

Conditions of Use

Rules for the Use of Information and Communication Facilities and Services

University of New England

Overview

UNE provides Information and Communication Technology facilities and services (ICT Systems) to support the teaching, learning, research and administration of UNE. This document provides guidelines of acceptable behaviour expected of users and intending users of the ICT Systems. UNE requires that each user be aware of these Rules.

ICT Systems are provided by UNE in order that staff, students and approved affiliates of UNE can conduct bona fide academic and administrative pursuits at UNE. Users must adhere to these Rules. Where users fail to use the ICT Systems in accordance with these Rules and UNE's policies, rules, regulations and procedures UNE, reserves the right to withdraw a user's access rights to any or all of the ICT Systems.

Scope

These Rules apply to all users of the ICT Systems.

Disclaimer

UNE accepts no responsibility for any damage or loss of data arising directly or indirectly from the use of any of the ICT Systems or for any consequential loss or damage. UNE makes no warranty, express or implied, regarding the ICT Systems offered or their fitness for any particular purpose. Whilst reasonable care, consistent with good business practice, is taken, UNE cannot guarantee the confidentiality of any data stored on any UNE computer system or transmitted through any network.

UNE's liability in the event of any loss or damage is limited to the fees and charges paid to UNE for the use of the ICT Systems which resulted in the loss or damage.

General

1. Users are subject to State and Federal laws that apply to information and communication technologies as well as to other relevant legislation, policies and regulations.
2. Users must use the ICT Systems in a manner that is in the best interests of UNE and conforms with UNE's policies, guidelines, rules, regulations and these Rules.
3. Adequate measures in accordance with UNE policy must be taken by users to ensure that the security of the ICT Systems is not compromised. This includes but is not limited to virus protection, password control, physical security and software security patches. Users of mobile computing equipment must ensure that special care is taken when reconnecting to the UNE network after connecting to other home, office or public networks.

4. Users may not intentionally create, install or execute any software that may have a detrimental effect on the ICT Systems.
5. Users can only use the ICT Systems that they have been authorised to use and only for the purpose for which they were provided.
6. Authorisation to use the ICT Systems is provided to the individual user and cannot be transferred or shared.
7. Users must not, under any circumstance, represent themselves as someone else, fictional or real, and must, upon request by an authorised member of staff, produce evidence of identity when using any of the ICT Systems.
8. No unauthorised device may be connected to the ICT Systems.
9. The content of electronic material stored or transmitted on the ICT Systems must be of a professional standard, uphold the image and reputation of UNE and must not be of obscene, harassing or offensive nature.
10. Users with access to the ICT Systems containing information which is sensitive, confidential and/or subject to legal constraints may not for any reason communicate that information to any third party unless expressly authorised by UNE to do so. Users may also not communicate any information which is sensitive, confidential and/or subject to legal constraints to another person, except when necessary for the accomplishment of the tasks for which the access is given or on request by a legally authorised entity.
11. Users must be aware of and not breach copyright legislation, software licence conditions and hardware licence conditions.
12. The ICT Systems cannot be used for private or commercial gain or for gain to a third party without the written permission of the Vice-Chancellor (or nominee) or the Director ITD (or nominee).
13. Personal use of the ICT Systems is permitted if it is considered reasonable by the user's supervisor and not detrimental to the business of UNE.
14. Users must abide by any relevant instructions given by the Director (Information Technology) or nominee. Such instructions may be issued by notice displayed near the computer facilities, by letter, by electronic communication, in person or otherwise.

Privacy and Surveillance

Users should be aware that system administrators are able to access everything on the network. Email boxes will normally contain the emails and attachments they have sent and received. Back-ups and archives may also contain copies of emails and attachments that have been deleted by the user. The date and time the message was transmitted, received and opened and the email addresses of the sender and recipients will be recorded. URLs (Uniform Resource Locators) or website addresses of websites visited, the date and time they were visited and the duration of site visits are logged. The keeping of these logs is necessary for the routine maintenance and management of networks and systems and for charging purposes. Log files will be stored on a secure system that is not accessible by anyone other than the system administrators.

UNE monitors the use of computers and IT systems in the following areas:

- Email server performance; logs, backups and archives of emails or information about those emails sent and received through UNE's mailservers.
- Logs, backups and archives of all internet access and network usage. While individual usage is not routinely monitored, unusual or high volume activity may be investigated further.
- Phone logs and information about ingoing and outgoing calls.
- Overall network performance including workstations, printers and other devices connected to the network as well as servers and other elements of UNE's IT infrastructure.
- Compilation and retention of logs of network activity.

The IT monitoring described above is currently in place, ongoing and continuous.

Some circumstances may require system administrators, the Director (Information Technology) or other authorised staff of the Directorate or UNE to access information contained in log files or files and data held on devices connected to the ITC Systems or transmitted over the ITC Systems. UNE may inspect, monitor or disclose electronic mail or other electronic files without the consent of the user, to the extent permitted by law:

- when required by and consistent with law;
- when there is reason to believe or suspect that violations of law or of UNE policies (such as, plagiarism and/or academic misconduct), rules, regulations and procedures may have taken place; or
- when there are compelling circumstances (where failure to act may result in significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or UNE policies, rules, regulations and procedures or significant liability to UNE or the University community).

Penalties for Non Compliance

All misuse of the ICT Systems must be reported to the Director (Information Technology Directorate) or nominee who must deal with each event as follows:

- If deemed appropriate, immediately withdraw the user's access privileges to the network for a period not exceeding two months pending investigation.
- Ascertain or review the facts pertaining to the alleged misuse and interview the person alleged to have committed the misuse. The person alleged to have committed the misuse may be accompanied by another person, as may the Director (Information Technology) or nominee.

After the interview, the Director (Information Technology) or nominee must inform the alleged person whether or not the allegation is found to be proven. If the allegation is found proven, the Director (Information Technology) or nominee is empowered to:

- recover any costs associated with the misuse;
- impose a fine not exceeding 5 penalty units for each offence;
- withdraw the offender's access privileges to one or more ITC systems for a period deemed appropriate but not exceeding 12 months by the Director (Information Technology Directorate);
- request appropriate actions by the offender to minimise impact of the offence;
- inform relevant law enforcement agencies of the facts of the case; and
- inform the relevant Dean (students) or supervisor (staff) of the offence and the penalty imposed.
- Recommended the user for disciplinary action through the appropriate disciplinary processes (i.e. through UNE's Misconduct Policies and Procedures for staff or the Student Disciplinary Committee for students)

Appeals:

Appeals must be made in writing within ten working days of the notification of the outcome of the investigation.

Declaration:

All users of the University's computing facilities are required to agree to the following declaration before being granted access to facilities:

I agree to comply with the Rules for the Use of University Information and Communication Technology Facilities.

Signed: _____

Date: _____