Ākonga Digital Services and Technology Use Policy

Controlled Document – refer to Official Documents site for the latest version of this document.

Version:	26.1	**Date Effective:**	25 November 2026
Responsibility:	Digital Services Manager	**Date Reviewed:**	25 November 2026
Approver:	Executive Director Operations	**Next Review Date:**	24 November 2029

1. Purpose

1.1 This policy establishes UCOL's mandatory requirements for the responsible, secure, and lawful use of UCOL accounts, devices, networks, information and digital services by ākonga (students) and other learners. It supports teaching, learning and UCOL business while protecting people, information and technology from misuse, loss, and cyber harm.

2. Organisational Scope

2.1 This policy applies to all enrolled ākonga and other learners given access to UCOL digital services. It applies on and off campus, including when UCOL services are accessed through UCOL managed, loaned or personally owned devices.

2.2 Ākonga who are also UCOL kaimahi (staff), contractors, or otherwise have kaimahi level access must comply with the Kaimahi Digital Services and Technology Use Policy when using that access.

3. Roles and Responsibilities

Role	Responsibilities
Ākonga and other learners	Comply with this policy; protect UCOL accounts, devices and information; use approved services; complete any required digital services and cyber security learning or awareness activities; apply safe digital practices; and promptly report incidents, losses, suspected breaches and accidental disclosures.
Teaching and support kaimahi	Explain and reinforce requirements relevant to learning activities; direct ākonga to appropriate guidance and support; use approved teaching and support processes; and promptly escalate suspected breaches, privacy issues and information risks.
Digital Services	Maintain approved technology standards and security controls; manage access; provide guidance; monitor threats; and respond to security incidents.
UCOL	Maintain supporting privacy, records management, disciplinary and security arrangements and periodically review this policy.

4. Policy Statements

4.1 Responsible and Acceptable Use

a) UCOL digital services must be used primarily for authorised learning, teaching, study, research and related UCOL activities.
b) Limited personal use is permitted where it is lawful and reasonable, does not interfere with work or learning, does not create material cost or risk, and does not breach another UCOL requirement.
c) Users must act lawfully, ethically, and respectfully, and must use only the access and information required for an authorised purpose.
d) UCOL digital services must not be used for unauthorised commercial activity.

4.2 Prohibited Use

a) Bypassing, disabling, probing, or interfering with security controls, monitoring, filtering, authentication, networks, or systems.
b) Accessing, changing, copying, or disclosing another person's account, content, or communications without authority.
c) Sharing passwords, authentication codes, approval prompts, access tokens, or authenticated sessions.
d) Installing, copying, using, or distributing unlicensed, unauthorised, or malicious software or content.
e) Using UCOL services to harass, threaten, defame, discriminate, impersonate, deceive, or distribute unlawful or objectionable material.
f) Intentionally consuming excessive storage, processing capacity or bandwidth, or disrupting service for others.
g) Connecting rogue network equipment, creating unauthorised bridges or hotspots, or connecting a device known or suspected to be compromised. Uploading UCOL owned, confidential, sensitive or personal information about others to personal email, personal cloud storage, unapproved artificial intelligence services, or any other unapproved platform.

4.3 Cybersecurity

a) Users must comply with UCOL authentication requirements for ākonga, including the use of a password and multi-factor authentication where required, using an approved authentication method. Users must deny and promptly report any unexpected authentication request.
b) Accounts must be used only by the person to whom they are assigned. Screens must be locked or sessions ended when a device is unattended.
c) Unexpected links, attachments, QR codes, payment requests and credential prompts must be treated cautiously, and unusual requests must be verified through a separate trusted channel.
d) UCOL information must be accessed, stored, and shared only through approved services and with the least access necessary.
e) Suspected phishing, malware, unauthorised access, privacy breaches, accidental disclosures, or lost or stolen devices that have accessed UCOL information must be reported promptly to the Service Desk.

f) Users must cooperate with reasonable containment, investigation, evidence preservation, and recovery actions. UCOL may restrict access, revoke sessions, or isolate a device where necessary to protect people, information, or systems.

4.4 Use of OneDrive and Approved Repositories

a) UCOL OneDrive is the approved personal storage location for study-related working files provided through the ākonga Microsoft 365 account.
b) Where UCOL requires work to be submitted or retained in a learning platform or another approved system, that system remains the authoritative location. Saving another copy in OneDrive does not replace the required submission or record.
c) Ākonga must share files only with intended recipients and must not use public or "anyone" links for confidential, sensitive, or personal information unless expressly authorised.
d) Ākonga must not move, delete or transfer UCOL information where a preservation instruction or applicable UCOL process requires it to be retained.
e) OneDrive synchronisation and version history do not replace a required submission, records-management requirement, or specialist backup. Ākonga remain responsible for retaining personal study material they are entitled to keep before their UCOL access ends.
f) UCOL records, licensed content, confidential information, and personal information about others must not be retained after access ends unless authorised.

4.5 Bring Your Own Device (BYOD)

Ākonga may use a personally owned device to access Microsoft 365, approved learning platforms and other UCOL services that are approved for use on personal devices. When using a personal device to access UCOL services, ākonga must:

a) Keep the device reasonably secure, including using a screen lock, current security updates and available security protections;
b) Protect their UCOL account and not allow another person to access UCOL services using their account or an active session;
c) Use only UCOL approved applications, services and network connections, and must not attempt to bypass UCOL security or access controls;
d) Minimise the storage of UCOL information on the device and comply with any restrictions on downloading or synchronising information; and
e) Promptly report loss, theft or suspected compromise of a device where it has been used to access or store UCOL information.

Ākonga are responsible for the purchase, maintenance, licensing, backup and repair of their personal devices and personal data. UCOL support is limited to reasonable assistance with accessing approved UCOL services.

UCOL may restrict or remove access to its accounts, applications, information or networks where reasonably necessary to protect UCOL information, people or systems.

Activity involving UCOL accounts, services and networks may be logged and monitored in accordance with law and UCOL policy.

4.6 Software and Hardware

Ākonga must not install, remove, reconfigure, or modify software, hardware, security tools, or system settings on UCOL owned or loaned devices unless authorised. License conditions apply to all UCOL provided software and services.

4.7 Information Protection and Privacy

a) Personal, confidential, or sensitive information must be accessed, used, stored, shared and disclosed only for an authorised purpose, using approved UCOL systems or repositories.
b) Recipients, attachments, and sharing permissions must be checked before information is sent or shared.
c) Information from UCOL systems must not be photographed, recorded, copied, or disclosed unless authorised.
d) Applicable privacy, copyright, records management, information classification, and preservation requirements must be followed.
e) Information sent, shared, stored, or accessed incorrectly must be reported promptly and must not be concealed.

4.8 Monitoring and Protective Action

UCOL may monitor and retain records of activity involving its accounts, networks, devices and services for security, operational, legal, and policy compliance purposes. UCOL may take immediate and proportionate protective action, including restricting access, quarantining a device, preserving evidence, or removing harmful content.

4.9 Non-compliance

Non-compliance may result in education or guidance, removal or restriction of access, recovery of costs where appropriate, action under applicable ākonga disciplinary processes, and referral to law enforcement or another authority where required. Any response will take account of seriousness, intent, impact, recurrence and applicable UCOL procedures.

4.10 Account Closure and Information Handover

Access is time limited and ends in accordance with enrolment and account lifecycle arrangements. Ākonga are responsible for exporting personal material they are entitled to retain before access ends. Required UCOL submissions and records remain in the approved learning or business system.

5. References

Internal

- Ākonga Bullying, Harassment and Discrimination Policy and Procedure
- Student Discipline Statute (Non-Academic) 2019
- Internet and Online Services Acceptable Use Policy
- Use of UCOL Premises and its Resources Out of Hours and for Private Use Policy

• Privacy Policy
External • Copyright Act 1994 • Crimes Act 1961 • Films, Videos, and Publications Classification Act 1993 • Harmful Digital Communications Act 2015 • Official Information Act 1982 • Privacy Act 2020 • Public Records Act 2005

6. Definitions

Term	Definition
Approved service	A digital service expressly provided or authorised by UCOL for the relevant purpose and access method.
Authoritative repository	The approved system or repository that holds the official or controlling version of information.
BYOD	A personally owned device used to access UCOL accounts, networks, information, or digital services.
Cybersecurity incident	An actual or suspected event that threatens the confidentiality, integrity or availability of information or systems.
Microsoft 365 license	The Microsoft applications and cloud services assigned by UCOL, subject to license terms, UCOL configuration and the permitted access method.
Personal information	Information about an identifiable individual.
UCOL information	Information created, received, held, or managed for UCOL activities, regardless of format or location.
UCOL managed device	A device owned or controlled by UCOL and administered through UCOL management and security controls.

Document Version History

Version	Effective Date	Created/Reviewed By	Reason for review
26.1	November 2026	Digital Services Manager	New student specific policy replacing the Computer Use Policy. Includes additional requirements relating to information security, passwords, and multi-factor authentication (MFA).