Information Technology Conditions of Use Policy

Section 1 - Audience

(1) This policy applies to all users of the University's ICT resources, connected systems, data and information assets.

Section 2 - Purpose

(2) The University has a responsibility to ensure the appropriate use of its ICT resources and to protect itself from any operational, financial, reputational, legal and compliance implications that could arise from their inappropriate use.

(3) This policy informs users of the University's ICT resources of their rights and responsibilities, and the University requires users to comply with this policy as a condition of use.

(4) In support of these objectives, this policy defines conditions of use to help ensure the confidentiality, integrity, and availability of University systems and information.

Section 3 - General Principles

(5) The University's ICT resources exist and are maintained to support the achievement of the University's objectives. Access to, and use of the University's ICT resources comes at a cost to the University and is not provided to users unconditionally. The University reserves the right to:

a. continuously monitor (subject to section 7 below) the use of its ICT resources;
b. deal appropriately with users who use ICT resources in ways contrary to this policy or contrary to law; and
c. undertake or perform any actions as required by any and all applicable laws, legislation and regulations.

(6) Materials and data produced, stored and destroyed using the University's ICT resources are to be managed subject to the relevant University policies, including the Records and Information Management Policy, Privacy and Information Access Policy, Intellectual Property Policy and Research Data and Primary Materials Management Procedure.

(7) The University accepts no responsibility for loss or damage, consequential loss or damage, or loss of data arising from the use or the maintenance of its ICT resources.

(8) All users must comply with this policy with respect to the University's ICT resources. A failure to comply with this policy may result in, without limitation:

a. for students, disciplinary action taken under the Student Conduct Rule for student misconduct;
b. for employees, disciplinary action taken under the relevant enterprise agreement, University policy and/or employment contract;
c. for service providers, termination of the contract with the University; and
d. for all users (including those categories above), restriction or cancellation of access to the University's ICT

resources; and

e. for all users, where a failure to comply could also amount to criminal conduct, referral to the relevant external authority.

Section 4 - Conditions of Use

Permissible Use

(9) Users may access and use the University's ICT resources for legitimate work, study and research purposes.

(10) Users are permitted to use the University's ICT resources for minor and incidental personal use. Access and use of the University's ICT resources is a privilege which can be restricted or cancelled by the University at any time if a user's personal use interferes with the operation of the University's ICT resources, burdens the University with incremental costs, or interferes with the user's obligations to the University.

(11) Incidental personal use does not extend to:

a. intentionally downloading, transmitting or storing unauthorised copyright material;
b. the use of peer-to-peer file sharing software or other software, as defined in "What applications are forbidden on the University network?" (as amended from time to time), that does not align with a business, research or teaching requirement of the University;
c. the use of unapproved Virtual Private Networking (VPN) services or network anonymisers while connected to, or connecting to, the University ICT network; or
d. the use of cryptocurrency mining software and hardware.

(12) Users should be aware that personal use of the University's ICT resources may result in the University holding personal information about the user and/or others which may then be accessed and used by the University to ensure compliance with this, and other policies.

Requirements

(13) Users must take reasonable steps to ensure the security of University information when it is stored or processed, and to prevent the loss or leakage of account credentials.

(14) Users must, when using the University's ICT resources, do so in a responsible, ethical and equitable manner, in accordance with the University's Code of Conduct and all applicable policies, laws, legislation and regulations.

(15) All users must take care to access the University's ICT resources, including email, only from secure or trusted computers, and to lock computers or log out of sessions before leaving any computer unattended.

Restrictions on Use

(16) Users must not use the University's ICT resources in a manner that is harassing, discriminatory, defamatory, vilifying, abusive, rude, insulting, threatening, obscene or otherwise inappropriate.

(17) Users must not use the University's ICT resources in such a way to cause embarrassment or loss of reputation to the University.

(18) Users must not use the University's ICT resources to impersonate, or falsify information about, other persons. This includes altering, removing, or forging email headers, addresses, or messages, or otherwise impersonating or attempting to pass oneself off as another person.

(19) Users must not use the University's ICT resources to access, store or transmit pornographic material of any sort other than with specific written approval from an authorised University Officer for research related purposes. Where an approval is granted, users must exercise caution, including the use of a secure drive (not a shared college drive) to avoid undue circulation or access to files.

(20) Users must not use the University's ICT resources in a manner that constitutes an infringement of copyright or infringes a person's moral rights (as defined under the Copyright Act 1968 (Cth)).

(21) Users must not download and/or store copyright material on University ICT resources (including websites and file shares), transfer copyright material to others or copy copyright material to any removable media using the University's ICT resources, unless the copyright material is appropriately licensed or the copyright owner has provided the appropriate consent.

(22) Users must not use the University's ICT resources to collect, use or disclose personal information in ways that breach the University's Privacy Management Plan.

(23) Users must not use the University's ICT resources for unauthorised profit making or commercial activities. Employees are referred to the University's Outside Work Policy.

(24) Users must not use the University's ICT resources to distribute unsolicited advertising material from organisations having no connection with the University or involvement in its activities.

(25) Users must not use the University's ICT resources in a manner which is likely to corrupt, damage or destroy data, software or hardware, either belonging to the University or to anyone else, whether inside or outside the University network. Users may only delete and alter data as required by authorised University activities with regard for data retention requirements outlined in the University's Records and Information Management Policy.

(26) Users must not use the University's ICT resources to gain, or attempt to gain, unauthorised access to any computer service. The use of another person's login, password or any other authentication device is not permitted.

(27) Users must not exploit any vulnerabilities in systems or use any technology designed to locate such vulnerabilities or circumvent security systems, apart from authorised staff in the course of their duties to assess system security.

(28) Users must not attempt to create or install any form of malicious software (for example worms, viruses, sniffers, malware, ransomware) which may affect computing or network equipment, software or data as part of the University's ICT resources, or which seek or gain access to data or user accounts, or eavesdrop on or intercept network transmissions; apart from authorised staff and researchers in the course of University-approved duties.

(29) Users must not extend the University network by introducing an unauthorised hub, switch, router, wireless access point, or any other service or device that permits more than one device to connect to the University's network.

(30) Users must not facilitate or permit the use of University ICT resources by persons not authorised by the University.

(31) Users must not make their individually assigned University password available to any other person.

(32) Users must not change operating system configurations, upgrade existing operating systems, or install new operating systems on University owned and managed devices. In exceptional cases, reinstallation of other operating systems may be permitted subject to prior approval by the Chief Information Officer (CIO) (or their delegate) through an IT Service Desk request.

(33) Users must not alter, or add to in any way to, computer equipment supplied by the University without prior authorisation via the IT Service Desk unless it is the connection of external equipment via externally accessible input

and output ports such as USB (Universal Serial Bus), VGA (Video Graphics Array), HDMI (High-Definition Multimedia Interface), Thunderbolt, and DVI (Digital Visual Interface).

(34) Network connections in University provided student accommodation facilities remain subject to this policy.

(35) To ensure compliance with state, federal and international data protection legislation, users must not, without appropriate authorisation, store or process University data in “cloud” services other than those provided by the University.

Section 5 - Personal Device Usage (including Bring Your Own Device (BYOD))

(36) Personal Device Usage includes any electronic device owned, leased or operated by an employee, contractor, affiliate or student of the University which is capable of storing data and connecting to a network, including but not limited to mobile phones, smartphones, tablets, laptops, personal computers and notebooks.

(37) Users must ensure that usage of personal devices both on the University network and when handling University data meets all the applicable requirements of this policy and the BYOD Manual.

(38) When using personal devices to connect to the University network, users shall ensure that such devices have up-to-date security patches and anti-virus software installed. Refer to the Information Security Patch Management Manual and Information Security BYOD Manual for further details.

Section 6 - Authorised Access

(39) Access to the University's ICT resources must be based on the concept of least privilege (i.e. access is to be limited on a need to know basis).

(40) All access to the University's ICT resources must be authorised by the appropriate System Owner.

(41) No user of University's ICT resources may ever knowingly exceed their authorised access level. If additional access is required for a user to perform their duties then this access must be granted by the System Owner or their delegate.

(42) The University reserves the right, at its discretion, to grant, limit or withdraw access to some or all of its ICT resources either temporarily or permanently.

Access to Email, Calendar and Related Services - Staff

(43) In the event of a staff member being absent on either unexpected or approved leave, or has left the organisation, that staff member agrees that the University may arrange for their supervisor to obtain access to their email, calendar, or any other ICT resource, in order to ensure that University operations are not disrupted.

(44) A request to arrange access to an absent staff member's email, calendar or other ICT resource must be made to the CIO by the Head of School or Division.

Proxy Access

(45) Proxy use of another user's account is permissible where both parties agree and where there is a legitimate business need for such access. Proxy access must be configured within the system and not through the sharing of credentials, and must be in accordance with any third party arrangements that the University has entered into.

Removal of Access

(46) The University will disable any user account which the University has provided to a user (such as a staff member, student, affiliate, etc) when that user ceases to be an authorised user, e.g. when a staff member ceases to be a member of staff, or a student withdraws from study at the University.

(47) The University may remove access to systems and functions when a user's role changes within the University, e.g. when a member of staff changes their job role, or a student graduates to become a University Alumni.

Extended Access

(48) Where it is in the interest of the University, approval may be given for access to its ICT resources after a person ceases to qualify as a user, as defined above. Such access may be provided at the discretion of a Delegated Authority in accordance with the University's Delegation of Authority Policy.

Section 7 - Monitoring

(49) Subject to any law or written agreement to the contrary, the University reserves the right to view, modify, copy, move, delete or otherwise handle as it sees fit the data and information assets stored on and accessed through the University's ICT resources, irrespective of any ownership or other rights claimed over the data or information assets.

(50) Consistent with generally-accepted business practice but without limiting the remainder of this section, the University may audit and monitor the use of the University's ICT resources. The University may also look at and copy any information, data or files (including non-University material) created, sent or received by users using, or while connected to, the University's ICT resources. Users are responsible for all activities originating from their account, including all information sent, requested, solicited or viewed from their account as well as publicly accessible information placed on a computer using their account.

(51) The University's electronic communication systems generate detailed logs of all transactions and use. Users should be aware that the University has the ability to access these records and that system administrators have the ability to access the content of electronic communications and files sent and stored using the University's ICT resources.

(52) The University reserves the right to remove or restrict access to any material within the University domain.

(53) The University will conduct computer surveillance continuously on an ongoing basis with respect to its employees who are using the University's ICT resources and connected systems to ensure that its users are complying with their obligations under this policy, the University's other applicable policies, standards, guidelines and procedures and all applicable legislation.

(54) Computer surveillance means surveillance by means of software or other equipment that monitors or records the information input or output, or other use, of a computer (including, but not limited to, the sending and receipt of emails and the accessing of internet websites).

(55) This computer surveillance will be carried out by the University by:

a. recording the detailed logs of all transactions and use by its users of the University's ICT resources;
b. accessing University email accounts, archives, backups or emails; even where the user has deleted an email, the University may still retain archived and/or backup copies of the email;
c. accessing files stored on network drives, computers or in cloud services to which the University has administrative access; even where the user has deleted a file, the University may still retain archived and/or backup copies of the file;

d. accessing University owned work computers, including computer security and event logs;
e. recording network traffic activity including internet usage (including sites and pages visited, files downloaded, video and audio files accessed and data input) and accessing these records;
f. accessing system and event logs and login activity relating to the University's ICT resources; and
g. monitoring on a continual basis, through manual analysis and automated correlation activities using the University's Security Information and Event Management (SIEM) solution.

(56) For the purposes of the Workplace Surveillance Act 2005 (Cth), this policy constitutes written notice of the University's computer surveillance of its employees.

(57) The University's users acknowledge that as a result of this computer surveillance, the University may prevent, or cause to be prevented, delivery of an email sent to or by, or access to an internet website by, the user.

(58) As soon as reasonably practicable, the University will notify an employee where an email has not been delivered except where:

a. the email was a commercial electronic message within the meaning of the Spam Act 2003 (Cth);
b. the content or any attachment to an email would or might result in an unauthorised interference with, damage to or operation of, a computer or computer network of the University or any program run by or data stored on such a computer or computer network;
c. the email or any attachment would be regarded by a reasonable person as being (in all circumstances) harassing, menacing or offensive; or
d. the University is not aware (or could not reasonably be expected to be aware) of the identity of the employee that sent the email or that the email was sent by an employee.

(59) The University will not prevent the delivery of an email or access to a website merely because:

a. the email was sent by or on behalf of an industrial organisation of the employees or an officer of such an organisation; or
b. the website or email contains information relating to industrial matters (as defined in the Industrial Relations Act 1996 (NSW).

(60) Each user acknowledges that the University may be required to produce the records it has obtained (as a result of the monitoring it has undertaken in relation to its ICT resources) as a result of a request made under the Government Information (Public Access) Act 2009.

Section 8 - Investigations

(61) Any identified use of equipment or services deemed inconsistent with any terms specified in this policy may be investigated by the University.

(62) Inappropriate use will be subject to consideration under relevant disciplinary or misconduct processes and may involve a range of actions, including but not limited to, suspension of access to the University's systems. See Code of Conduct and Student Conduct Rule for more information on disciplinary and misconduct processes.

(63) Written approval of the appropriate DVC, COO or equivalent is required for any investigation activity.

(64) The University may withdraw access to the University's ICT resources commensurate with managing the risk of the activity while the investigation is in process.

Section 9 - Confidentiality and Privacy

(65) While the University's ICT resources are electronically safeguarded and maintained in accordance with current best practice, no guarantee can be given regarding the confidentiality, integrity and availability of any information.

(66) Email and other records stored in the University's ICT resources may be the subject of a subpoena, search warrant, discovery order or similar legal application.

(67) Disclosure outside the University of any personal information must be in accordance with the Privacy and Personal Information Protection Act 1998 No 133, the Government Information (Public Access) Act 2009, the Health Records and Information Privacy Act 2002 No 71, the University's Privacy and Information Access Policy and its Privacy Management Plan.

Section 10 - Reporting

(68) Users must promptly report breaches of this policy and any information security incidents, breaches or suspected breaches to Information Technology Services through the University IT Service Desk.

(69) Users have an obligation under the University's Code of Conduct and the Public Interest Disclosures Policy to report misuse of the University's resources.

Section 11 - Security Instructions

(70) Users must abide by any relevant instructions given by the CIO or nominated officers. Such instructions may be issued by notices displayed in the vicinity of computing facilities, by letter, by electronic communication, in person or otherwise.

Section 12 - Enforcement

(71) All Users of the University's ICT resources should be aware of this policy, their responsibilities and obligations.

(72) Non-compliance with the provisions of this policy may result in action under the University's policies, code of conduct or enterprise agreements, and may also result in referral to a statutory authority and/or agency.

(73) The CIO (or delegate) is responsible for monitoring use of the University's ICT resources.

(74) If the CIO (or delegate) deems that an identified use of equipment or services is inconsistent with any terms specified in this policy, such use may be investigated by the University.

Section 13 - Exceptions

(75) Exceptions to this policy may be requested by a user in writing to the CIO. Exceptions will be assessed based on the business impact, the security risk that the proposed exemption may pose, and any compensating controls that may be implemented in relation to the proposed exemption.

Section 14 - Roles and Responsibilities

(76) The CIO is responsible for IT Conditions of Use Policy development and manages arrangements for information security.

(77) The CIO is responsible for:

a. ensuring that users are aware of this policy;
b. monitoring use of the University's ICT resources, and disconnecting or restricting a user's access if the user has failed to comply with this policy or any of the University's other IT policies, standards, guidelines and procedures;
c. maintaining this policy; and
d. regularly reviewing and updating this policy to ensure that the policy continues to be suitable, adequate and effective.

Information Security Team

(78) The Information Security Team reports to the Associate Director, Enablement who reports to the Chief Information Officer. The Information Security Team is responsible for:

a. performing compliance and audit functions in accordance with this policy; and
b. investigating and reporting on suspected breaches of this policy.

All Users

(79) All users of the University's ICT resources are expected to recognise the importance of this policy, and to be familiar with the provisions of this policy and to support the processes that will appropriately manage security and the confidentiality, integrity and availability of the data assets and University information.

(80) The requirements set out in this policy do not in any way authorise a user to disregard any obligations the user is required to comply with by law.

(81) Any user who is unsure of the meaning of any of these terms, should seek advice from the IT Service Desk prior to use, either:

a. by phone on +61 2 492 17000;
b. online at IT Service Desk; or
c. by email at 17000@newcastle.edu.au.

Status and Details

Status	Historic
Effective Date	17th June 2019
Review Date	17th June 2021
Approval Authority	Chief Information Officer
Approval Date	11th June 2019
Expiry Date	9th October 2022
Responsible Executive	David Toll Chief Operating Officer
Enquiries Contact	Information Security Team

Glossary Terms and Definitions

"University" - The University of Newcastle, a body corporate established under sections 4 and 5 of the University of Newcastle Act 1989.

"Risk" - Effect of uncertainty on objectives. Note: An effect is a deviation from the expected, whether it is positive and/or negative.

"Asset" - Any tangible or intangible item (or group of items) that the University owns or has a legal or other right to control and exploit to obtain financial or other economic benefits.

"Commercial activities" - As defined in the University of Newcastle Act 1989.

"Connected systems" - Systems or computers connected to the University's ICT resources (including through non-University equipment).

"Law" - All applicable statutes, regulations, by-laws, ordinances or subordinate legislation in force from time to time anywhere in Australia, whether made by the Commonwealth, a State, a Territory or a local government and, where the context permits, includes the common law and equity.

"Personal information" - Has the same meaning as in the Privacy and Personal Information Protection Act 1998 (NSW).

"Student" - A person formally enrolled in a course or active in a program offered by the University or affiliated entity.

"Student misconduct" - Academic misconduct, non-academic misconduct and/or research misconduct.

"Disciplinary action" - When used in relation to staff of the University, this is as defined in the applicable and current Enterprise Bargaining Agreement, or the staff member's employment contract. When used in relation to students of the University, this is as defined in the Student Conduct Rule.

"Exemption" - When referring to a student's learning pathway, exemption means being excused from undertaking preparatory subjects, units, modules or competencies in a course or program, while still being required to undertake the same number of subjects, units, modules or competencies as would be completed if an exemption had not been granted. For all other uses of this term, the generic definition applies.

"ICT resources" - All information and communication technology resources and facilities.

"Information asset" - A body of information, knowledge or data that is organised as a single entity and has value to

the University.

"Officer" - Has the meaning given in the Corporations Act 2001 (Cth), or any replacing legislation.

"Program" - When referring to learning, a program is a sequence of approved learning, usually leading to an Award. For all other uses of this term, the generic definition applies.

"Removable media" - Any type of storage device that can be removed from an ICT resource while the system is running.

"Research" - As defined in the Australian Code for the Responsible Conduct of Research, or any replacing Code or document.

"Staff" - Means a person who was at the relevant time employed by the University and includes professional and academic staff of the University, by contract or ongoing, as well as conjoint staff but does not include visitors to the University.

"System Owner" - An authorised individual who has been allocated responsibility by the University and is held accountable for an ICT resource.

"Third party" - A person or group other than the University or any of the University's partner institutions.

"College" - An organisational unit established within the University by the Council.