Computer Systems Regulations

Responsibility: Chief Information Officer
Approving authority: Vice-Chancellor
Last reviewed: May 2019
Next review: May 2024

Application

1. These regulations apply to all users of the University of Waikato's computer systems and ICT.

Purpose

2. The purpose of these regulations is to provide a framework for the use of the computer systems and ICT provided by the University for use in teaching, learning and research and to support the effective operation of the University.

Related documents

3. The following documents set out further information relevant to these regulations:
   - Code of Student Conduct
   - Corporate Data Management Policy
   - ICT Strategy 2017-2019
   - Information Security Standards
   - Personal Information and Privacy Policy
   - Privacy Act 1993
   - Public Records Act 2005
   - Social Media Policy
   - Staff Code of Conduct
   - Student Discipline Regulations
   - University of Waikato Privacy Statement

Definitions

4. In these regulations:

   computer system means a system made up of ICT components

   information and communications technology (ICT) means hardware and software, data and associated infrastructure and devices that are:

   i. owned, leased, controlled or operated by the University, or
   ii. connected by physical or wireless connection to the University network

   ICT includes, but is not limited to, computers (such as desktops, laptops, tablets), storage devices (such as portable hard drives, USB and flash memory devices, CDs, DVDs), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers and telecommunication equipment, networks, software, cloud services, databases and any other similar technologies as they come into use

   objectionable material means all material which is objectionable as defined in the Films, Videos, and Publications Classification Act 1993 and any other material which could reasonably be described as unsuitable or offensive having regard to the circumstances in which, and the persons to whom, it becomes or may become available

   system manager in relation to a computer system means:

   i. a Pro Vice-Chancellor, Deputy Vice-Chancellor, Head of School, Director or equivalent, or delegated authority
   ii. the Chief Information Officer or delegated authority

   University means the University of Waikato

University network means any University communications and data network on and between its campuses or other locations, including the internet

user means a person using a University computer system who is:

i. a staff member of the University, whether employed on a fixed-term, continuing, full-time, part-time or casual basis
ii. a student enrolled at the University
iii. a contractor, or
iv. any other person authorised to use a University computer system by a system manager.

Principle

5. University computer systems and ICT resources are made available to users for the purpose of teaching, learning and research and to support the effective operation of the University.

Access to computer systems and ICT resources

6. A user's entitlement to access and use the University's computer systems and ICT resources is:
   i. by virtue of their status as a staff member, student, contractor, or
   ii. otherwise afforded them by a system manager.

Responsibilities

7. University computer system and ICT resource users must:
   a. comply with all applicable New Zealand laws, including but not limited to, law on copyright, privacy, defamation, fraud, objectionable material and human rights
   b. comply with the terms of any licence agreement between the University and any third party that governs the use of software, computer systems or other ICT resources
   c. comply with any instruction given by a system manager about the use of the University's computer systems or ICT resources
   d. respect the rights of other users with respect to access to computer systems and ICT resources and enjoyment of use
   e. take all reasonable precautions to secure their passwords, account credentials, software and data; if access is compromised or potentially insecure they must immediately notify the ITS Service Desk and, as soon as is practicable, implement a new secure password.
8. University computer system and ICT resource users must not:
   a. use or attempt to use a computer system in a manner that will incur costs to the University without the consent of the relevant cost centre manager, or will incur costs to any other person or organisation without the consent of that person or organisation
   b. gain access or attempt to gain access to a computer system without authorisation as a user of that computer system by a system manager
   c. use a University computer system or ICT resources to attempt to gain unauthorised access to computer systems or ICT resources of any third party
   d. do anything that deliberately damages, restricts, jeopardises, impairs or undermines the performance, usability, reliability, confidentiality or accessibility of any computer system or ICT resource
   e. use a computer system or ICT resource to deceive others, including by impersonating another person
   f. give their password or divulge an access code to any other person that enables access to a computer system or use the username and password of another user to log into any University system
   g. use, make copies or distribute proprietary software, media or data without the authority of the software provider or media or data owner
   h. distribute outside the University, in whole or in part, an application program containing embedded proprietary software, or publish material identifying proprietary software, without the written permission of the software provider

i. use a computer system or ICT resource to impede the activities of the University or to interfere with the reasonable use of computer systems or ICT resources by another person
j. use a computer system or ICT resource for the purpose of accessing, sending or attempting to send objectionable material or abusive, fraudulent, harassing, threatening or illegal content
k. use a computer system or ICT resource in any way that constitutes discrimination, bullying or harassment
l. use a computer system or ICT resource in a manner, or for a purpose, which would or could bring the University into disrepute
m. assist, encourage or conceal any unauthorised use, or attempt at unauthorised use, of any computer system or ICT resource
n. make unreasonable use of a computer system or ICT resource for personal purposes, including undertaking private business activity, without the consent of the Chief Information Officer
o. use a computer system or ICT resource in a way that is inconsistent with their conditions of enrolment, employment or contract.

9. Internet and online resource users must:
   a. ensure that any University internet (web) publication conforms to lawful and reasonable employer instructions and policies regarding on online publication, including the Social Media Policy
   b. not, unless authorised by a system manager, request or accept payment, in money, goods, services, favours or any other form of remuneration, either directly or indirectly, for any activity using a University computer system or ICT resource
   c. acknowledge that the University is not responsible for the content of, or events arising from, communications or interactions between users and others on internet sites where access is not controlled by the University.
10. System managers are responsible for:
   a. maintaining security of the computer systems for which they are responsible sufficient for authorised users to make effective use of the facilities on those systems
   b. maintaining the integrity of users' passwords and privacy, and any other security mechanisms
   c. monitoring the activities of users and inspecting files and other information for the specific and sole purpose of ensuring compliance with these regulations.
11. The Chief Information Officer is responsible for:
   a. determining and issuing Information Security Standards to ensure appropriate levels of performance, security, compatibility and legal compliance of computer systems including, in the event of a serious and imminent threat to the operation or security of a computer system or ICT resource, urgent Information Security Standards.
   b. taking any immediate action appropriate to ensure that system performance, security, compatibility and legal compliance are protected if they believe on reasonable grounds that an Information Security Standard issued under subclause 11a of these regulations has been breached.

Personal information and privacy

12. The University of Waikato Privacy Statement describes how the University collects, stores, uses and shares personal information and explains the rights of staff, students and others in relation to those activities.
13. System managers have authority to:
   a. inspect and monitor the University computer systems or ICT resources for which they have responsibility where:
      i. there are reasonable grounds to suspect there may have been or be a breach of any University statute, code, regulation or policy, the terms of a University employment agreement or contract for services, or of New Zealand law, or

ii. for systems maintenance, problem resolution and capacity planning purposes or for similar reasons related to ICT security, performance or availability.

b. access personal information about a user and the user's activities on University computer systems or ICT resources for which they have responsibility where there are reasonable grounds for suspecting that the user may have breached these regulations

c. provide personal information accessed under subclauses 13a and b of these regulations to staff of the University responsible for cost centre management, student discipline and staff discipline, or other relevant authorities, including, if a crime appears to have been committed, the Police.

Breaches

14. The Chief Information Officer or delegated authority may immediately exclude from any computer system or ICT resource any user who they consider to be, or to have been, in breach of these regulations where that breach poses a serious or imminent threat to the operation or security of a computer system or ICT resource while the matter is investigated.
15. The exclusion of any user from the use of any computer system or ICT resource must be notified to the user at the time of exclusion.
16. The exclusion of a student user from the use of any computer system or ICT resource for more than 24 hours must be reported to the relevant Head of School and the Director of Student Services to be taken into account in terms of the student's coursework.
17. The exclusion of a staff user from the use of any computer system or ICT resource must be reported to their line manager at the time of exclusion.
18. Any exclusion of a user for more than 72 hours must be reported to the Vice-Chancellor.
19. Any user who has been excluded from the use of any Computer system or ICT resource under clause 14 of these regulations may appeal the exclusion decision to the Vice-Chancellor.
20. The Vice-Chancellor may suspend an exclusion until an appeal has been heard and determined.
21. If, under clause 14 of these regulations or at any other time, the Chief Information Officer considers that a breach of these regulations contravenes the Code of Student Conduct or the Staff Code of Conduct they may refer the matter to be dealt with in accordance with clauses 24-25 of these regulations.

Waivers and variations

22. Only the Chief Information Officer has authority to vary or waive the provisions of these regulations in individual cases.

Responsibility for monitoring compliance

23. The Chief Information Officer is responsible for monitoring compliance with these regulations and reporting any breaches to the Vice-Chancellor.
24. Breaches of these regulations by students may result in disciplinary action under the Student Discipline Regulations.
25. Breaches of these regulations by staff may result in disciplinary action under the Staff Code of Conduct.
26. Breaches of these regulations by contractors or any other authorised users will be dealt with in accordance with the relevant contract or arrangement