Purpose

To inform the University community about acceptable use of the University’s computing and communications facilities.

Scope

To inform the University community about acceptable use of the University’s computing and communications facilities.
This Policy applies to all computing and communications facilities provided by the University and to all users and uses of such services.

Legislative Context

- Australian Public Service Code of Conduct
- Australian Public Service Regulations
- Crimes Act 1914
- 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
- Victorian TAFE Teaching Staff Multi-Business Agreement 2009
- University Collective Agreement, Academic and General Staff Employees
- University Legislation: Statute 6.1 Student Discipline and Regulation 6.1 – Student Discipline
- Victorian Equal Opportunity Act 2010

Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>means this Policy and includes the Schedules and Procedures incorporated by reference.</td>
</tr>
<tr>
<td>Schedule</td>
<td>means a Schedule to this Policy. Further definitions appear in the relevant Schedules.</td>
</tr>
</tbody>
</table>

Policy Statement

Federation University Australia provides students and staff with access to computing and communications services in support of its teaching, learning, research and administrative activities. These facilities include:

- Access to a data communications network, which links the majority of University computers on campus including wired and wireless communications. The University Network is connected to an external network linking the University 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 and other on line resources.
- Access to external High Performance Computing facilities.
- Access to various printing facilities.
- An after hours access card system, allowing students access to some laboratories after business hours.
- An integrated data network across all campuses, with individual log ins for staff and students providing access to personal and shared storage space, both on the network and cloud based, and individual email accounts.
- ITS Service Desk 1800 333 864
- Student computer laboratories located across all campuses offering PC Windows based workstations and Apple Macintosh laboratories in selected locations.

Set out below are the terms governing the use of these facilities. The University may revise these terms from time to time.
These terms apply to all users and apply to use of all information technology services. Users will be required to sign or indicate their acceptance of the terms prior to obtaining access to information technology services systems. Regardless, use of any such facilities indicates acceptance of these terms. If unsure of the meaning of any of these terms, seek advice from the ITS Service Desk prior to use – phone 1800 333 864.

General

The University provides access to standalone or networked personal computers, multi-user computers and to other ITS resources accessible via on-campus networks.

It is expected that all users will make use of University computing and communications facilities in a manner, which is ethical, lawful, effective, efficient, in accordance with other University policies and not to the detriment of others. Usage must also be in line with a current course of study or job function.

In some cases external conditions of use apply. For example, the University must ensure all of its Internet traffic relates to its teaching, learning, research and administrative activities as per Australian Academic & Research Network (AARNet) usage policy.

Some services are provided on a cost recovery basis. Laser printing and colour printing are available on a fee-for-service basis.

Use of University facilities for external (non-University) work must be negotiated with the Deputy Vice-Chancellor (Student Support & Services) and will be on a fee-for-service basis.

Who Can Use The Facilities?

The following categories of people are permitted access to the computing and communication facilities:

• Students of the University for learning and research activities;
• Academic, teaching, general, associate & sessional staff who require access to ITS resources and services as part of their duties;
• Associated individuals (visiting fellows, honorary research associates);
• University based student and staff associations;
• Participants in Cooperative Research Centres and other collaborative bodies and
• Students living in University provided accommodation where Internet or network access is provided using University infrastructure.

These categories are governed by University policy and legislation and may alter over time.

Entitlements

All students are entitled to a network login account which will enable access to computing resources. Accounts are automatically created upon successful enrolment and are accessed via a user id and password. Access to any other computing and communications facilities requires authorisation.

Staff of the University are entitled to a network login account which will enable access to computing resources. Access to this account is created when the appropriate application has been authorised and lodged. Access to any other facilities is provided on a needs basis and must be authorised.

Responsibilities - Personal
The University expects all users to exercise responsible and ethical behaviour when using the computing and communications facilities. Please assist the University to keep the network available and accessible by observing the following guidelines:

- Take responsibility for using University 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 any software not provided by the University.
- Intentionally downloading unauthorised software or material breaching copyright is prohibited.
- The University network should not be used for private gain. Nor should it be used to store or collect personal information about others where not commissioned to do so.
- Connection of non-University hardware to, or interference with, the University network is not permitted without express authorisation by the Deputy Vice-Chancellor (Student Support & Services). This includes, but not limited to, wireless networking devices, printers, file servers (including web) and network equipment.
- Abide by any relevant instructions given by the Vice-Chancellor 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.

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 University enforces minimum password length and complexity rules; and
  - Log out of the network when not using it or leaving the workstation.
- Respect security measures and the integrity of University systems and files. Do not attempt to adversely interfere with the operation of the University’s computing, communications or any other facilities using the University’s 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 University computing facilities, on request of a University 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 Deputy Vice-Chancellor (Student Support & Services).

Refer Information Security Policy

Electronic Communications
Electronic communications encompasses all methods of communication utilising the University network and server infrastructure. This includes, but is not limited to, voice, video, email, instant messaging, conference calls (voice and video), file transfer and application sharing.

Federation University Australia encourages staff and students to appropriately use communication services in order to achieve the mission and goals of the University. The University also encourages the use of electronic communication to share information, to improve communication and to exchange ideas. Given that universities place high value on open communication of ideas, including those new and controversial, the intention of the University is to maximise freedom of communication for purposes that further the goals of the University.

While the University encourages the freedom of communication to further the goals of the University, there are some rules around the use of electronic communication service. These include, but are not limited to:

- Individuals must not use computing and communication facilities for commercial activities except in cases of University sanctioned activities;
- Electronic Communications services must not be used to solicit goods and services or to offer them to other members of the University community. For example, advertising rental of properties, sale of personal goods;
- Advertising or sponsorship is not permitted except where such advertising or sponsorship is clearly related to or supports the mission of the University or other service being provided;
- 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;
- University supplied email addresses should not be used as a personal email address. These are provided for University business only;
- University 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, with the exception of recording in support of teaching processes e.g. lecture capture, 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.
- For calls to both the Contact Centre and Service Desk, callers will hear a message advising calls may be recorded for quality and training purposes and be given the option to opt out of having the call recorded.

The University 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. Members of the University community are expected to demonstrate good taste and sensitivity to others in their communications.

Federation University Australia has established university and campus wide group Email addresses in order to allow more effective use of inter campus Email. Group-mailing addresses have been created for each campus and for the University 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 University business only and must not be used for personal or commercial activities;
- All communications sent to any of these group addresses should be University related. Personal announcements (eg Lost Pets, For Sale, Lights left on, Lost property etc) must not be sent to these “everyone” addresses;
- For wider distribution across all campuses, use of FedNews, or equivalent, is encouraged;
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. However, 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 University equipment or services for intentionally transmitting, communicating or accessing pornographic or sexually explicit material, images, text or other offensive material.
- It is not acceptable to intentionally create, send or access information (including pornography) that could damage the University’s reputation, be misleading or deceptive, result in victimisation or harassment, lead to criminal penalty or civil liability, or be 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 on the grounds of:
  - age;
  - carer and parental status
  - disability (including physical, sensory and intellectual disability, work-related injury, medical conditions and mental, psychological and learning disabilities)
  - employment activity
  - gender identity, lawful sexual activity and sexual orientation
  - industrial activity
  - marital status
  - physical status
  - political belief or activity
  - pregnancy and breastfeeding
  - race (including colour, nationality, ethnicity and ethnic origin)
  - religious belief or activity
  - sex
  - expunged homosexual conviction
  - personal association with someone who has, or is assumed to have, one of these personal characteristics.

Refer to Equal Opportunity and Valuing Diversity Policy

- 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 University reserves the right to audit and remove any illegal material from its computer resources without notice.
- Respect others’ sensibilities and handle potentially offensive material with discretion.
- Any form of Bulling or Harassment using Electronic Communications services will not be tolerated and any instances will be dealt with appropriately.

Internet

The University encourages staff and students to use the Internet in order to further the strategic and operational objectives of the University. The University encourages the use of the Internet to share information, to 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 exercise caution when entering into on-line University related purchasing arrangements. As with telephone orders, proper authorisation for purchases must be first obtained. 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 Purchasing Card Policy.

Where a genuine reason exists (i.e. to support teaching, learning or research activities) that requires access to sites that would be normally regarded as inappropriate, the authorisation of the Dean or Director is required.

There are no individual student quotas for Internet access, but usage limits and restrictions will apply and be enforced.

Internet usage and usage levels will be monitored by automated tools and any users found to have excessively high usage or inappropriate usage will be investigated and action taken where appropriate. This action may include removal of Internet access privileges for a period of time.

**Virus Infections**

In the event of virus or malware infection of University owned devices, it is the position of the University to clear the virus infection where possible or, if required, restore the device to a default image. Files affected by viruses that are stored in University agreed files servers will be recovered from the last available backup where appropriate. Locally stored files on the device and non-backed up files may be lost.

The University will not pay or negotiate with individuals or organisation who attempt to hold University data to ransom.

**Social Media**

Federation University Australia acknowledges the rapidly growing use of social media by staff and students and encourages its use, in accordance with the Social Media Policy, 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 University's communities and stakeholders on a global level.

Inappropriate use of social media that results in negative perception of the University, its staff or students, or not in line with the Social Media Policy may be subject to disciplinary action in accordance with this policy.

**Copyright**

- Materials and works accessible on the Internet are covered by copyright, unless there is an express statement to the contrary. Every employee and student has a responsibility to respect the rights of copyright owners and authors in works they access on the Internet, to the extent and for purposes expressed in the Copyright Act 1968. See the following University Guidelines: Audiovisual Copying & Communication, and Print & Graphic Electronic Copying & Communication.

- Acknowledge copyright obligations on electronic information, including computer software. Documents and other information accessed or used, should be cited with a proper bibliographic reference. Software and related materials protected by copyright law, licences or other contracts may not be pirated, resold or otherwise infringed.

**Reporting**

- Staff and students are encouraged to report breaches of these guidelines to their supervisor, lecturer, teacher or an appropriate senior officer. Inform the University of any suspected breach of these terms (for example, if aware that someone has used another’s personal account).
Any instances of Harassment or Bullying, including Cyber Bullying, should be referred to the Bullying Prevention and Management Policy for information and appropriate actions.

Privacy

Staff nominated by the Deputy Vice-Chancellor (Student Support & Services) will be authorised to monitor all aspects of the University network and associated infrastructure. They are also able to report any suspected inappropriate and / or illegal activity to the Manager, IT Security and Risk in the first instance for further investigation in accordance with FedUni Incident Investigation procedures.

It is also the role of the ITS Security team to actively monitor and analyse all network related activity included, but not restricted to, Internet Usage, email and dissemination and use of programs and data across the University network infrastructure.

This monitoring will be done for the sole purpose of identifying and responding to any suspected inappropriate activity.

"The content of e-mail and other electronic communications will only be accessed by the ITS Security team-
1. after approval has been obtained from the Vice-Chancellor or delegated officer; and
2. if the access is permitted by law."

All information reported to the ITS Security team shall be treated in the strictest confidence. Any reported information will be logged and relevant action taken, including reporting to relevant School or Section heads and other management as required.

See Information Privacy Policy

Facilities

- For safety reasons, do not attempt to repair any computer equipment. Please report all faults to the Service Desk, especially if the fault appears hazardous. Equipment must remain in laboratories and cabling and equipment left alone.
- In order to maintain the facilities at the best possible level eating or drinking in any of the computer laboratories is not permitted.

Health and Safety / Disability Access

- The University will supply chairs, tables and/or computers in each laboratory specifically for the use of people with disabilities. Please make these accessible to these people at all times.
- Software, such as screen readers and voice to text software, are available in all laboratories for use by people with disabilities. If there are any problems with these facilities please contact the Service Desk.
- Observe basic safety rules, such as wearing sensible footwear in the computer laboratories at all times, so that the possibility of accidents is minimised.

Accessing University Data During Staff Absence

During any planned absence from the University, all staff members must ensure that data and information required to conduct the business of the University 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 a staff member should put such notifications in place from home or by contacting the ITS 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 University computers or databases. Such requests will be undertaken to ensure operational requirements of the University can continue unobstructed, using the following process.

Data, in this context, refers to information relevant to conducting the business of the University which includes email, data stored on a local personal computer or laptop including external storage devices, and data stored on supplied network storage.

The use of this process to access data for purposes other than those stipulated above, will not be permitted (other processes may be used by the University to access data in exceptional circumstances). Appropriate consideration must be given to the privacy of the staff member and the senders of any emails or messages to that staff member.

1. The staff member’s manager will attempt to contact the staff member and reach agreement about reasonable alternative arrangements.

2. If the staff member is not able to be contacted and/or reasonable alternative arrangements cannot be agreed upon, the manager will advise the relevant Director or Dean.

3. The Director or Dean of the area must first be satisfied that reasonable efforts have been made to agree upon alternative arrangements and that the business of the University will be obstructed or delayed by the lack of access to the staff member’s data.

4. If the Director or Dean is satisfied, all requests to monitor or access another user’s data must be made in writing to the Director, Information Technology Services setting out the reason(s) for making the request.
   a. Where the Director, Information Technology Services endorses the request, he or she will then forward it to the Director, Human Resources for approval, upon which the Director, Information Technology Services will authorise a staff member to action the request with or without notice to the user whose data is to be monitored or accessed.
   b. Where the Director, Information Technology Services or the Director, Human Resources does not endorse the request, he or she will notify to requester in writing specifying the reason for rejection.

Where permission is given, the manager must access the data on a need-to-know basis only and must keep a record of all data accessed and provide this to the staff member as soon as possible. In the event of a University sanctioned investigation, all details will be recorded by the investigating individual.

The use of email as the means of communicating these requests is sufficient.

**Enforcement**

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

**Minor infringements**

For a first time offence of a minor infringement, a warning will be issued. A second time offence will result in automatic denial of access to one or all facilities for a period of three working days and up to two weeks.

**Serious Infringements**

A serious infringement includes, but is not limited to, a third and subsequent offence of a minor infringement and will result in automatic denial of access to one or all facilities and will be referred to the Deputy Vice-Chancellor (Student Support & Services). This may result in:

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

Disclaimer

The University accepts no responsibility for any damage to or loss of data, hardware or software arising directly or indirectly from use of the University’s computing and communications facilities or for any consequential loss or damage. The University makes no warranty, express or implied regarding the facilities offered, or their fitness for any particular purpose.

Supporting Documents

• Information Privacy Policy
• Information Security Policy
• Equal Opportunity and Valuing Diversity Policy
• Copyright Procedure
• Copyright Take Down Procedure
• Purchasing Card Policy
• Bullying Prevention and Management Policy
• Social Media Policy
• Social Media Procedure
• Data Classification and Usage Procedure
• Data Storage Procedure

Responsibility

Responsibility

• The nominee of the Vice-Chancellor, the Deputy Vice-Chancellor (Student Support & Services) is the responsible officer for the control and administration of this Policy.
• The nominee of the Vice-Chancellor, the Deputy Vice-Chancellor (Student Support & Services) will review this Policy by December 2019 and every two years thereafter with the outcome of the review to be reported to the Vice-Chancellor, via ITS Steering Committee.

Review of Policy

The nominee of the Vice-Chancellor, the Deputy Vice-Chancellor (Student Support & Services) will review this Policy by November 2019 and every two years thereafter with the outcome of the review to be reported to the Vice-Chancellor, via ITS Steering Committee.

Promulgation

The Use of Computing and Communication Facilities Policy will be communicated throughout the University community via:
1. an Announcement Notice via FedNews website and on the ‘Recently Approved Documents’ page on the ‘Policies, Procedures and Forms @ the University’ website to alert the University-wide community of the approved Policy;
2. distribution of e-mails to Head of School / Head of Department / University staff; and/or
3. documentation distribution, eg. posters, brochures
4. Notification to Schools

Implementation

The Use of Computing and Communication Facilities Policy will be implemented throughout the University via:
1. An Announcement Notice posted on the FedNews webpage;
2. Inclusion in the University Policy Library;
3. Distribution of e-mails to Deans / Directors / University staff; and
4. Staff induction sessions.