

University of New England

RULES FOR THE USE OF INFORMATION AND COMMUNICATION FACILITIES AND SERVICES

Document data

Document Type	Rules
Administering entity	Information Technology Directorate
Date approved	September 2009
Records management system number	D09/112214
Approved by	Council
Indicative time for review	Annually from March 2009
Responsibility for review	Director, Information Technology
Related policies or other documents	

Contents

Rationale and Scope.....	1
Principles.....	1
Policy	2
- Security	2
- Appropriate Use.....	2
- Privacy and Surveillance	3
Penalties for Non Compliance	3
- Illegal Activity	3
- Security.....	5
- Appropriate Use.....	5
Appeals	6
References	7

1. Rationale and Scope

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 required of users of the ICT Systems. UNE requires that each user comply with these Rules as a condition of access to the systems. The rules apply to:

- All staff, students and non-UNE registrants who have access to the University's ICT systems and infrastructure.
- All University Associates who use the University's ICT infrastructure or services.
- All users of ICT equipment owned or leased by the University.
- All equipment connected to University data and voice networks.

2. Principles

2.1 The University and users of the University's ICT systems are subject to State and Federal laws that apply to information and communication technologies as well as to other relevant legislation, policies and regulations.

2.2 Users must use the ICT Systems in a manner that is in the best interests of UNE and conforms to UNE's policies, guidelines, rules, regulations and these Rules.

3. Policy

3.1 Security

- 3.1.1 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.
- 3.1.2 You shall not use any account that has been created for another user without authorisation from the Director IT or nominee.
- 3.1.3 Unless you have the explicit authorisation of the Director IT (or nominee), you shall not possess any tools, nor undertake any activities on UNE systems or services that could result or assist in the violation of any UNE policy, software licence or contract. Prohibited tools include but are not limited to: Trojans, worms, network packet observers or sniffers. Prohibited activities include but are not limited to: performing denial-of-service attacks, forging routing information for malicious purposes.

3.2 Appropriate Use

- 3.2.1 The content of electronic material stored on University ICT equipment or transmitted on the University network must be of a professional standard and uphold the image and reputation of UNE.
- 3.2.2 Users must not use the University network to access, store or transfer illegal material.
- 3.2.3 Users of the University's ICT systems must not transfer material that is likely to cause offence to the recipient, and must not use the University ICT facilities or services to express views that discriminate, harass, vilify, or bully any other users or groups. Users must not slander or defame any individual or organisation.
- 3.2.4 Content published on the University's ICT systems must comply with the University's Web Policy.
- 3.2.5 Users with access to the ICT Systems containing information which is sensitive, confidential and/or subject to legal constraints must comply with relevant privacy legislation and the University's Privacy Statement.
- 3.2.6 Users must not breach copyright legislation, software licence conditions and hardware licence conditions and must only use software for which they have a current licence.
- 3.2.7 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) and must be within the limitations of licences and Agreements.
- 3.2.8 You may use University facilities and services for incidental personal use (e.g. occasional emails and web browsing during work breaks) provided that such use does not interfere with University business operations, does not breach any Federal legislation, State legislation or University policy or an ICT vendor's conditions of use or licence agreement. Some examples of interference with

- University business operations include: disrupting ICT facilities or services, burdening the University with significant costs; or impeding one's work or other obligations to the University.
- 3.2.9 Users must abide by any reasonable and relevant instructions given by the Director (IT) or nominee in relation to use of the University's ICT facilities. Such instructions may be issued by notice displayed near the computer facilities, by letter, by electronic communication, in person or otherwise.

3.3 Privacy and Surveillance

The University complies with the Federal Privacy Law as it applies to Australian and ACT government agencies, and complies with the Workplace Surveillance Bill (2005).

Users should be aware that UNE logs and stores information on 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 relating to incoming 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.

UNE may inspect, monitor or disclose electronic mail or other electronic files without the consent of the user, to the extent permitted by law.

Users of University ICT equipment and services should be aware that email records and documents stored on University computers or systems are legally considered to be documents of the University under the *Freedom of Information Act 1989* (NSW).

4. Penalties for Non Compliance

4.1 Illegal Activity

4.1.1 Illegal Activity – UNE Staff and non-UNE registrants.

Where a formal complaint of illegal activity or alleged illegal activity by a University staff member (or non-UNE registrant) on the University's ICT systems has been made to the Director IT:

The Director IT (or nominee) will advise the staff member (or non-UNE registrant) of the complaint and will withdraw access to the University's ICT systems commensurate with managing the risk of the activity pending investigation. This may range from withdrawal of

internet and email services, to complete removal of the person's access to University ICT equipment and systems.

- i) The Director IT (or nominee) will investigate the alleged activity, and will forward findings to the University Legal Counsel.
- ii) The University Legal Counsel will inform the relevant law enforcement agency where appropriate.
- iii) The University Legal counsel will notify the relevant Cost Centre Manager, (or in the case of a Cost Centre Manager that person's supervisor) of the allegation and will provide information as relevant to the case and to the extent permitted by law.
- iv) The Cost Centre Manager (or Cost Centre Manager's supervisor) will, with advice from University Legal Counsel, manage the investigation with reference to the University's Code of Conduct and within the misconduct / serious misconduct processes under the current UNE Workplace Agreement.
- v) The University may elect to confiscate computing equipment accessed by the user alleged to have committed the offence.
- vi) ITD will provide electronic records and information to the relevant law enforcement agencies via the Director HRS within the limits of the law.

4.1.2 Illegal Activity -student

Where a formal complaint of illegal activity or alleged illegal activity by a student of the University of New England on the University's ICT systems has been made to the Director IT:

- i) The Director IT (or nominee) will advise the student of the complaint and will withdraw access to the University's ICT systems commensurate with managing the risk of the activity pending investigation. This will **not** normally include removing access to the University's Learning Management Systems.
- ii) The Director IT (or nominee) will investigate the alleged activity, and will forward findings to the University Legal Counsel.
- iii) University Legal Counsel will inform the relevant law enforcement agency where appropriate.
- iv) Where the student resides in a University college and the activity occurred from or within the College network University Legal Counsel will notify the relevant Head of College; where the student does not reside in a College, the Director, Student Administration and Services will be informed instead.
- v) The relevant Head of College or Director, Student Administration and Services will manage the investigation with reference to the Student Behavioural Misconduct Rules
- vi) The University may elect to confiscate computing equipment accessed by the user alleged to have committed the offence.
- vii) ITD will provide electronic records and information to the relevant law enforcement agencies via the Director HRS within the limits of the law.

4.2 Security

4.2.1 If the security of the University's ICT systems is at risk or under attack:

- i) ITD will immediately act to disable or disconnect the offending device to isolate it from the University's network. Where the security breach is from outside the University's network ITD will act to protect the network in whatever way it sees fit depending upon the type of breach.

- ii) Where the device is within the University network, the Director IT (or nominee) will contact the owner of the device to advise a security breach and a pending investigation in to contravention of the Rules.
- iii) The Director IT (or nominee) will investigate the facts relating to the incident.
- iv) Where appropriate, the Director IT (or nominee) will 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 IT (or nominee).
- v) After the interview, the Director IT (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 (IT) or nominee is empowered to:
 - Recover any costs associated with the misuse;
 - Request appropriate actions by the offender to minimise the impact of the offence;
 - Recommend the user for disciplinary action through the appropriate misconduct processes. For staff – UNE’s Workplace Agreement misconduct/ serious misconduct processes; for students – Student Behavioural Misconduct Rules.

4.3 Appropriate Use

For breaches of the Rules in relation to Appropriate Use:

4.3.1 UNE staff and non-UNE registrants

Where a formal complaint of a breach of the Rules in relation to appropriate use by a University staff member (or non-UNE registrant) on the University’s ICT systems has been made to the Director IT:

- i) The Director IT (or nominee) will advise the staff member or non-UNE registrant) of the complaint and will withdraw access to the University’s ICT systems commensurate with managing the risk of the activity pending investigation. This may range from withdrawal of internet and email services, to complete removal of the person’s access to University ICT equipment and systems.
- ii) The Director IT (or nominee) will investigate the alleged activity, and will notify, by email or in writing, the relevant Cost Centre Manager, or in the case of a Cost Centre Manager that person’s supervisor of the allegation and will provide information as relevant to the case and to the extent permitted by law.
- iii) The Cost Centre Manager (or Cost Centre Manager’s supervisor) will manage the investigation with reference to the University’s Code of Conduct and within the misconduct / serious misconduct processes under the current UNE Workplace Agreement.
- iv) The University may elect to confiscate computing equipment accessed by the user alleged to have committed the offence.
- v) ITD will provide electronic records and information to the Cost Centre Manger (or Cost Centre Manager’s supervisor) within the limits of the law.

4.3.2 UNE Students

Where a formal complaint of a breach of the Rules in relation to appropriate use by a UNE student on the University’s ICT systems has been made to the Director IT:

- i) The Director IT (or nominee) will advise the student of the complaint and will withdraw access to the University's ICT systems commensurate with managing the risk of the activity pending investigation. This will **not** normally include removing access to the University's Learning Management Systems.
- ii) The Director IT (or nominee) will investigate the alleged activity, and will forward findings by email or in writing to the Director, Student Administration and Services, or where the student resides in a University College and the activity has occurred within the College network, the relevant Head of College of the allegation and will provide information as relevant to the case and to the extent permitted by law.
- iii) The Director, Student Administration and Services or the Head of College will manage the investigation within the processes defined by the Student Behavioural Misconduct Rules
- iv) The University may elect to confiscate computing equipment accessed by the user alleged to have committed the offence.
- v) ITD will provide electronic records and information to the relevant law enforcement agencies via the Director HRS within the limits of the law.

5. Appeals

Appeals against the penalties must follow processes defined in the University's Workplace Agreement for University staff, or the Student Behavioural Misconduct Rules for students. Non-UNE Registrants may appeal penalties in writing within ten working days of the notification of the outcome of the investigation to the Director IT or in the absence of the Director IT to the Chief Operating Officer.

6. References

- University of New England Privacy Statement <http://www.une.edu.au/policies/pdf/privacystatement.pdf>
- UNE Web Publishing, Content and Online Applications Policy <http://www.une.edu.au/policies/pdf/web.pdf>
- Dignity and Respect in the Workplace Charter <http://www.une.edu.au/eoo/charter/dignityrespect.php>
- Staff Code of Conduct <http://www.une.edu.au/policies/pdf/codeofconductstaff.pdf>
- Curtin IT Services, IT Policy Manual, Version 3.2, July 2008.
- The University of Queensland, Handbook of University Policies & Procedures, (accessed 25th March 2009).
- NSW Office of Industrial Relations, Workplace Surveillance Act, <http://www.industrialrelations.nsw.gov.au/rights/employer/workplace+surveillance+act.html>
- Freedom of Information Act 1989 (NSW).
- UNE Workplace Agreement <http://www.une.edu.au/hrs/handbook/05/5.09.pdf>
- Student Behavioural Misconduct Rules <http://www.une.edu.au/policies/pdf/studentbehaviouralmisconductrules.pdf>