Computer Systems Policy

Responsibility: Chief Information Officer
Approving authority: Vice-Chancellor
Last reviewed: December 2024
Next review: December 2029

Application

1. This policy applies to all staff users of the University of Waikato's computer systems, networks and ICT resources.

Purpose

2. The purpose of this policy is to provide a framework for the acceptable use of the computer systems, networks and ICT resources provided by the University for staff use in teaching, learning and research, and to support the effective administration and operation of the University.

Related documents

3. The following documents set out further information relevant to this policy:
   - Corporate Data Management Policy
   - Desktop Computer Standards
   - Information Security Standards
   - Personal Information and Privacy Policy
   - Privacy Act 2020
   - Public Records Act 2005
   - Records Management Policy
   - Social Media Policy
   - Staff Code of Conduct
   - University of Waikato Privacy Statement

Definitions

4. In this policy:
   computer system means a software application and/or a system made up of one or more software applications
   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 resource means, 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
   network means any University communications and data network on and between its campuses or other locations, including the internet

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

staff means any person with an employment agreement with the University, including an independent contractor (being a person with a contract for services with the University); or an employee of a separate organisation that is contracted to perform work on University premises; or any person otherwise given access to University computer systems, networks and ICT resources

system manager in relation to a University computer system means:

i. the Chief Information Officer or delegated authority

ii. a Pro Vice-Chancellor, Deputy Vice-Chancellor, Head of School, Director or equivalent, or delegated authority

University means the University of Waikato

University business means any activity that a staff member is expected to undertake during the course of their work

user means a person using a University computer system, network or ICT resource.

Principle

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

Access to University computer systems, networks and ICT resources

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

Responsibilities

7. University computer system, network 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, networks or ICT resources
   d. respect the rights of other users with respect to access to University computer systems, networks and ICT resources and enjoyment of use
   e. use only University computer systems and productivity suite resources for University business
   f. only access University computer systems, networks and ICT resources to which they have been granted access and acknowledge that, in accordance with the Corporate Data Management Policy, the ability to read, execute, modify, delete or copy information accessed via them does not imply permission to do so

g. acknowledge that all information and communications created, transmitted or stored through the University's computer systems, networks and ICT resources are considered information assets owned by the University and may be accessed, monitored, reviewed and disclosed for security, investigation, maintenance and legal purposes; there can be no expectation of privacy with respect to these information assets
h. ensure that confidential and other sensitive University information is not stored on ICT resources used when travelling to countries where there is risk of foreign interference and/or cybercrime
i. ensure that personally identifiable information, confidential information and other sensitive information accessed via University computer systems, networks or ICT resources is kept secure and remains confidential, even after employment ceases
j. 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
k. complete any mandatory computer use training within the prescribed timeframe for completion
l. immediately contact the ITS Service Desk as soon as they become aware of any event in relation to the use of University computer systems, networks or ICT resources which threatens the availability, integrity or confidentiality of University information, or which breaches any standard, policy, procedure or any associated requirement, or is contrary to law.

8. University computer system, network and ICT resource staff 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, network or ICT resources to attempt to gain unauthorised access to computer systems, networks 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, network or ICT resource
   e. connect or attempt to attach any network switching or routing equipment to a University network without authorisation
   f. use a University computer system, network or ICT resource to deceive others, including by impersonating another person
   g. use personal email accounts, social media accounts or other non-University online systems accounts to conduct University business
   h. forward any digital communication received as part of University business to any personal account

i. maintain access to University computer systems, networks and ICT resources when they are no longer employed or contracted by the University, unless authorised by the Chief Information Officer
j. give their password or divulge an access code to any other person that enables access to any University computer system or use the username and password of another user to log into any University computer system
k. use, make copies or distribute proprietary software, media or data without the authority of the software provider or media or data owner
l. 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
m. use a computer system, network or ICT resource to impede the activities of the University or to interfere with the reasonable use of computer systems, networks or ICT resources by another person
n. use a computer system, network or ICT resource for the purpose of accessing, sending or attempting to send objectionable material or abusive, fraudulent, harassing, threatening or illegal content
o. use a computer system, network or ICT resource in any way that constitutes discrimination, bullying or harassment
p. use a computer system, network or ICT resource in a manner, or for a purpose, which would or could bring the University into disrepute
q. assist, encourage or conceal any unauthorised use, or attempt at unauthorised use, of any computer system, network or ICT resource
r. make unreasonable use of a computer system, network or ICT resource for personal purposes, including undertaking private business activity, without the consent of the Chief Information Officer
s. use a computer system, network or ICT resource in a way that is inconsistent with their conditions of employment or contract.

9. University internet and online resource users must:
   a. ensure that any internet (web) content accessed, uploaded or downloaded conforms to New Zealand laws, including but not limited to, law on copyright, privacy, defamation, fraud, objectionable material and human rights 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, network 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. ensuring that University information assets are classified and appropriately protected to prevent data leakage or loss
d. monitoring the activities of users and inspecting files and other information for the specific and sole purpose of ensuring compliance with this policy.

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, network 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 this policy or any Information Security Standard issued under subclause 11a of 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, networks 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 staff user and the user's activities on University computer systems, networks or ICT resources for which they have responsibility where there are reasonable grounds for suspecting that the staff user may have breached this policy
    c. provide personal information accessed under subclauses 13a and b of this policy 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
    d. permit access on their behalf by other staff to a staff user's University computer system, network and ICT resources as appropriate to undertake the activities listed in subclauses a to c and to ensure the ongoing effectiveness of University administration and operations.

Breaches

14. The Chief Information Officer or delegated authority may immediately exclude from any University computer system, network or ICT resource any staff user who they consider to be, or to have been, in breach of this policy where that breach poses a serious or imminent threat to the operation or security of a University computer system, network or ICT resource while the matter is investigated.
15. The exclusion of any staff user from the use of any computer system, network or ICT resource must be notified to the staff user at the time of exclusion.

16. The exclusion of a staff user from the use of any computer system, network or ICT resource must be reported to their line manager at the time of exclusion.
17. The exclusion of a staff user from the use of any computer system, network or ICT resource for more than 24 hours must be reported to the relevant divisional Pro Vice-Chancellor, Head of School and the Director of People and Capability.
18. Any exclusion of a staff user for more than 72 hours must be reported to the Vice-Chancellor.
19. Any staff user who has been excluded from the use of any Computer system or ICT resource under clause 14 of this policy 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 this policy or at any other time, the Chief Information Officer considers that a breach of this policy contravenes the Staff Code of Conduct they may refer the matter to be dealt with in accordance with clause 23 or 24 of this policy.

Waivers and variations

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

Responsibility for monitoring compliance

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