



Acceptable Use of IT

Policy UP19/1

Approver	Senate
Sponsor	Deputy Vice-Chancellor (Operations)
Owner	Chief Information Officer
Secretary	Corporate Secretary
Policy Type	Institutional
Policy Category	Operations and Support Services

1 Purpose

- 1.1 The purpose of this Policy is to —
- (a) Outline acceptable and prohibited uses of University Digital Resources in order to —
 - i. safeguard the reputation of the University by encouraging responsible online behaviour;
 - ii. protect the UWA Digital Identity of members of the University Community; and
 - iii. safeguard University Information, IT Services and IT Assets.
 - (b) contribute to maintaining a University culture of integrity.
- 1.2 This Policy is to be read in conjunction with the following —
- (a) Information Protection Policy;
 - (b) Information Retention Policy;
 - (c) Information Privacy Policy; and
 - (d) The Codes of Ethics and Codes of Conduct.

2 Definitions

Term	Definition
Cyber Security	The protection of the confidentiality, integrity and availability of Digital Resources. Cyber Security focuses on the technical aspects of safeguarding University Information, forming an integral part of Information Protection.
Digital Identity	Information, such as user account, password or an email address, used by computer systems to represent a member of the University Community.
Digital Resources	Any IT Service, IT Asset, Digital Identity or digital Information of UWA.
IT Assets	Any tangible thing, belonging to, or contracted to the University, which is worth protecting and used to access, process, store or transmit data.
IT Services	The combination of processes, expertise and resources by which University IT deliver value to the University Community to enable the achievement of their business objectives.
Personal Device	A non-University owned and/or provided device that is used to access IT Services or University Information. This includes, but not limited to, smartphones, tablets or equivalent devices, laptop and desktop computers, Internet of Things devices, radio communication devices, peripheral devices and portable storage devices.
Personal Use	Use of Digital Resources that is not for the purposes of University Activity. That is studying and/or working at the University, and/or taking part in recreation or other activities organised by the Guild and/or University; and/or any services and/or performance of official duties of the University, regardless of location.

Term	Definition
Policy	An approved instrument registered on the UWA Policy Library that expresses principles to regulate behaviour and practice.
Regulated Digital Content	Material, including but not limited to — (1). in breach of intellectual property or copyright; (2). malware; (3). unauthorised software; (4). in violation of academic integrity requirements; (5). unlawfully obtained; (6). containing child exploitation material; (7). advocates for a terrorist act; (8). detailed instruction or promotion in crime or violence; (9). instruction in paedophilic activity; (10). gratuitous, exploitative and offensive depictions of violence or sexual violence; (11). has been classified RC or X 18+ by the Classification Board.
Third Party	Any individual other than a Student or Employee, or any organisation that is not part of the University Group or affiliated bodies.
University	Is The University of Western Australia, and any and all subsidiary or associated entities.
University Activity	Studying and/or working at the University, and/or taking part in recreation or other activities organised by the Guild and/or University; and/or any services and/or performance of official duties of the University, regardless of location.
University Community	All individuals who engage in University activity and/or use University property.
University Officer	Any of the following — (1). Senate Members and members of committees of the Senate (2). Employees (3). Clinical Academics (4). Contractors (5). Honorary, Adjunct, Clinical (excluding Clinical Academics) or Emeritus Appointments (6). Committee Members (7). individuals acting in the name of the University on a Financial Commitment.
University Property	Tangible and non-tangible things, belonging to, or contracted to the University or members of the University Community, including campuses, facilities and services.

3 Scope

- 3.1 The scope of this Policy applies to –
- (a) the entire University; and
 - (b) Controlled Entities and affiliated and partner organisations when utilising University Digital Resources.
- 3.2 This Policy applies to the entire University Community, including students, staff, associates, visitors, third parties and automated agents acting on behalf of the University Community or IT Assets, when handling University Digital Resources.

4 Acceptable Use of IT Practices

- 4.1 Members of the University Community must only use University Digital Resources for acceptable, legal and ethical purposes.
- 4.2 The University provides Digital Resources to enable teaching, learning, research and administration, including approved University Consultancy as defined in the Consultancy Policy.

- 4.3 Limited Personal Use is acceptable provided it does not:
- (a) Interfere with the operation of these resources,
 - (b) Incur additional costs for the University, or
 - (c) Serve private commercial purposes and personal financial gain.
- 4.4 University Officers must complete Cyber Security induction training provided by the University as soon as practical after receiving access to their UWA Digital Identity, as well as annual refresher training and any additional training as directed. The training program may include targeted phishing simulations to strengthen the cyber resilience of the University Community.
- 4.5 Members of the University Community must not bypass or tamper with security measures or jeopardise, access, copy, alter or destroy Digital Resources if they are not specifically authorised to do so.
- 4.6 Members of the University Community must not create, access, download, possess or distribute digital content that is —
- (a) illegal;
 - (b) considered as any form of harassment or discrimination, or otherwise interferes with the principles of the University's Code of Ethics and Code of Conduct; or
 - (c) considered as Regulated Digital Content.
- 4.7 The University may grant access to Regulated Digital Content to support valid research and teaching purposes upon written approval of the DVCR or their delegate.
- 4.8 To the extent allowed by law, the University accepts no responsibility for loss or damage, or consequential loss or damage, arising from the use of its Digital Resources, or for users whose actions breach legislation or University Policy.

5 Safeguarding Devices

- 5.1 The University Community must take all reasonable steps to protect University Digital Resources whenever undertaking University Activity using University-owned or personal devices, on University Property or remotely.
- 5.2 Personal Devices may be used to —
- (a) connect to University Wi-Fi networks; or
 - (b) remotely access University Information or IT Services via VPN.
- 5.3 Personal Devices must not be connected to wired network ports on University Property without authorisation by University IT.
- 5.4 Personal Devices used to access University Information or consume IT Services must be kept up-to-date, securely configured and free of known security vulnerabilities.
- 5.5 The University may refuse to provide IT Services to devices that do not comply with security requirements.
- 5.6 The University Community must return University-issued IT assets (e.g., laptops, phones, peripherals and other equipment) when their employment, enrolment or engagement with the University ends, or when otherwise directed by the University.

6 Safeguarding Access

- 6.1 Members of the University Community must keep their access credential, such as passwords and multi-factor authentication (MFA) codes, confidential and must not share with anyone.

- 6.2 Members of the University Community are responsible for all activities originating from their UWA Digital Identities, unless the account has been compromised, and the incident is promptly reported to the University IT Service Desk.
- 6.3 Access to University Digital Resources is granted in line with the principle of least privilege, i.e. providing the minimum levels of access required to perform agreed University Activity.
- 6.4 Third Parties authorised to access University Digital Resources must agree to comply with this Policy.
- 6.5 University Officers authorising Third Party access are accountable for ensuring that the Third Party is provided with the minimum levels of access required to perform agreed University Activity.
- 6.6 University Officers authorising Third Party access are accountable for the timely revocation of Third Party access and return of University-provided IT Assets to University IT when no longer required.
- 6.7 The University regards communications conveyed by UWA Digital Identities to be University Information.
- 6.8 The University may monitor, log, examine or disclose activity performed by UWA Digital Identities or related to University Digital Resources for security, operational and compliance purposes.
- 6.9 Members of the University Community making Personal Use of University Digital Resources accept that it may be subject to such monitoring and analysis.
- 6.10 The University may suspend any UWA Digital Identity or access to University Digital Resources upon breaching Policies.

7 Reporting of Incidents and Inappropriate Use

- 7.1 Members of the University Community who identify or suspect any unacceptable use or other breach of this Policy must report it as soon as possible, by —
 - (a) contacting the University IT Service Desk; or
 - (b) submitting an anonymous report in accordance with the Public Complaints Policy.

8 Non-Compliance

- 8.1 Breaches of requirements or negligence in the performance of responsibilities set out by the Policy may be considered as Misconduct and addressed through formal Misconduct Process.

Legislative Context

Relevant Legislation or Regulations
<i>University of Western Australia Act 1911 (WA)</i>
<i>University of Western Australia Statute (2020)</i>

End