IT Acceptable Use Policy (GC)

Queensland Institute of Business Technology Pty Ltd
ABN 38 076 195 027

Document

Document Name	IT Acceptable Use Policy (GC)
Brief Description	This Policy applies to all system users and represents terms and conditions that must be met when using any Griffith College IT resource.
Responsibility	College Director and Principal
Initial Issue Date	22/10/2007
Authorising Body	Management Committee

Version Control

Date	Version No.	Summary of Changes	Reviewer Name and Department/Office
01/08/2017	5	Policy changes prior to December 2019 are found on H drive.	College Director and Principal
14/10/2022	6	Revised and updated to newer template and RASCI	IT Manager

Related Documents

Name	Location
Griffith University IT Code of Practice	Griffith University Portal
Information Security Policy	PDF

Contents

1 Purpose and Scope

1.1 Introduction

This Acceptable Computers or Systems User Policy sets out the approach of Griffith College relating to the management of the use of systems and computers.

1.2 Purpose

The purpose of this Policy is to ensure that all systems and computer users at Griffith College have respect for the law, other people and for Griffith College's mission and values.

1.3 Scope

This policy is effective at Griffith College and applies to all system users at any location, including those using privately owned computers or systems that connect to Griffith College computer and network resources. This policy represents the minimum requirements that must be met.

In general, this policy is not intended to inhibit access to information services that authorised Griffith College managers have made accessible for public inquiry (e.g. internet) via Griffith College computer and network resources. However, use of such services to access or attempt to access information not intended for public display or use, or to circumvent or violate the responsibilities of system users or system administrators as defined in this policy, is prohibited.

All employees should be reminded of this policy on an annual basis. All students agree to abide by the policies in place at Griffith College during their enrolment.

The computers and computer network at Griffith College together with access to the internet and email are provided primarily for educational, professional and business purposes. The use of these facilities should therefore be consistent with that purpose

2 Policy Statement

2.1 Underlying Principles

Users must adhere to all elements of this policy. The principles of behaviour relating to the use of Griffith College IT resources include:

- respect for the law;
- respect for other people; and
- respect of Griffith College's mission and values.

The principles of conduct of users also assume:

- integrity;
- diligence;
- economy; and
- efficiency.

2.2 Griffith University IT Code of Practice

As well as the contents of this policy all users must adhere to the Griffith University IT Code of Practice.

2.3 Responsibilities

2.3.1 Navitas Board

The Navitas Board is ultimately responsible for ensuring the services and resources it provides within the Group are used in efficient, lawful, proper and ethical ways (appropriate use). The Navitas Board delegates this responsibility to the Executive team.

2.3.2 Navitas Chief Executive Officer (CEO), Executive General Managers

The Chief Executive is accountable to the Navitas Board for the appropriate use of information assets, with all Executive General Managers having a responsibility for the effective implementation of this Acceptable Use Policy in their business unit. This will be achieved through the delegation of responsibility for the management of acceptable use to the Griffith College Managers. To support this, common tasks will include:

- Authorising User account establishment for all users who require access to the network and its resources;
- Ensure all users are made aware of this Policy in relation to their work at Griffith College;
- Ensure users are made aware of their responsibilities for IT Security;
- Ensure that all work practices comply with this Policy;
- Lead by example with respect to this Policy;
- Notify the relevant IT department staff when a user's access to a service or system should be withdrawn;
- Review use of IT resources and take responsibility for any costs incurred in respect of this.

2.3.3 Navitas UPA IT Manager

In addition to ensuring the effective implementation of this Policy in their business unit the IT Manager is accountable for the ongoing development, approval, implementation, awareness and effectiveness of this Policy and the supporting processes and documentation. To support this, common tasks will include:

- Ensure that IT services and resources are being used in an optimal way;
- Investigate breaches of this Policy, taking action when required and reporting to other agencies (eg. the Police) when necessary;
- Maintain accurate system records, monitor records and archive as appropriate;
- Disclose usage where appropriate;
- Provide access controls where possible to limit usage not consistent with this policy;
- Management of IT security procedures and best practices including the ongoing maintenance of the IT Security Policy;
- Authorise certain Navitas & Griffith College staff members (generally within IT Services) to monitor accounts, files, stored data and network data or to disconnect IT equipment in the event of an IT security breach;
- Authorise any extraordinary action taken to monitor IT services;
- Instruct IT Support Authorised Staff in privacy, confidentiality and need-to-know principles in relation to treatment of data, information and material discovered by IT Support Authorised Staff whilst monitoring.

2.3.4 Navitas UPA IT Support Specialists

Under delegation from their Managers, and the Navitas UPA IT Manager, IT Services are responsible for IT security matters within Griffith College. To support this, common tasks will include:

- Receiving reports of IT security breaches from users and to take appropriate remedial action;
- Abiding by the Griffith College Privacy Policy;

- Providing additional information for users that request assistance on understanding their responsibilities under the IT Security and Acceptable Use Policies;
- Ensuring IT resources provides adequate security of users' information through limiting of access to information by non-authorised users.

2.3.5 Griffith College Line Management

All Griffith College Managers are responsible for ensuring that all employees are aware of this policy and their responsibilities defined here.

2.3.6 All Griffith College Users (e.g. employees, students)

All Griffith College users have a general duty of care and are responsible for being aware of and complying with this Policy. This will include:

- ensuring their usage complies with this Policy, and for informing the IT department when they cease their association with Griffith College;
- respecting the physical hardware and network configuration of Griffith College and Navitas-owned networks. Users must not extend the physical network on which their system resides (e.g. extra switches or a wireless connection);
- not performing any unauthorised, deliberate action that damages or disrupts a computer system, alters its normal performance, or causes it to malfunction;
- not using Griffith College and Navitas systems to gain unauthorised access to other computers, networks or information regardless of the intention;
- reporting any suspected security problems or unacceptable use to their local IT Support, and not demonstrating the problem to others. Any user who believes their files have been tampered with should immediately change their password and contact IT support with the specific details;
- avoid sending large attachments, especially to the internal Griffith College staff email address, or other large distribution lists;
- assuming that electronic files are not necessarily secure. Users of electronic mail systems should be aware that electronic mail in its present form is not secure and is vulnerable to unauthorised access and modification;
- respecting the Griffith College Privacy Policy and treating all confidential or sensitive information appropriately;
- not using any of Griffith College's official branding materials (e.g. name or logo) on their personal web pages, e-mail, or other messaging facilities.

2.4 Acceptable Use Principles

2.4.1 User Accounts (e.g. employee accounts, student accounts)

Users are ultimately accountable for all actions attributed to their User Account. To support this Users are responsible for safeguarding their passwords and/or other sensitive access control information related to their accounts or network access. Similarly, system users must recognise the sensitivity of all other passwords and computer or network access information in any form, and must not use, copy, transmit, share or divulge such information. Any attempt to conduct such actions by a system user is a violation of this policy.

Users shall ensure access privileges are restricted to their own use only. Users must not share their accounts, nor grant accounts to others nor otherwise extend their own authorised computer and network access privileges to others. System users must not implant, execute or use software that allows them unauthorised remote control of computer and network resources, or of accounts belonging to others. If specific access is required, the appropriate IT Officer should be contacted rather than disclosing a password.

System users must not implant, execute or use software that captures passwords or other information while the data are being entered at the keyboard or other data entry device. Users must not obtain nor attempt to obtain any electronic communication or information not intended for them. In particular, system users must not attempt to intercept or inspect

information (e.g., packets) en route through Griffith College computer and network resources, nor use Griffith College computer and network resources to attempt to intercept or inspect information en route through networks elsewhere.

Unattended workstations must always be logged off or left in the Workstation Locked mode (Ctrl + Alt + Delete, Windows key + L) when the operator leaves their workstation unattended. All passwords must meet the following minimum standards:

- All accounts must have passwords;
- Passwords for accounts must not be shared, unless a Group account has been specifically authorised in writing;
- Passwords must be resistant to a computer program that checks passwords against previously used passwords and passwords that are easily discovered or compromised by human or computational means;
- Passwords must use a mix of alpha and numeric characters, and contain at least 6 characters if the operating system supports passwords of that length;

Passwords to computer and network resources containing computerised institutional data will not be issued over network media in clear text unless a secondary means of authentication is provided (multi-factor authentication).

2.4.2 IT Systems Use

Users will, by default, only have access to the information and systems that they need, to perform their function. Elevated local access privileges must only be granted for essential and specific purposes.

Users must be aware that removable storage like USB connected media, flash drives, CDs or DVDs are a security risk. The loss of these storage media is a common place occurrence and therefore users must be responsible for them. Where employees have confidential data stored on the removable storage, the employee must encrypt the data. There are data loss prevention systems in place to prevent usage of removable media in most instances.

Confidential information stored on portable devices (e.g. laptops, mobiles, PDAs) must also be encrypted. This ensures that the data remains confidential in the event of loss or theft. Users may not copy any information or software stored on their desktop or laptop computer, for personal use. Users may not use Griffith College systems for any of the following activities:

- Gambling or any form of Internet gaming;
- Share trading unless you have the prior consent of your Executive General Manager;
- Use any Griffith College and/or Navitas IT systems for personal financial gain, solicitation or private business purposes;
- Posting any Griffith College Information to Internet bulletin boards, discussion lists, news groups, chat groups or other Internet discussion forums that are accessible by the public unless you are authorised by your Manager to do so.

2.4.3 Safe Practices

All Griffith College users (e.g. employees, students) shall work in accordance with safe computing practices to minimise the risks associated with computer viruses.

Users are advised to use caution when opening email attachments from unknown sources. Users shall not open any received .exe, .pif, .com, vba, or. scr files without prior consultation with IT staff. If virus protection software detects a virus from an incoming file or email, consult IT Support immediately. If a computer is acting strangely, there may be an undetected virus. This does not happen often, but it is worth checking with IT Support. The willful introduction of computer viruses or other disruptive/destructive programs into Griffith College computers or networks, or into external networks using the Griffith College network, is strictly forbidden.

Removal or deactivation of antivirus software on Griffith College computers is not permitted except where advised and conducted by Griffith College IT Support staff. Under no circumstances are Griffith College users to send out virus warnings to other staff or external

locations. Where appropriate, Griffith College IT Support will issue communications regarding computer virus warnings.

2.4.4 Inappropriate Material

If a user is the recipient of inappropriate material, or end up at an inappropriate website, they must:

- Delete this material or close the web browser/tab immediately;
- Advise your manager and IT Support that you have received or accessed such content. If the sender is known, the user must ask them to stop sending inappropriate material to Griffith College email accounts.

Users must not access, create, download, print, store, forward or send inappropriate content. Examples of which include, but are not limited to:

- Information or images containing indecent material (this includes pornographic or other sexually explicit material), or other material, which explicitly or implicitly refers to sexual conduct or preference;
- Information or images containing profane or abusive language. This includes anything that refers to or supports discrimination of any kind;
- Unwelcome propositions;
- Any defamatory, illegal, offensive, annoying or harassing material;
- Information intended to incite criminal activities or instructs others how to commit such acts.

If a user is in doubt as to whether the material they are accessing is inappropriate, it should be treated as such and removed from the computer.

2.4.5 Email

Emails must be written with the same consideration as any physical communication, which would feature the Griffith College logo. When sending emails, users must take the appropriate measures to make sure the message has been sent to its intended recipient. Where appropriate, a user may save a copy of business or study related email.

All Griffith College staff members are required to use an official College email address when corresponding with any stakeholder on a College related matter. This would include casual teaching staff corresponding with students.

Users must not make use of Griffith College resources to forward chain letters or spam mail, alter messages so they appear to have been sent by someone else, or delete/edit the automatic signature that appears on the bottom of Griffith College emails.

There is always a risk of false attribution with electronic communications. It is possible that communications may be modified to reflect a false message, sender or recipient. In these instances, an individual may be unaware that he or she is communicating with an impostor or receiving fraudulent information. At any stage if a user has a concern with the contents of a message received or the identity of the publisher of the electronic information, action should be taken to verify their identity by other means. If a user believes an electronic communication has been intercepted or modified, your manager should be informed.

2.4.6 Monitoring

Griffith College reserves the right to regularly audit IT systems to ensure compliance with this policy.

As part of normal system operations, Griffith College & Navitas reserves the right to maintain logs of email system activity. These logs identify the sender, recipient, message size, relay, date and time. As part of normal system operation, Griffith College network systems generate logs of all internet activity and access. These systems are the DNS and internet cache. The

logs from these sites identify destination sites, pages, page download size, and originating Griffith College computer.

Remote access connections to Griffith College are monitored. Monitoring includes connection dates and times and may include access to system resources. To ensure compliance to licensing obligations Griffith College & Navitas reserves the right to scan all Griffith College equipment to detect illegal or non-Griffith College registered software and remove it. All files, including those generated via Internet email and proprietary email systems, are generally accessible by persons with system administration privileges (e.g. Griffith College IT staff). Users are discouraged from maintaining anything private on the servers or desktop computers. Access to Griffith College IT systems is provided to users on the condition that they consent to monitoring in accordance with this and the Information Security Policy.

2.4.7 Griffith College Assets

Hardware always remains the property of Griffith College and/or Navitas. On cessation of association with Griffith College, all hardware in the possession of the user must be returned in a clean, tidy, working and prompt fashion to Navitas IT staff. Griffith College devices are issued for use by Griffith College users only. Devices and accessible Griffith College resources (e.g. internet access) are not provided for non-Griffith College users to use (i.e. friends, family etc).

Where possible, hardware shall be purchased from Griffith College and Navitas' preferred suppliers. Where this is not possible hardware shall be purchased in Australia to ensure that any warranty is easily claimable.

The unauthorised duplication of copyrighted computer software violates the law and is contrary to Griffith College's standards of conduct and business practice. Griffith College disapproves of such copying and recognises the following principles as the basis for preventing its occurrence. Griffith College & Navitas:

- neither permits nor tolerates the making or use of unauthorised software copies within the organisation under any circumstances;
- will provide in a timely fashion sufficient quantities of legitimately acquired software to meet all software needs for all computer hardware;
- will comply with all licensing terms and conditions regulating the use of any software it acquires;
- will enforce strong controls to prevent the making or use of unauthorised software copies. These will include effective measures to verify compliance with these standards and appropriate disciplinary action for any violation of these standards; and
- will take steps to inform current and future users of their legal responsibilities in relation to software theft.

All software purchases must go through the IT Department. This is to ensure that:

- software is correctly added to the asset register upon purchase and receipt;
- software is allocated against the asset in the database;
- audits of software on computers can occur against a reliable account of owned software;
- site licence price savings can be achieved through a coordinated approach to purchasing software;
- upgrades of software can occur, generally business wide, to ensure minimum confusion between versions;
- areas are not disadvantaged by not having access to upgraded software if appropriate/suitable for position and hardware;
- all instances of licence documentation, software media and copies of delegation / invoice details for the software are held and accounted for in the company.

Software always remains the property of Griffith College on cessation of association with Griffith College, access to software and associated services is forfeited.

Users are not permitted to install their own software on any Griffith College computers, without prior approval from their supervisor or manager and IT. Failure to comply may result in users being held personally responsible for any data loss or penalties imposed for breach of copyright.

Installation or use of peer to peer (P2P) file sharing programs, such as LimeWire or BitTorrent, is not permitted on computers connected to the Griffith College network. Users shall not download, or authorise downloading of, information or software using Griffith College computer systems that would violate copyright, license agreements or contract of usage.

2.4.8 Breaches

Any security exposures, misuse or non-compliance must be reported as soon as an occurrence is identified to IT Support. Failure to comply with this policy may result in any or all of the following:

- Suspension and/or termination of access to Griffith College systems;
- Additional disciplinary action as determined by relevant Managers in line with existing policies;
- Referral to law enforcement authorities for criminal prosecution;
- Other legal action, including action to recover civil damages and penalties.

2.4.9 Confidential Information

Griffith College staff members have a duty to keep confidential:

- All Griffith College data unless the information has been approved for external publication; and
- Information provided in confidence to Griffith College by other entities.

Each staff member is under a duty not to disclose Griffith College business information unless authorised to do so. Breach of confidentiality through accidental or negligent disclosure may expose a staff member to disciplinary action.

2.4.9.1 What Is Confidential Information

Company and/or sensitive information includes and will include all trade and business secrets and other confidential information and documents relating to the affairs or business of the Company or any person with whom you come into contact as a result of your employment with the Company or who may come into your possession in the course and by reason of your employment whether or not the same were originally supplied by the Company.

Confidential information includes any information (written or verbal) of a commercial, technical or financial type which is not publicly available. Staff must not make unauthorised copies of any material (original or not) such as correspondence, company manuals, printouts, floppy disks, customer lists, diaries, file notes or any other material which is accessible through employment with Griffith College. All such material is and remains the property of the company. All company property must be returned upon termination of employment.

2.4.10 Legal Requirements

For legal purposes email has the same standing in court as paper documents. Users must be aware that Griffith College can be involved in litigation. Any records relating to use and activities in relation to email, internet and intranet are discoverable by way of court order or subpoena. These include matters affecting legal proceedings, affecting personal affairs of employees, parents, students, or third parties, as well as relating to research, or other communications even if communicated in confidence.

Email residing on or transmitted across the Griffith College system is the property of Griffith College. All electronic files are the property of Griffith College, and users should act on the

basis that they can be, and where necessary will be, held accountable for their messages and their stored files. While all transmissions remain the property of Griffith College by law, all efforts to retain professional confidentiality will be made. All internet activity is recorded for individual users. Reports of this activity are continually being monitored. Over time, all users could expect that the record of their internet activity may be viewed by senior staff within Griffith College. Should access to an individual's files or internet logs be necessary for an alleged criminal offence or serious disciplinary matter, the individual concerned will generally be advised of the circumstances of the complaint and be present when the files or logs are opened. Notwithstanding the above, Griffith College reserves the right for any reason whatsoever to inspect without forewarning any files or logs held on any Griffith College computer.

3 Responsibilities

Responsibility	CDP	CFM	QCM	AD	DSAS	PC	AB	PAC	DMA	IT	All
Maintain currency of policy	A	C	C	C	C	C	C	C	C	RA	I
Section 2.4.1	A	A	A	A	A	A	A	A	A	RA	CI
Sections 2.4.2 to 2.4.5	A	C	C	C	C	C	C	C	C	RA	I
Sections 2.4.6 to 2.4.8	S	C	C	C	C	C	C	C	C	RA	I
Sections 2.4.9	RA	A	A	A	A	A	A	A	A	RA	CI
CDP = College Director & Principal, CFM = College Financial Manager, QCM = Quality & Compliance Manager, AD = Academic Director, DSAS = Director, Student & Academic Services, PC = Program Convenor, AB = Academic Board, PAC = Program Advisory Committee, IT = IT Manager, All = Staff, R = Responsible, A = Accountable, S = Supporting, C = Consulting, I = Informed											

4 Compliance

4.1 General

The IT Manager will ensure staff are informed about this Policy through staff meetings and communications.

Students will be made aware of this Policy through the College website, Policy Library and digital campus.

4.2 Relevant Legislation

Griffith College is required to comply with a range of legislation and regulation both at a state and a federal level. Users need to be aware that certain conduct may breach laws outside of Griffith College and lead to criminal or civil proceedings and/or penalties for which they will be held personally accountable. In Australia these laws include:

- Equal Opportunity Act 1992 (QLD)
- Sex Discrimination Act 1984 (Cth)
- Disability Services Act 2006 (QLD)
- Disability Discrimination Act 1992 (Cth)
- Racial Discrimination Act 1 975 (Cth)
- Classification of Publications Act 1991 (QLD)
- Copyright Act 1968 (Cth)
- Privacy Act 1988 (Cth)
- SPAM Act 2003 (Cth)

- Other relevant Commonwealth and/or State laws such as those relating to the transmission of offensive material and Telecommunications.

4.3 Review

This Policy is tested and reviewed at least every 24 months and when at the time of any changes to the regulatory compliance requirements, legislation, regulation and guidelines. This review process aims to ensure alignment to appropriate strategic direction of Griffith College and continued relevance to Navitas' current and planned operations.

4.4 Records Management

All records in relation to this document will be managed as follows:

Record type	Owner	Location	Retention	Disposal
Policy	College Director and Principal	Policy Hub	Permanently with control in place for revisions	Policy Hub archive