Acceptable Use of IT Policy

Policy Number	UP19/1	**Steward**	Chief Information Officer
Approval Date	22 November 2022	**Administrator(s)**	AD Cyber Security and Technology Risk
Assessment Date	22 November 2025	**TRIM File**	F19/523
Approver	Vice-Chancellor		

1 Purpose

(A). The purpose of this **Policy** is to —

(1). support the **University Community** in making acceptable **Cyber Security** and ethical decisions in order to —

(a). protect the **UWA Digital Identity** of members of the University Community;

(b). safeguard the reputation of the **University** by encouraging responsible online behaviour; and

(c). safeguard **University Information**, **IT Services** and **IT Assets**; and

(2). contribute to maintaining a University culture of integrity.

(B). In this Policy —

2 Scope

2.1 Institutional Scope

(A). The scope of this Policy applies to the entire University.

2.2 Individual Scope

(A). The scope of this Policy applies to the entire University Community when handling University Information or using IT Services on —

(1). **Personal Devices**; and/or

(2). IT Assets provided by the University.

3 Acceptable Use of IT

(A). **Acceptable Use of IT** means making decisions that comply with personal security responsibilities and the University's Code of Ethics and Code of Conduct when handling University Information or utilising UWA Digital Identities, Information Technology Services (IT Services) or IT Assets.

(B). UWA Digital Identity means information, such as user account, password or an email address, used by computer systems to represent a member of the University Community.

(C). IT Services means the combination of processes, expertise and resources by which Uni IT deliver value to the University Community to enable the achievement of their business objectives.

4 Acceptable Use of IT Practices

(A). The University Community will take all reasonable steps to protect University Information, UWA Digital Identities, IT Services and IT Assets both on **University Property** and when working remotely.

(B). Members of the University Community will be responsible for all activities originating from

their UWA Digital Identities.

(C). The University will provide training and guidance to maintain a cyber-secure environment.

(D). **University Officers** and **Contractors** must complete **Cyber Security** induction training as soon as practical after receiving access to their UWA Digital Identity, as well as annual refresher training and any additional training as directed.

(E). The University will provide UWA Digital Identities, IT Services and IT Assets for **University Activity** and to enable teaching, learning, **Research** and administration, with limited **Personal Use** permitted.

(F). Personal Use means use of UWA Digital Identities, IT Services and IT Assets that is not for the purposes of University Activity.

(G). Members of the University Community must only use UWA Digital Identities, IT Services and IT Assets for acceptable, legal and ethical purposes.

(H). Members of the University Community must not bypass or tamper with security measures or jeopardise, access, copy, alter or destroy any University Information, UWA Digital Identities, IT Service or IT Asset if they are not specifically authorised to do so.

(I). The University will regard communications conveyed by UWA Digital Identities to be University Information.

(J). The University may suspend any UWA Digital Identity upon breaching Policies.

5 Regulated Digital Content

(A). Members of the University Community must not create, access, download, possess or distribute digital content that is —

(1). illegal;

(2). considered as any form of harassment or discrimination, or otherwise interferes with the values of the University's Code of Ethics and Code of Conduct, or

(3). considered as **Regulated Digital Content**.

(B). Regulated Digital Content means 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.

(C). The University may grant access to Regulated Digital Content to support valid Research and teaching purposes upon written approval of an authorised University Officer.

6 Personal Devices

(A). Personal Devices may be used to —
(1). connect to University Wi-Fi networks; or
(2). remotely access University Information or IT Services via VPN.

(B). Personal Device means 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.

(C). Personal Devices must not be connected to wired network ports on University Property without authorisation by University IT.

(D). Personal Devices used to access University Information or consume IT Services must not have known security vulnerabilities.

(E). The University may refuse to provide IT Services to devices that do not comply with security requirements.

7 Third Party Access

(A). Members of the University Community will not provide access to University Information, IT Services and IT Assets to **Third Parties** unless approved by an authorised University Officer.

(B). Third Parties authorised to access University Information, IT Services or IT Assets must agree to comply with this Policy and the following Policies —
(1). Code of Ethics and Code of Conduct;
(2). Cyber Security Policy;
(3). Information Privacy Policy; and
(4). Information Protection Policy.

(C). University Officers authorising Third Party access will be accountable for ensuring that the Third Party is provided with the minimum levels of access required to perform agreed University Activity.

(D). 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.

8 Reporting of Incidents and Inappropriate Use

(A). Members of the University Community who identify or suspect any Cyber Security incident or breach of this Policy must report it as soon as possible, by —

(1). contacting the University IT Service Desk; or

(2). submitting an anonymous report in accordance with the Public Complaints Policy.

9 Monitoring

(A). The University may monitor, log, examine or disclose activity performed by UWA Digital Identities or related to University Information, IT Services or IT Assets for security, operational and compliance purposes.

(B). Members of the University Community making Personal Use of IT Services or IT Assets accept that it may be subject to such monitoring and analysis.

Definitions

Acceptable Use of IT is defined in section 3

Child Exploitation Material is defined in the Child Protection Policy.

Contractor is defined in the Policy Framework Policy.

Copyright is defined in Intellectual Property Policy.

Cyber Security is defined in the Cyber Security Policy.

Intellectual Property is defined in the Intellectual Property Policy.

IT Assets is defined in the Cyber Security Policy.

IT Services is defined in section 3

Personal Device is defined in section 6

Personal Use is defined in 4

Policy is defined in the Policy Framework Policy.

Regulated Digital Content is defined in section 5

Research is defined in the Research Integrity Policy.

Third Party is defined in the Policy Framework Policy.

University is defined in the Policy Framework Policy.

University Activity is defined in the Policy Framework Policy.

University Community is defined in the Policy Framework Policy.

University Information is defined in the Information Protection Policy.

University Officer is defined in the Policy Framework Policy.

University Property is defined in the Policy Framework Policy.

UWA Digital Identity is defined in section 3

End