Acceptable Use of Digital Services Policy

Section 1 - Purpose and Context

(1) Western Sydney University (University) provides Digital Services to enable and support University activities. The University must protect its Digital Services and meet legal obligations, and the University will take steps to prevent and disallow inappropriate use of Digital Services.

(2) This policy outlines what the University considers to be acceptable and appropriate use of Digital Services. The policy also sets out the responsibilities of all Authorised Users to access the University's Digital Services, and describes penalties for policy breaches.

Application and Compliance

(3) This policy applies to all current students, staff, contractors, consultants, and visitors who have access to any Digital Service.

Section 2 - Definitions

(4) Words and terms used in this policy are defined in Section 6 - Terms and Acronyms.

Section 3 - Policy Statement

(5) The University grants access to its Digital Services to Authorised Users, for the purpose of pursuing and advancing its business and educational goals.

(6) The University requires that all Authorised Users are aware of what conduct is expected of them in making use of University Digital Services, and provides information and guidance (including this policy) to aid Users in determining its expectations [Ref. ISO 27002 section 5.1]. Refer to Student Misconduct Rule or the Code of Conduct policies.

(7) University Digital Services are and remain the property of the University. This includes named email accounts that are provided to Authorised Users for use with their study, research or work.

(8) The University is committed to allowing its Authorised Users to make incidental personal use of its Digital Services, provided such use is legal, and does not breach University policies. Credentials are not to be shared or used for non-University services.

(9) If an Authorised User breaches the terms of this policy, their access may be restricted or revoked. Any breaches of this policy will be reported to the relevant University or regulatory authority or the police to take appropriate action, depending on the nature and seriousness of the breach.

Section 4 - Procedures

Policy Breaches and Penalties

(10) All Authorised Users should report breaches of this policy to the CIDO (or nominee), immediately. Breach reports will be treated confidentially. Any investigations of alleged breaches will be conducted as defined in the Workplace Surveillance Policy or the Student Misconduct Rule.

(11) The CIDO (or nominee) may temporarily deny or restrict access to Digital Services, including email, in order to:

a. prevent policy or legal breaches,
b. launch an Investigation of any potential breaches (as defined in the Workplace Surveillance Policy), or
c. mitigate threats or risks to the University or its Digital Services.

(12) If an Authorised User breaches this policy, intentionally or inadvertently, the CIDO (or nominee) will decide what actions should be taken, which may include:

a. the User will lose access to some or all Digital Services (for a period of time or completely, depending on the nature of the breach);
b. the User's activities are treated as a breach of policy and referred for action under the Student Misconduct Rule, the Code of Conduct or the disciplinary processes of the relevant staff agreement; and/or
c. the User's activities should be referred to the relevant external authority (e.g. the State or Federal Police, or the ICAC) for investigation of illegal or unlawful activities.

Access to and Use of IT Resources

(13) Only Authorised Users may access or use Digital Services for purposes related to their relationship with the University.

(14) The University participates in Eduroam. Users of Eduroam must abide by the policies of their home and visited organisations. Other organisations' access policies may be more restrictive than Western Sydney University's policies.

(15) Accessing University Digital Services (internally or remotely) as an affiliate or associate requires an application approved by the manager from the University business unit, school, or research centre who is sponsoring the affiliate.

(16) When Authorised Users leave the University, their User accounts — including documents, email and internet access (and records of access) — are archived and retired. This means that ex-staff and -students will not have access to their user accounts or emails after leaving. Therefore, before leaving the University, users are responsible for:

a. tidying their own documents and mailboxes;
b. ensuring their managers or teams have the necessary information to safeguard business operations;
c. making copies of any personal information that they will require;
d. contacting any internal or external correspondents to make them aware that the University email address will be retired (see the Staff Separation Checklist or ServiceNow Knowledge Article 0012730 – Staff Off-Boarding for more details); and
e. ensuring University Intellectual Property remains with the University. While copies of personal data are acceptable, University business remains university property; no departing Authorised User is permitted to take any University Digital Information. See the Intellectual Property Policy for more information.

Termination of Access

(17) Staff access will be terminated after their employment is ended. Student email accounts are archived and retired after they have graduated or otherwise ceased their study with the University. Affiliate or Associate access will be terminated at the end of the approval period or contract/term of the appointment.

(18) After access is terminated, the University will only consider requests for creating a data extract for email or consolidated document retrieval if the request relates to:

a. a legal or investigative matter, as determined by the Office of General Counsel, a valid external authority (such as the State or Federal Police, or the ICAC, or an authorised investigator) or
b. an internal business requirement, once a compelling, legitimate business reason is supplied by the requester and approved by the CIDO (or nominee).

Authorised Users' Responsibilities

(19) All Authorised Users are responsible for:

a. complying with this and all other University policies;
b. in the use of Digital Services, treating others with respect, civility and maturity (refer to the Code of Conduct and the Student Misconduct Rule);
c. choosing a strong password for their user account and changing it periodically (as defined in the Digital Information Security Policy);
d. ensuring that all relevant University policies are followed when using personal devices with University Digital Services and network infrastructure. Refer to Clause 21 for additional information;
e. not providing their password to anyone, including other Users, supervisors, managers, or ITDS support staff;
f. not asking other Users for their password(s);
g. not accessing or attempting to access programs or data stored under another person's Credentials, without permission from that Authorised User and the CIDO (or nominee).
h. keeping their Credentials secure; not displaying an Authorised User account password where others can see it or easily find it. Account Credentials are effectively an Authorised User's digital identity. Email or documents sent under an Authorised User's account credentials will be traced back to them. [Ref. ISO 27002 9.2.4]
i. not attempting to undermine the confidentiality, integrity, or availability of University Digital Services without appropriate approval (such as study or job requirements). Actions that fall under this definition include: [Ref. ISO 27002 section 9; Higher Education Standards Framework (Threshold Standards) 2021 section 7.3.3b]]
    i. preventing or attempting to prevent Authorised Users’ access to Digital Services;
    ii. intentionally or negligently degrading performance;
    iii. examining, copying, renaming, changing, or deleting programs, files, data, messages, or information belonging to the University or any other Authorised User;
    iv. modifying, uninstalling or disabling any software or hardware;
    v. altering any restrictions associated with any University computer system, computer account, network system, personal computer software protection or other of the University's Digital Services;
    vi. running network wide security assessment tools without permission from the area supervisor and ITDS;
    vii. utilising cloud storage solutions for University digital information that have not been approved by ITDS; and
    viii. removing any University Digital Services from University premises without authorisation.
j. ensuring that Clause 19(h) is complied with unless the Authorised User has requested and received an exemption, documenting where the intended use is in support of university business, learning, teaching or research.

k. not attempting to access any Digital Services remotely, except through channels provided, authorised, and supported by Information Technology and Digital Services. See the Digital Information Security Policy for more information.
l. not using University Digital Services for private commercial enterprises or personal gain. This includes, but is not limited to, gambling, trading, and/or soliciting.
m. not using University Digital Services to excess for personal reasons (e.g., playing games on library or lab computers).

(20) Authorised Users must not access or use University Digital Services in ways that:

a. are likely to disrupt the authorised use of Digital Services by other Authorised Users;
b. could disrupt the University's business and operations;
c. contravene University rules, policies, procedures and/or guidelines;
d. are unlawful or illegal;
e. may diminish the University's image and reputation;
f. use, disclose or expose personal information about staff and/or students without approval;
g. may threaten, bully, harass, vilify, unlawfully discriminate, or perform any other action that University considers to be unacceptable or unlawful behaviour (see the University's Discrimination, Harassment, Vilification and Victimisation Prevention Policy and Bullying Prevention Policy for more information);
h. may be defamatory or libellous;
i. distribute or access material that the University considers unacceptable or offensive. This includes, but is not limited to, malicious, pornographic, gambling, or terrorist material. Authorised Users requiring access to unacceptable or offensive content for research or study should request a specific exemption for access to be permitted;
j. attempt to gain unauthorised access to other systems, data, or Digital Services, either internal or external to the University [Ref. Cybercrime Act, schedule 1]; or
k. promotes, instructs, or incites any of the above.

BYOD — Bring Your Own Device

(21) When using BYOD, Authorised Users must take all reasonable steps to: [Ref. ISO 27002 sections 9.3, 9.4]

a. prevent the theft or loss of University Digital Information;
b. keep information confidential where appropriate;
c. not hold any University Digital Information that is Confidential and Sensitive on a BYOD device;
d. delete any University business information from any personal devices immediately after it is no longer required. This includes information contained within emails;
e. ensure that relevant information is copied back onto University systems and manage any potential data integrity issues with existing information;
f. report the loss of any device containing University data (including stored or saved email) to the IT Service Desk;
g. advise the University if the device is lost or stolen. Be aware that if the University is advised that the device is lost or stolen, the University may wipe messages, by remote action, from the device. The University is not responsible if unrelated or personal information is lost in this process;
h. remove all data belonging to the University on any BYOD devices before leaving the University; and
i. be aware of any data protection issues and ensure Confidential and Sensitive University Digital Information is handled appropriately (see the Privacy Policy for more information).

Security of Data and Systems

(22) All Authorised Users are responsible for the security, privacy and confidentiality of University data held or transmitted under their Credentials. This includes the secure storage of data for which Users are responsible. Please refer to the Privacy Policy, and Privacy Management Plan documents. [Ref. ISO 27002 section 7.2]

(23) Authorised Users are responsible for security and appropriate use of all systems that are accessed under their Credentials, including BYOD devices. Authorised Users are expected to report any breach in digital security to the IT Service Desk. [Ref. ISO 27002 section 7.2.1]

(24) To protect University data and databases, direct access to data in databases using interactive tools (such as Toad or Excel ODBC links) is restricted. Authorised Users must only store data collected using these tools on University Digital Services designated for the data's ongoing processing. Users are not permitted to store such extracted data on BYOD machines or any personal external device or media. [Ref. ISM Control 1083; ACSC Essential 8]

(25) The University uses spam and phishing detection software, URL blocking controls and other methods for minimising risk to Digital Services [Ref. Higher Education Standard Framework section 6.2.1e]. See the Cyber Security Policy for more detail.

(26) When responding to requests for assistance with Digital Services from Authorised Users, Service Desk personnel can make use of software that allows them to control another computer or device remotely. Staff may only attempt remote control access with the Authorised User's permission, and only in the performance of duties directly related to their work.

Monitoring

(27) Monitoring of computers, and activities performed on those computers, is performed as a part of routine IT practices by ITDS. See the Workplace Surveillance Policy for more details.

(28) University Digital Services and data (including email) remains the property of the University. The University reviews and monitors its Digital Services (including email) to ensure proper functioning. The University reserves its right to recover or otherwise protect that data (including by deletion) at all times (Refer to the Email and Internet Policy for details).

(29) The University reserves its right to monitor messages and materials accessed, sent or received over its network to check that the security measures have not been undermined or that University Digital Services are not being abused. The University is committed to responding promptly to any potentially damaging publication by any action deemed necessary, including withdrawing its service from Users and removing any unacceptable materials. (Refer to the Email and Internet Policy for details about website blocking).

Section 5 - Guidelines

(30) The University recommends the following measures for best practice when using Digital Services:

a. Workstations should be locked or logged off when not in use.
b. Labels on any University Digital Services should not be removed, defaced, or modified.
c. Staff should undertake training in the use of Digital Services (such as email or Microsoft Office use) via Staff Online.
d. All Authorised Users are advised to be wary of using Digital Services in ways that cause a breach of copyright. See the Copyright Policy for more information.
e. Any University Records created, altered, received, or maintained with or on Digital Services are required to be

archived with the University's Records and Archives Management Systems, unless an alternative computerised system has been classified by the University as a System of Record. See the Records and Archives Management Policy for more information.

f. University data (or data relevant to Authorised Users' role with the University) should be stored on approved University storage, such as the 'My Documents' folder on a Standard Operating Environment (SOE) computer (which is not the local hard drive).

(31) The University recommends the following measures for using BYOD equipment:

a. Devices should be screen locked when not in use.
b. Devices should have up-to-date antivirus protection.
c. Devices should have up-to-date operating systems.
d. All Authorised Users should enable and use appropriate security measures (such as a passphrase or PIN) on the device.
e. All Authorised Users should save and back up their work. The University accepts no responsibility for lost data on any BYOD equipment.

Reference Information

(32) This policy is to be read in conjunction with the following University documents:

a. Email and Internet Policy,
b. Cyber Security Policy,
c. Digital Information Security Policy,
d. Bullying Prevention Policy,
e. Intellectual Property Policy,
f. Discrimination, Harassment, Vilification and Victimisation Prevention Policy,
g. Student Misconduct Rule,
h. Code of Conduct,
i. Copyright Policy,
j. Records and Archive Management Policy,
k. Privacy Policy,
l. Workplace Surveillance Policy, and
m. Staff Separation Checklist or ServiceNow Knowledge Article KB0012730.

(33) This policy makes reference to the Australian Signals Directorate's Information Security Manual and related Essential 8 controls.

(34) This policy makes reference to Australian Standard AS/NZS ISO/IEC 27002, which can be accessed under "Standards On-line Premium (SAI Global)" via the alphabetical listing in the e-Resources section of the University Library.

Section 6 - Terms and Acronyms

(35) The following definitions apply for the purpose of this policy:

a. Affiliate Users include (but are not limited to):
    i. Board of Trustees' members and members of Board Executive Committee;

ii. Visiting fellows, and research associates;
iii. External (non-profit) community groups needing temporary access
iv. Third parties, vendors, and contractors engaged in the provisioning of service or services on behalf of the University; and
v. Official affiliation/associations of Western Sydney University

b. Authorised User: a person who is a currently enrolled or attending student, a current employee, or a formal supplier, joint venture partner, affiliate or associate of the University who is granted access and provided with authentication Credentials by the University. Eduroam Users are also Authorised Users.
c. BYOD (bring your own device): the ability for staff or students to use non-University equipment (such as laptops, smart phones, tablets and similar devices) to connect to the University's network.
d. CIDO: Chief Information and Digital Officer
e. Confidential and Sensitive Material: any information or material that a person knows or ought reasonably to know is confidential or sensitive, including but not limited to:
i. The Personal Information of staff or students
ii. Student, staff or research subject health information
iii. Unpublicised strategic, legal, financial, or research information
iv. Any data that could compromise any facet of the University, including reputation
f. Credentials: constituted by a username and password, and used to access University Digital Services.
g. Digital Services: synonymous with IT Resources; all services (e.g., data, voice, video) delivered through electronic means. This includes the capture, storage, retrieval, transfer, communication and/or dissemination of information electronically and the technologies used in support of these activities. Such technologies encompass systems, software, hardware, communications and network facilities. The method of delivery may be hosted within University IT facilities, externally or a combination. They may be paid or free, subscribed or purchased, provided through a cloud or as a managed service.
h. Eduroam: An educational roaming internet service offered by multiple organisations worldwide, including Western Sydney University. This provides University staff and students access to internet through Eduroam when at another member's campus/facility.
i. Eduroam user: a person granted Eduroam access and credentials by an Eduroam organisation (such as Western Sydney University). Eduroam users are Authorised Users and granted access to the University's internet.
j. ICAC: the Independent Commission Against Corruption
k. Incidental personal use: the utilisation of Digital Services for personal reasons (e.g. checking or sending email that is not related to study or work; utilising the internet for personal reasons). Incidental, by the nature of the word, does not include extended or continuous use.
l. ITDS: Information Technology and Digital Services
m. IT Resources: refer to Digital Services.
n. IT Service Desk: a team within ITDS, established to be the first point of call for staff and students, for all IT matters.
o. Monitoring: a form of Surveillance; the collection or storage of information, or the creation of records, in a routine and passive manner; the routine review of the information or the routinely collected records to ensure the integrity, security and service delivery of the University’s Digital Services. Monitoring does not involve actively investigating or keeping track of an individual or their activities. Monitoring is conducted as permitted by the Workplace Surveillance Policy.
p. Remote Desktop Software: an application, protocol, or other software solution that allows a computer or similar device to connect to the University's hardware or network without being on-site. This does not include the University's Wi-Fi network.
q. System of Record: a University Digital Service that has been reviewed and serves the purpose of record keeping requirements as defined in the Records and Archives Management Policy.

r. University digital information: any data stored electronically, or used by, or on behalf of the University in the conduct of its teaching, research, or business. University information is the property of the University. See the Intellectual Property Policy for more information.

s. University email: the official email service the University provides to staff and students, including the content of emails, electronic attachments to emails and transactional information associated with such communications. University email is a Digital Service and is the property of the University. University emails are emails sent or received using a University email account.

t. University Records: are any records made or received, and kept, by any person in the course of the exercise of official functions in the University, or for any purpose of the University, or for the use of the University (State Records Act 1998 (NSW)), and include records in any format such as paper, electronic (email, spreadsheets, word processing documents, images, etc), audio or video (cassettes, recordings or files), film, photographs (printed or digital), publications and microfilm/fiche. [Ref. Records and Archives Management Policy].

Status and Details

Status	Current
Effective Date	20th December 2019
Review Date	3rd January 2022
Approval Authority	Vice-Chancellor and President
Approval Date	20th December 2019
Expiry Date	Not Applicable
Unit Head	Scott Snyder Chief Information and Digital Officer s.snyder@westernsydney.edu.au
Author	Anita King 45701708
Enquiries Contact	Anita King IT Assurance Specialist 45701708