably misconstrue that a personal view represents the official position of the University. In circumstances where readers might reasonably conclude a personal view is representative of the University, the user must clearly state that the opinion expressed is that of the writer, and not necessarily that of the University, or words to that effect.

The University logos and trademarks are the property of the University and may only be used for approved University documents.

6. PRIVACY

The University IT resources, systems and facilities are the property of the University. Anything sent or received using the network, systems and facilities of the University will therefore be transmitted and

stored on University property (or on third party property on behalf of the University). Accordingly it is likely to be reviewed by the University. This applies whether you use the University IT resources at a University site, at home, or any other location, including but not limited to externally hosted applications.

a) The University's email system may involve the storage of emails outside of Australia. To the extent that any of your emails contain any confidential or Personal Information (as that term is defined in the Information Privacy Act 2009), you acknowledge that data may be stored overseas. While the University has entered into confidentiality arrangements to protect the privacy of such data (including adherence to the EU-US Privacy Shield), you acknowledge that any data stored outside Australia may be subject to compulsory access through process of law, under the relevant jurisdiction in which it is stored.

b) The University therefore reserves the right to monitor both usage and content of email messages, instant messages, discussion forums and visits to Internet sites using University resources to:

    a. identify inappropriate use;
    b. protect system security;
    c. maintain system performance;
    d. protect the rights and property of the University;
    e. determine compliance with policy and state and Commonwealth laws.

c) The University also monitors and records network traffic including:

    a. email and internet sites accessed;
    b. usage data such as account names, source and destination accounts and sites;
    c. user location data;
    d. dates and times of transmission or access;
    e. size of transmitted material;
    f. other usage related data such as utilisation of wireless access points.

This information is used for accounting purposes, troubleshooting, systems management, analytics, user personalisation, and meeting legal and compliance obligations.

d) The University reserves the right to inspect, copy, store and disclose the contents of the electronic communications of its employees and other authorised users (e.g. students), to:

    a. identify inappropriate use;
    b. respond to a complaint;
    c. respond to an investigation request;
    d. verify an allegation of misuse

This can be done upon authorisation from appropriate University managers, the Police or other Law enforcement agencies to assist in the investigation of any alleged offence. The contents of electronic communications, properly obtained for legitimate business purposes, may be disclosed without permission of the employee or authorised user.

e) Monitoring and inspection can apply to personal and business use of intranet or internet services and personal and business related electronic communications.

f) You should always assume that everything you send by e-mail, instant messaging, post to a newsgroup or LISTSERV or post via a web site is totally public and might be read by people other than expected recipients.

g) To ensure that critical personal data such as passwords are protected from being intercepted, misaddressed or misrouted, they must never be sent by email. All login pages must use secure protocols such as HTTPS and SSL encrypted LDAP.

h) Any email messages or instant messages whether personal or business, may be accessed as documents under the Right to Information Act and may also be tendered in court as evidence

i) You should always assume that any web site you visit will at least know the Internet address you are coming from and that the same is true for email that you send.

7. COPYRIGHT COMPLIANCE

The University is committed to compliance in its use of copyright material. All creative works, including software, media, databases and datasets are automatically protected by the Commonwealth Copyright Act 1968, which sets out the rights of copyright owners and users. In addition, use of copyrighted works are enabled by licences. Staff and students are required to comply with copyright law and licences. Full information is available in the here.

8. CONSEQUENCE OF MISUSE OR ABUSE

The University considers any breach of your responsibilities to be a serious offence and reserves the right to copy and examine files or information resident on or transmitted via University Information Technology resources.

The Office of Digital Solutions may temporarily remove material from web sites or close any account that is endangering the running of the system or that is being reviewed for inappropriate or illegal use.

Failure to comply with Griffith University IT policies may result in sanctions relating to the individual's use of IT resources (such as suspension or termination of access, removal of online material or closure of website services); the individual's employment (up to and including immediate termination of employment in accordance with applicable university policy); the individual's studies within the university (such as student discipline in accordance with applicable university policy); prosecution under State, Commonwealth and International Laws; or any combination of these.