

Use and Provision of ICT Services and Facilities

Contents

Use and Provision of ICT Services and Facilities	1
Introduction	2
Context	2
Purpose	2
Scope.....	2
Rationale.....	2
Principles/Statement	2
Entitlement.....	2
Responsibilities and obligations	3
Conditions of Use - Security.....	3
Conditions of Use – Electronic Communications	4
Conditions of use - Internet	5
Inappropriate Use.....	5
Privacy	6
Enforcement.....	6
Disclaimer	7
Reference and Supporting Information	7
Definitions	7
Supporting Documents.....	7
External Legislative Context (Links)	7
Internal Policy and Procedures.....	8
Responsibility.....	8
Document Version Control Table	8

Introduction

Context

Access to the internet is provided to staff and students for the teaching and business purposes of the Institute. This access is a finite resource and must be used responsibly to ensure its availability for its' primary purpose.

Purpose

To inform TAFE Gippsland (the 'Institute') stakeholders about the provision and acceptable use of the Institute's computing and communications services and facilities.

Scope

ICT services are provided to all Institute staff and students. Limited services are also provided to Institute contractors, sub-contractors, customers and partners, and as such, this Policy applies to all stakeholders in the use of these services and facilities.

Rationale

Principles/Statement

The Institute provides students and staff with access to computing and communications services in support of its teaching, learning and administrative activities. These facilities include: -

- Access to a data communications network, which links the majority of Institute computers on campus. The Institute network is connected to an external network linking the organisation with external people, organisations and data that is commonly referred to as the Internet.
- Access to a range of Internet based services such as email, the World Wide Web, Learning Management Systems such as Moodle and other on line resources.
- Access to external high performance computing facilities.
- Access to various printing facilities.
- After-hours access to some computing facilities after business hours, upon individual approval.
- An integrated data network across all campuses, with individual accounts for staff and students, providing access to personal and shared storage space on the network or online and individual email accounts.
- Student computer laboratories located across all campuses offering PC Windows based workstations and Apple Macintosh laboratories in selected locations.

Limited personal use of the Internet and Institute computing facilities is acceptable as long as it occurs ethically, responsibly and in line with all other Institute policies.

Entitlement

Staff of the Institute are entitled to an email, network (including Internet) account. Access to this account is created when the appropriate application has been authorised and lodged. Access to any other services or facilities is provided on a needs basis and must be authorised. Casual staff will be allocated resources as required.

Staff will be issued with a dedicated desktop or laptop computer (based on the requirements of their position), where they are employed at a fraction of 0.6EFT or above.

After lodging a request via the ICT services portal, staff should receive a response to their request within 1 business day. Staff can expect all routine service requests to be resolved with 5 working days or they will

receive written advice within 5 working days explaining why an issue may take longer (i.e. resolution is dependent on purchasing additional equipment, etc.). Accounts will remain valid until course completion, at which time students will have 2 weeks to enable them to save any data and emails they wish to keep, after which time, the accounts will be deleted.

All students are entitled to an email, network (including internet) account. Accounts are created by students after successful enrolment and are accessed via a user id and password. Access to any other computing and communications facilities requires authorisation.

Through the Student Account Manager function (SAM - <https://webapps.tafegippsland.edu.au/sam>), The Institute provides all enrolled students with the ability to create an institute online services account, which includes a TAFE Gippsland student email account hosted by Microsoft's O365 service. The institute provided email account is the normal means by which the Institute will communicate with students and as such all students must agree to regularly check their student email account.

Responsibilities and obligations

The Institute expects all users to exercise responsible and ethical behaviour when using the computing and communications facilities. All users are required to assist the Institute to keep the network available and accessible by observing the following guidelines:

- Take responsibility for using Institute computing and communications system in accordance with their appropriate authorised purposes. Unauthorised software must not be installed on the computers. For the purposes of this Policy, "unauthorised software" includes, but is not limited to; games, instant messaging and chat programs, file transfer and peer-to-peer file sharing programs.
- Intentionally downloading unauthorised software or material breaching copyright is prohibited.
- The Institute network should not be used for personal or private gain, nor should it be used to store or collect personal information about others where an individual is not commissioned to do so by the institute.
- The 'TAFE-GIPPSLAND' and 'eduroam' Wi-Fi networks are the designated BYOD networks, and therefore the only networks that staff or students are permitted to connect non-Institute devices to. Interference with any Institute networks is not permitted.
- Staff and students must abide by any relevant instructions given by the Chief Operating Officer (COO) or delegated officer. Such instructions may be issued by notice displayed in the vicinity of computing facilities, by letter, by electronic communication, in person or otherwise.
- Downloading and also making available for download, material covered by copyright is not permitted and will be dealt with in accordance with this Policy and relevant copyright policy and legislation.
- Configuration changes to Institute computers are not to be made without authorisation – this includes, but is not limited to, screensavers, bitmaps, backgrounds, images, and screen resolutions.

Conditions of Use - Security

- The use of computing facilities is controlled through a "user id" assigned access rights and protected by a personal password. Passwords must remain confidential. Users will be held responsible for unauthorised use of their privileges. To help keep access secure: -
 - Keep passwords confidential and change them frequently;
 - The Institute enforces minimum password length and complexity rules; and
 - Log out of the network whenever not using it or leaving the workstation.
- Respect security measures and the integrity of workplace systems and files. Do not attempt to adversely interfere with the operation of the Institute's computing, communications or any other facilities using the Institute network.

- Care should be exercised when providing access to personal files. Protection has been put in place to prevent access to personal files to ensure privacy. Incorrectly set protection will put files at risk of deletion, manipulation, plagiarism or inappropriate use. Staff should be especially careful if the data they have responsibility for is of a corporate nature.
- Provide identification (for example by student card) when using the Institute's computing facilities, on request of a staff member.
- No form of computer hacking (such as illegally accessing other computers or accounts, knowingly attempting to bypass internal controls or security) is allowed, including scanning, penetration or monitoring tools without express permission from the Manager ICT Services.

Refer ICT009 Information Security Policy

Conditions of Use – Electronic Communications

Electronic communications encompasses all methods of communication utilising the Institute network and server infrastructure. This includes, but is not limited to, voice, video, email, on line text message, conference calls (voice and video), file transfer and application sharing.

The Institute encourages the use of electronic communication to share information, to improve communication and to exchange ideas. The intention of this Policy is to maximise freedom of communication for Institute purposes within a framework that is both lawful and responsible.

- Individuals must not use Email for personal commercial gain.
- Communications Group Lists will only be created and used for official Institute business.
- Electronic Communications services must not be used to solicit goods and services or to offer them to other members of the Institute community. For example, advertising rental of properties, sale of personal goods.
- Advertising or sponsorship is not permitted except where such advertising or sponsorship is approved by the marketing department and is clearly related to or supports the mission of the Institute.
- It is prohibited to use Electronic Communication Services to libel, to send or subscribe to pornographic material, to harass, threaten other individuals, unlawfully vilify or to transmit offensive language or images.
- Email systems should not be used for permanent storage of files. File attachments should be saved to an appropriate location and emails that are no longer required should be deleted. Regular use of email archiving tools should also be used to keep mail box sizes to a manageable level and within Institute storage quota levels.
- The Institute supplied email addresses should not be used to register on inappropriate or suspicious web sites or mailing lists as this can often contribute to the receiving of SPAM emails. In these cases, the emails can be classified as legitimate as you have subscribed to receive them.
- When using the Electronic Communication recording facilities, ALL parties must give verbal consent both prior to recording starting and again once the recording has commenced. If any party does not wish to have the session recorded, it must not be activated.
- The Institute cannot protect individuals against the existence or receipt of material that may offend them. Those who make use of electronic communications are warned that they may willingly or unwillingly come across, or be recipients of, material that they may find offensive.
- Group-mailing addresses have been created for each campus and for the Institute as a whole. The following conditions of use will be applied in order to maintain both the efficiency and usefulness of the group Email service.
- Group Email addressed may be used for Institute business only and must not be used for personal or commercial activities. All communications sent to any of these group addresses should be Institute

related. Personal announcements (e.g. lost pets, for sale, lost property, etc.) must not be sent to these “everyone” addresses.

- For wider distribution across all campuses, use of the Institute intranet, or equivalent, is encouraged.
- Communications should be sent to the smallest group that covers the requirements. The use of Institute Email groups, will be limited to staff in specific Institute roles who can demonstrate a need.

Conditions of use - Internet

The Institute encourages staff and students to use the Internet in order to further the strategic and operational objectives of the organisation, and encourages the use of the Internet to share information, improve communication and to exchange ideas.

- Internet access is provided to all staff and students for use as a tool in completing job functions or in line with a course of study and should be used accordingly.
- Staff must not enter into on-line purchasing arrangements on behalf of the Institute without authorisation. On-line purchases normally involve the use of credit or charge cards, and due regard must be had to conditions regulating their use. Refer to Institute Purchasing Policies.
- Where a genuine reason exists (i.e. to support teaching or learning activities), that requires access to sites that would be normally regarded as inappropriate and/ or are blocked, the authorisation of the Chief Operating Officer is required to access those sites.
- Individual student quotas for Internet access are not enforced, however usage limits and restrictions will apply and may be enforced. Internet usage levels will be periodically checked, and any users found to have excessively high usage will be investigated and action taken where appropriate. This action may include removal of Internet access privileges for a period of time.
- The Institute will log all staff and student Internet traffic and will refer to logs as required. Staff or student internet usage may be investigated with the approval of the Manager Human Resources and/ or Manager ICT Services.
- When publishing online in the name of TAFE Gippsland, staff or students should ensure that the material would not be refused classification under the existing classification regime applying in Victoria, Australia, or which may reasonably be regarded as objectionable or offensive, or which is illegal or which may expose the Institute to legal liability, or embarrassment or is detrimental to Institute interests.

Inappropriate Use

When utilising the Internet or other forms of electronic communication, it is expected that those using the services will do so in an ethical, lawful, respectful, and appropriate manner. Inappropriate use of these services may result in disciplinary action including loss of privilege to use said services.

Inappropriate use includes, but is not limited to:

- Use of Institute equipment or services for intentionally transmitting, communicating or accessing pornographic or sexually explicit material, images, text or other offensive material.
- Intentionally creating, sending or accessing information (including pornography) that could damage the reputation of the Institute.
- Being misleading or deceptive, resulting in victimisation or harassment, leading to criminal penalty or civil liability, or being reasonably found to be offensive, obscene, threatening, abusive or defamatory.

It is inappropriate and potentially unlawful to transmit, communicate or access any material which may discriminate against, harass, bully or vilify colleagues or fellow students or any member of the public. Staff or Students may not intentionally create, transmit, distribute, or store any offensive information, data or material that violates Australian or State regulations or laws.

The Institute reserves the right to audit and remove any illegal material from its computer resources without notice. Staff and students will respect others' sensibilities and handle potentially offensive material with discretion.

Any form of bullying or harassment using Electronic Communications services will not be tolerated and any instances will be dealt with appropriately

The Institute acknowledges the rapidly growing use of social media by staff and students and encourages its use, in accordance with the institute social media procedure, for the purposes of learning, engaging, connecting and collaborating. Social media has become a key tool for staff and students to connect and engage with the Institute's communities and stakeholders on a global level. Inappropriate use of social media that results in negative perception of the Institute, its staff or students, or not in line with the social media procedure may be subject to disciplinary action in accordance with this policy.

Privacy

The Institute keeps and may monitor logs of all activity on its infrastructure including any computers, laptops, phones and data cards. This monitoring may reveal information such as which Internet servers have been accessed by employees, and the email addresses of those with whom they have communicated. The Institute will not, however, engage in real time surveillance of Internet usage, will not monitor the content of email messages sent or received by its employees, and will not disclose any of the logged, or otherwise collected, information to a third party except under compulsion of law.

On authority of the CEO, Director People and Culture or Chief Operating Officer and if the organisation reasonably believes that inappropriate use of computing or communication facilities has occurred, the Institute may review all data sent or received via its electronic communications infrastructure or placed into its storage.

It is important to remember that electronic communications may be deemed official documents that are subject to the same laws as any other form of correspondence. They are subject to statutory record keeping requirements and can be subpoenaed or "discovered" during legal processes.

Messages conveyed by electronic communication systems through the Internet are capable of being intercepted, traced or recorded by others. Although such practices may be illegal, there should not be an expectation of privacy and care must be taken with confidential documents.

During any planned absence from the workplace, all staff members must ensure that data and information required to conduct the business of the Institute are accessible and that notification facilities, such as telephone and email, out-of-office messages, are in place. In the event of unplanned leave, if practical the staff member should put such notifications in place from home or by contacting the ICT Service Desk.

A staff member's manager has the right to request notifications be put in place due to staff absences and to request access to data and information stored on Institute computers or databases with the approval of the Senior Human Resources Advisor. Such requests will be undertaken to ensure operational requirements of the Institute can continue unobstructed. Data, in this context, refers to information relevant to conducting the business of the Institute which includes email, data stored on a local personal computer or laptop including external storage devices, and data stored on supplied network storage.

Enforcement

Failure to abide by these terms will be treated as misconduct.

Staff and students are encouraged to report breaches of these guidelines to their Manager, teacher or an appropriate senior officer (for example, if they become aware that someone has used another's personal account).

A serious infringement will result in automatic denial of access to one or all facilities and will be referred to the Institute's Executive. This may result in:

- A prolonged denial of access to one or all facilities;
- Referral to the appropriate disciplinary procedures;
- Expulsion or termination; and/or
- Referral to law enforcement agencies (where the misconduct constitutes a legal offence).

Disclaimer

The Institute accepts no responsibility for any damage to or loss of data, hardware or software arising directly or indirectly from use of the Institute's computing and communications facilities or for any consequential loss or damage.

The Institute makes no warranty, express or implied regarding the facilities offered, or their fitness for any particular purpose, and does not guarantee the security of data transmitted through these services. All traffic is monitored and reviewed for content control.

By using this service you agree to work within the Institute's policy framework.

Reference and Supporting Information

Definitions

Term	Definition
Responsible and ethical behavior	Behaving in a manner (online), which is mindful of social norms, does not negatively reflect on the Institute and is within Australian law.
Social media	Online services that enable the public to openly communicate and share ideas.

Supporting Documents

External Legislative Context (Links)

- [Australian Public Service Code of Conduct](#)
- [Australian Public Service Regulations](#)
- [Crimes Act 1914](#)
- [Australian Copyright Corporation](#)
- [Copyright Act 1968](#)
- [Copyright Amendment \(Digital Agenda\) Act 2000](#)
- [Freedom of Information Act 1982](#)
- [Information Privacy Act 2000](#)
- [Public Records Act 1973](#)
- [Public Service Act 1999](#)
- [Privacy and Data Protection Act 2014](#)

Internal Policy and Procedures

ICT 009 Information Security Policy

ICT 010 Social Networking and Online Technology Policy

Responsibility

Chief Operating Officer

Manager ICT

Please Note: For further information or assistance regarding policies and procedures contact:
qa@tafegippsland.edu.au | URL: www.tafegippsland.edu.au

Document Version Control Table

Item	Summary of Update	Version Control	Revised Date
1	Original Policy Document	1.0	5/9/2014
2	Revised	2.0	1/10/2020