5Australian Capital Territory

University of Canberra Facilities (Information and Communication Technology Network) Rules 2023

made under the

University of Canberra Act 1989, s 40 (Statutes) **and** ***University of Canberra (Facilities) Statute 1992***

PART 1 – PRELIMINARY

1. Citation

These Rules may be cited as the *University Facilities (Information and Communication Technology Network) Rules 2023*.

2. Commencement

These Rules commence on the date of approval by Council.

3. Repeal

The *University of Canberra University Facilities (Information and Communication Technology Network) Rules 2006* are revoked. All decisions made under those Rules are taken to have been made under these Rules.

4. Interpretation

(1) In these Rules, unless the contrary intention appears:

account means a computer account assigned to a user under rule 5;

affiliate means an individual who is not a staff member or a student of the University, but who has been granted access to the University's ICT Services by virtue of their relationship with the University.

child means a person under the age of 18 years;

Dean means an Executive Dean of a Faculty or a Dean of Graduate Research;

Director means the Director of an administrative service, research institute, or commercial unit of the University, not including a Portfolio;

Executive Employee means a Vice-Chancellor, Deputy Vice-Chancellor, Vice-President, Chief People Officer or the Chief Digital Officer;

Faculty means a faculty of the University headed by an Executive Dean;

general access laboratory means a room designated as such under rule 13 and may include adjacent space, such as corridors, toilets, storerooms, tea rooms and foyers used primarily to support or facilitate ICT Services in the University;

information means data held electronically in the ICT Services;

identity card means an identity card issued by the University to a member of staff, affiliate, or a student of the University;

ICT means Information Communications Technology;

ICT network means the University information and communication technology network, including University hardware, software and information as defined in these Rules, and all infrastructure linking University hardware and technology platforms. It includes wired, wireless, and other technologies used to deliver functions, access services, and link hardware and applications;

ICT Services means all the infrastructure that facilitates the ICT Network and includes:

(a) buildings and permanent installations;
(b) information services;
(c) fixtures, cabling and capital equipment;
(d) commercially procured managed services; and
(e) Software as a Service (SaaS) that hold, transmit, manage, use and analyse or access information, or carry communications;

Internet of Things (IoT) means a network of interrelated devices with sensors, processors, software, and other technologies that connect and exchange data with other devices and systems over the internet;

limited personal use means use of the ICT Services in accordance with the policy and guidelines on limited personal use;

member of staff means a member of the academic staff or the professional staff of the University;

personal hardware means computer and communications equipment, components, parts of components owned by a user, including, whether wired or wireless, remote and portable computers, tablets, mobile telephones, laptop computers, Internet of Things (IoT) devices, servers and the like owned or provided by the user and connected to the ICT Services.

Portfolio means a Portfolio of the University headed by an Executive Employee;

restricted area means a location designated as such under rule 12 and may include adjacent space, such as corridors, toilets, storerooms, tea rooms and foyers used primarily to support or facilitate ICT Services in the University;

Rights Holder means an owner or exclusive licensee of a relevant copyright under the *Copyright Act 1968 (Cth)*;

software means licensed software products and computer programs and includes any updates and new releases of products;

supervisor means a member of staff for the time being in charge of any area of the University described in these Rules as part of the ICT Services of the University;

University hardware means the computer and communications equipment, components, parts of components of the University including network access ports, whether wired or wireless, remote and portable computer and communications equipment such as mobile telephones, laptop computers, Internet of Things (IoT) devices, servers and the like owned or provided by the University;

URL means the Uniform Resource Locator of a website;

user means a person (wherever located) who accesses ICT Services.

(2) A reference in these Rules to a decision includes a reference to:
- (a) granting, refusing to grant, suspending or revoking a permission, or imposing terms or conditions; and
- (b) giving a direction; and
- (c) waiving or refusing to waive the whole or a part of a penalty; and
- (d) affirming, varying, setting aside or making a decision.

PART 2 – ACCESS TO AND USE OF THE INFORMATION AND COMMUNICATION TECHNOLOGY NETWORK

5. Authorised Access

(1) A person must not use ICT Services unless they are authorised by an Executive Employee.

(2) It is a condition of the authorisation referred to in subrule (1) that the user must comply with the conditions, and have regard to the policy and guidelines, on the use of and access to the University's ICT Services issued by an Executive Employee from time to time.

(3) Notwithstanding if a person uses their personal hardware or University hardware, a person commits a breach of these Rules if the person:

(a) uses ICT Services without authorisation; or

(b) obtains access to information without being authorised to do so; or

(c) uses another user's account except where the usage forms part of a maintenance or support job authorised by an Executive Employee; or

(d) uses, for purposes other than those identified in subrule (4), facilities which they are authorised to use; or

(e) uses or accesses ICT Services contrary to the conditions, policy and guidelines identified in subrule (2).

(4) Except for limited personal use, a person must use ICT Services for the purposes for which they are employed, being for the educational, research and administrative business of the University.

(5) A person who contravenes subrule (4) commits a breach of these Rules.

(6) Notwithstanding rules 14 and 15, the University may establish conditions for access and use of the ICT Services, including the imposition of charges or quotas.

(7) A user who exceeds a quota imposed by conditions established under subrule (6) must pay to the University a charge and, in relation to the amount to be recovered, rules 17, 18 and 22 shall apply as if the amount of the charge were a monetary penalty imposed under rule 17.

(8) An officer nominated by an Executive Employee may assign an account to a user to enable the user to access that part of the ICT Services for which the account is required.

6. Acceptable use

(1) A person who knowingly or recklessly uses any part of the ICT Services for private gain, or for a financial gain to a third party, commits a breach of these Rules unless authorised under the conditions, policy and guidelines issued under subrule 5(2).

(2) A user of ICT Services commits a breach of these Rules if they copy:

(a) the information of another user contained on ICT Services (without the consent of the other user); or

(b) any software contained on ICT Services (without the consent of the licensor of the software); or

(c) information belonging to the University which the user is not authorised to access; or

(d) information which infringes or facilitates the infringement of copyright material in breach of the *Copyright Act 1968 (Cth);* or

(e) information external to the University in breach of any licences held by the University providing for online access to that information by authorised users.

(3) A user of ICT Services, whether the ICT Service identifies the user or equipment as affiliated with the University or not, commits a breach of these Rules if they use ICT Services:

(a) in a manner that brings the University into disrepute; or

(b) to publish or send unsolicited emails, messages or other communications, except if the user is, by virtue of their role at the University, authorised by an Executive Employee to send communications of this type; or

(c) to send or communicate obscene, offensive, harassing or defamatory messages or material to another party whether at the University or at another place.

(4) A person who represents themselves as another person, whether fictional or not, commits a breach of these Rules if they use such misrepresentation to:

(a) obtain access to ICT Services or any part of it; or

(b) purport to be the author of any work or information on ICT Services; or

(c) send any email, messages, communication or information on ICT Services.

(5) A person commits a breach of these Rules if they wilfully or recklessly:

(a) damage any item, article, component or part of any ICT Services; or

(b) erases, deletes, alters, or damages any information on ICT Services, other than information in their own account or an account they are otherwise authorised to administer.

PART 3 – INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY

7. Passwords

(1) A person commits a breach of these Rules if:

(a) they are in possession of a username or password that in combination provides access to ICT Services; and

(b) they use the combination to obtain access without authorisation; or

(c) they disclose the combination to another person.

8. System Security

(1) A user must not do anything, or omit to do anything, that adversely affects the security of ICT Services.

(2) If a user obtains information on ICT Services to which the user is not authorised to have or becomes aware of a breach of security relating to ICT Services, the user must make a report in accordance with rule 25.

9. Access to facilities

(1) An Executive Employee may direct that an individual be granted access to physical ICT Services where necessary in the circumstances.

(2) If a person on University premises accesses ICT Services contrary to these Rules, an Executive Employee may direct the person to leave the premises.

10. Interfering or Subverting

(1) A user must not interfere with the operation of the ICT Services.

(2) A person who wilfully, negligently, or without authority or excuse:

(a) causes interference with the operation of all or part of ICT Services;

(b) attempts to subvert the security of any part of ICT Services;

(c) destroys, erases or alters information stored in, or inserts information into ICT Services or any part of the ICT Services; or

(d) interferes with, interrupts or obstructs the lawful use of a part of the ICT Services; or

(e) impedes or prevents access to, or impairs the usefulness or effectiveness of, data stored in the ICT Services or information stored on behalf of the University in hardware that is not a University computer;

commits a breach of these Rules.

(3) A person authorised by an Executive Employee may take immediate action to stop any equipment in the University found to be interfering with the operation, or subverting the security, of any part of the ICT Services from continuing to do so.

11. Power to Remove Material

(1) If an authorised officer of the University detects or is informed about the existence of files, articles or materials that contravene these Rules, any law or the policies or procedures of the University, an Executive Employee, acting reasonably, may authorise the quarantining and removal of the material from ICT Services.

The University will not be liable for any damage resulting from the quarantining or removal of material in accordance with subrule (1).

PART 4 – ROOMS AND LABORATORIES

12. Restricted Areas

(1) An Executive Employee may, by writing signed by the Executive Employee, designate an area to be a restricted area.

(2) Subject to subrule (3), no person is permitted to enter a restricted area, other than a member of staff authorised by the Executive Employee or a person who is invited to enter such a room by such a member of staff.

(3) The Executive Employee may grant permission to a person to enter a restricted area and may, at any time, suspend or revoke the permission.

(4) Permission under subrule (3) may be subject to such terms and conditions, if any, as the Executive Employee considers appropriate.

(5) A supervisor may direct any person, other than a member of staff or a person to whom permission has been granted under subrule (3), to leave a restricted area and may take such action as is reasonably necessary in all the circumstances to ensure compliance with any such direction.

(6) It is a breach of these Rules under these Rules for a person to fail to comply with a direction given under subrule (5).

13. General Access Laboratories

An Executive Employee may, in writing Executive Employee, designate a room to be a general access laboratory.

14. Powers of an Executive Employee in relation to restricted areas and general access laboratories

(1) An Executive Employee may, in writing:

(a) determine the general terms and conditions under which, and the procedures by which, users may:

i. operate or use any equipment in, or any services of, restricted areas and general access laboratories; or

ii. borrow any equipment or other item from the restricted areas and general access laboratories; or

iii. have access to a restricted area or general access laboratory; and

(b) vary any terms, conditions or procedures determined under paragraph (a); and

(c) determine, from time to time, the days on which, and the hours during which, the restricted areas and general access laboratories, are to remain open or be closed; and

(d) determine, from time to time, the days on which, and the hours during which, any specified equipment in, or services of, the restricted areas and general access laboratories are to be available for operation or use; and

(e) determine, from time to time, any charges applying for access to restricted areas and general access laboratories.

(2) It is a breach of these Rules for a person to, without the permission of a supervisor, act in contravention of any terms, conditions or procedures determined by an Executive Employee under (1).

(3) It is a breach of these Rules for a person to allow a child, other than a child who is a student of the University or a member of staff, to enter or remain in any room or other area covered by a determination made under (1) except:

(a) with the permission of a supervisor, and

(b) under the control of an adult at all times. a breach of these Rules

(4) Where an Executive Employee is satisfied that a person has committed a breach of a provision of rule 14, an Executive Employee may direct that person to leave the restricted areas and general access laboratories for such period, not exceeding 24 hours, as the Executive Employee determines.

(5) A person directed to leave the restricted areas and general access laboratories under subrule (4) must not re-enter the restricted areas and general access laboratories until the expiration of the period determined under that subrule.

(6) The Executive Employee may take such action as is reasonably necessary in all the circumstances to give effect to a decision made by the Executive Employee under this rule 14.

15. Powers of the Supervisor in relation to restricted areas and general access laboratories

(1) The supervisor may require any person in a restricted area or general access laboratory to produce evidence of their entitlement:

(a) to operate or use any equipment in, or any services of, restricted areas and general access laboratories; or

(b) to borrow equipment or other items from restricted areas and general access laboratories; or

(c) to have access to restricted areas and general access laboratories.

(2) If a person fails to comply with a requirement under subrule (1), the supervisor may direct that person to leave the restricted areas and general access laboratories until such time as the person produces evidence of their entitlement.

(3) Except for the purposes of producing evidence of their entitlement to access restricted areas and general access laboratories, a person who has been given a direction in accordance with (2) must not re-enter the restricted areas and general access laboratories until they have produced evidence of such entitlement.

(4) The supervisor may, if the supervisor considers it appropriate to do so, on such terms and conditions as are, from time to time, determined by an Executive Employee, grant permission to any person to:

(a) display or distribute any notice or pamphlet in the restricted areas and general access laboratories; or

(b) organise or take part in a gathering in the restricted areas and general access laboratories; or

(c) organise, mount or attend an exhibition in the restricted areas and general access laboratories; or

(d) remove from the restricted areas and general access laboratories any equipment or other item held in the restricted areas and general access laboratories that is not available for borrowing by that person; or

(e) operate or use any equipment in, or services of, the restricted areas and general access laboratories otherwise than in accordance with normal operating or using procedures of the restricted areas and general access laboratories as determined under rule 14; or

(f) remove any equipment or other item from the restricted areas and general access laboratories otherwise than in accordance with the normal borrowing procedures of the restricted areas and general access laboratories as determined under rule 14; or

(g) have access to restricted areas and general access laboratories otherwise than in accordance with the access terms, conditions and procedures as determined under rule 14; and may, in like manner, suspend or revoke a permission so granted.

(5) The supervisor may take such action as is reasonably necessary in all the circumstances for the purpose of carrying out a decision made under this rule 15.

(6) It is a breach of these Rules under these Rules for a person to fail to comply with a direction given under this rule 15.

PART 5 – PENALTIES

16. Offences

(1) A person who:

(a) commits a breach of these Rules; or

(b) repeats a breach of these Rules; or

(c) otherwise contravenes a provision of these Rules;

is liable to a penalty set out in rule 17.

17. Penalties

(1) Subject to rule 18, if an Executive Employee finds that a person has committed a breach of these Rules, the Executive Employee may, in relation to the offence:

(a) decide to take no action;

(b) reprimand the person committing the offence;

(c) with the consent of the Vice-Chancellor, and, where the person is a staff member, in consultation with the Chief People Officer:

i suspend the person from the use of all or part of ICT Services under their management;

ii close the relevant account;

(d) refer the matter to:

i if the person is a student of the University – a Prescribed Authority under the *University of Canberra (Student Conduct) Rules 2023*;

ii if the person is a member of staff – the person authorised to investigate staff misconduct matters under the Enterprise Agreement;

iii if the person is an affiliate – in accordance with the terms and conditions of the relevant agreement, policy or guideline that established the affiliation;

(e) determine the conditions under which the person may have access to the ICT network;

(f) determine compensation payable by the person to the University for damage to the ICT Services; or

(g) determine compensation payable by the person to the University for the failure to return University hardware or software by the date determined under rule 14(1); or

(h) take any action, being a combination of the actions specified in paragraphs (b) to (h) (inclusive).

(2) If the Executive Employee determines in accordance with subrule (1) that compensation is payable by a person, the person must pay to the University such amount as the Vice-Chancellor determines not exceeding:

(a) the lesser of:

i an amount equivalent to the cost of the repair of the damage; and

ii $5,000; or

(b) if the damage is irreparable or an item borrowed under the conditions determined under rule 16(1) is not returned by the specified date – the lesser of:

iii an amount equivalent to the cost (including any reasonable administrative cost) of replacing the item or article or part of the ICT Service, as the case may be; and

iv $5,000.

(3) Nothing in subrule (2) prevents the University from recovering, in a court of competent jurisdiction, that part of:

(a) the amount of the cost of the repair of the damage caused by a person; or

(b) the amount equivalent to the cost (including any reasonable administrative cost) of replacing the item or article or part of the ICT Services damaged by the person (as the case requires) that exceeds $5,000.

(4) The Vice-Chancellor may, in relation to a breach of these Rules for which the sole penalty is a monetary penalty:

(a) waive or reduce the monetary penalty payable for the offence; or

(b) extend the time for the payment of the monetary penalty.

(5) If a person becomes liable to pay to the University a monetary penalty or other amount under this rule, the person must pay to the University the amount specified in the notice given under subrule 18(3) in relation to the matter no later than 1 month after:

(a) if an appeal is not lodged under rule 22 in relation to the finding giving rise to the liability – the date of the notice; or

(b) if an appeal is lodged under rule 22 in relation to the finding giving rise to the liability – the day on which the decision is given in respect of the appeal.

(6) A person who is liable to pay to the University a monetary penalty or other amount under this rule, is not entitled to use the ICT Services, unless otherwise authorised in writing by the Executive Employee if the amount remains unpaid after the time referred to in subrule (5) has expired.

(7) A determination made under this rule 19 must be in writing and must be given to the person in relation to whom it is made.

18. Imposition of Penalties

(1) If it appears to an Executive Employee that a person is in breach of these Rules, the Executive Employee, acting with the agreement of the Vice-Chancellor, may immediately suspend the person from the ICT Services for an initial period not exceeding 28 days.

(2) A suspension under subrule (1) takes effect as soon as written notice of it is given or delivered to the person suspended.

(3) A penalty (other than a suspension referred to in subrule (1)) must not be imposed on a person unless:

(a) the person is given written notice of:
  i the breach that is alleged to have been committed by the person; and
  ii the penalty that is proposed to be imposed for the alleged breach in addition to any suspension under subrule (1); and
(b) the notice is accompanied by a copy of this rule and of rule 22; and
(c) a period of not less than 7 days, or any shorter period that is agreed to by the person, has elapsed since the giving of the notice; and
(d) any written representations made, during the period referred to in paragraph (c), by the person to the Executive Employee about the alleged offence or the proposed penalty, or both of them, have been taken into account; and
(e) in the case of a person who appeals against a finding or penalty under rule 22 – the decision of the Appeals Committee is given to the appellant and the Executive Employee under subrule 22(13).

PART 6 – APPEALS AND REVIEWS

19. Review of Decisions of Supervisor

(1) Where a person is dissatisfied with a decision of a Supervisor made in the exercise of a power conferred on the Supervisor under these Rules, the person may apply in writing to the Executive Employee for review of the decision.

(2) An application for review of a decision will be limited to the grounds that, when making their decision, the Supervisor:

(a) did not take all relevant material or circumstances into account; or
(b) took irrelevant material or circumstances into account; or
(c) demonstrated bias that disadvantaged the person in the making of the decision.

(3) The Executive Employee must, as soon as practicable after receiving an application under subrule (1), review the decision in such manner as the Executive Employee considers appropriate and may, having regard to all of the circumstances of the case and all the material provided by both parties:

(a) affirm, vary or set aside the decision under review; or
(b) set aside the decision under review and make a decision in substitution for that decision.

20. Review of decisions of an Executive Employee

Where a person is dissatisfied with a decision of an Executive Employee made in the exercise of a power conferred on an Executive Employee under these Rules, the person may make a complaint about the decision following a relevant process, being:

(a) if the person is a member of staff of the University, through the complaint procedures set out in the University's Enterprise Agreement; or
(b) if the person is a student of the University, through the *Student Grievance Resolution Policy*.

PART 7 – MISCELLANEOUS

21. Personal Information

The University collects or receives personal information of users. In the course of managing the operation and use of the ICT Services the University is authorised to use that information in connection with efforts to ensure that its use and that of other users complies with all relevant legislation and University policy and guidelines.

22. Monitoring and Logging Access and Use and Content

(1) The University monitors and records all access to and contents of the ICT Services and retains such records. The University may use such records and information in accordance with the provisions of these Rules.

(2) The monitoring and recording includes but is not restricted to:

(a) URLs of sites visited the date and time they are visited and the duration of site visits. Network addresses accessing URLs (including caches) and the URL address are recorded and may be correlated;
(b) email messages transmitted by or to a University registered email account, including the date and time the message was transmitted, received and opened and the e-mail address of the sender and recipients;
(c) use of the ICT servers, facilities and services, both by access timestamp and originating network addresses and may correlate user access to particular addresses;
(d) access to secured rooms and buildings by identity card, logins to all applications, services, servers, systems and platforms;
(e) telephone numbers and contact details of all calls made using ICT Services;

(f) software and systems usage data, and reports relating to use of ICT infrastructure;
(g) all network data including date, time, source, origin, destination and content.

23. Reporting Breaches

(1) If, in connection with the use of the ICT Network or ICT Services, a person has knowledge of an actual or suspected breach of a law of the Commonwealth or Australian Capital Territory, or this Rule, a person must report the breach to an Executive Employee.

(2) Executive Employees must treat all reports made under (1) confidentially and must refer the matter to an appropriate University authority for investigation.

(3) Where the matter requires a referral to an external agency, including ACT Policing, the Executive Employee must consult with the Vice-Chancellor, who will make the referral.

(4) The University will protect the interests of any member of staff or student reporting a suspected breach in good faith and in a responsible way.

24. Notices

(1) For the purpose of these Rules, a notice or communication that is hand-delivered or sent by electronic or printed post to a person at a place shown in the records of the University as the person's:

(a) semester address; or
(b) work address; or
(c) permanent home address; or
(d) e-mail address

is regarded as having been given to the person on the date on which the notice was hand-delivered or, if it is sent by post, on the date on which it would, in the ordinary course of post, have been delivered to the person.

25. Application of Regulation of *University of Canberra (Student Conduct) Rules 2023, the Charter of Conduct and Values and the University of Canberra Enterprise as in force and amended from time to time.*

Nothing in the Rules excludes the operation of the provisions of the *University of Canberra (Student Conduct) Rules 2023*, the Charter of Conduct and Values, and the University of Canberra Enterprise Agreement in relation to a breach of these Rules.

Made by Council on 15 March 2024.