	UWC			
UNIVERSITY of the WESTERN CAPE	**ACCEPTABLE USE POLICY**	Council Approval Reference Number	C2021/03 (29 June 2021)	
		Implementation Date	1 July 2021	
		Parent Policy	Information Security Policy	
		Version Number	1.17	
		Revision / Amendment Date	May 2021	
		Policy Owner	Director: ICS	
		Executive Management Portfolio	ED – Finance and Services	
		Contributors	Refer to revision history	
		Circulated by:	ICS	
		Circulated to:	**Consultation Channel**	**Date presented**
			IT Portfolio Steering	01 Feb 2021
			Executive Management	23 Feb 2021
			UWC Institutional Forum	30 April 2021
			Senate Executive Committee	30 April 2021
			Senate Academic Planning	30 April 2021
			IT Governance Committee	17 May 2021
			UWC Senate	25 May 2021
			UWC Council	29 June 2021
		Approval Date:	29 June 2021	

UNIVERSITY OF THE WESTERN CAPE (UWC)

ACCEPTABLE USE POLICY

DATE OF LAST APPROVAL: C2021/03 (29 JUNE 2021)

This policy should be reviewed and maintained in line with the practices outlined in the 'ICS Policy Framework and Guideline' document.

Contents

1. Introduction

The UWC IT department (hereafter "IT") is responsible for providing staff, students, third parties and guests (hereafter "user") with the necessary ICT equipment, systems and information assets (hereafter "ICT resources") to enable the academic programme and its supporting processes. UWC has a legal obligation towards ensuring the acceptable use and protection of its ICT resources to minimise the risk of information security and cyber threats such as phishing, ransomware, computer malware, data loss, system unavailability or degraded performance, theft and unauthorised access, modification or disclosure of information. Every user has a responsibility towards protecting UWC's ICT resources and by accessing or using these resources, irrespective of device ownership and connectivity methods, users agree to be bound by this Policy and the overarching Information Security Policy.

1.1 Purpose

This Policy serves as a **functional policy** that underpins the **overarching Information Security policy**. The purpose of this policy is to outline **acceptable and unacceptable behaviours for accessing and/or using UWC's ICT resources**. This Policy is not intended to restrict staff, contractors or third parties who have a legitimate need to carry out certain IT duties as part of their jobs nor is it intended to restrict students from their academic freedom. This Policy must be read in conjunction with other applicable policies as listed in section 6 of this document.

1.2 Applicability and Scope

This policy applies to **all UWC staff, Council members, students, third parties and guests** who have access to UWC's ICT resources.

The scope of this Policy includes **all UWC-owned, licensed or leased IT equipment, systems and information assets** (collectively "ICT resources"), as well as any **personal devices connecting to UWC's network.**

2. Definitions

"Must"	"Must" imposes a legal obligation on the reader implying that something is mandatory.
"Will"	"Will" is similar to "must" however implies a future obligation.
"Should"	"Should" implies that the reader has a choice, i.e. there may be a valid reason to bypass a requirement, however the full

	implications must be understood and carefully assessed before choosing a different recourse.
"Establish"	For the purposes of this policy, "establish" implies defined (documented) and implemented.
Acceptable use	Refers to the responsible, ethical and lawful use of ICT resources in accordance with this Policy and applicable laws and regulations to prevent any reputational damage, legal liability or risk to UWC.
IT	The Information Technology (IT) department that is responsible for delivering Information and Communication Technology (ICT) services to the UWC community.
ICT resources	For the purposes of this Policy, ICT resources is the collective term used for ICT equipment, systems and information assets.
ICT equipment	Includes but is not limited to UWC-owned or leased computer hardware, software, servers, desktop computers, laptops, mobile devices, removable media, telephones, printers, photocopy machines, fax machines and ancillary equipment.
Information asset	Any information or data that is of value to UWC whether in electronic or hard copy format and if its security is compromised, it would have a significant impact on the institution's business operations.
Personal information	Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to: a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; b) information relating to the education or the medical, financial, criminal or employment history of the person; c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; d) the biometric information of the person;

	e) the personal opinions, views or preferences of the person; f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; g) the views or opinions of another individual about the person; and h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;
Processed / processing	Refers to any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including: a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; b) dissemination by means of transmission, distribution or making available in any other form; or c) merging, linking, as well as restriction, degradation, erasure or destruction of information;
Systems	UWC's information systems including network, operating system, application or database software.
Classified information	UWC's Sensitive, Confidential and Internal data that requires a higher level of protection as defined in the Data Classification Standard.
Users	Any person (e.g. UWC student, staff, third party, etc.) who has been authorised to access UWC's information assets and related systems.

3. Policy Statements

3.1 General requirements

3.1.1 Email and internet use

3.1.1.1 Offensive material: Users must not use the ICT resources to access, download, store, post or distribute material that is obscene, indecent or pornographic. Special care is required when sending material electronically or posting on the internet (e.g. through web pages or social media). Researchers who intend to access, store or distribute such material legitimately in the course of their work must seek written permission in advance from the appropriate Research Ethics Committee. Child pornography is strictly prohibited.

3.1.1.2 Unsolicited and offensive email: Users must not initiate or forward unsolicited email chain letters, jokes or other mass emails (i.e. spam) or offensive emails including hate speech, profanity, pornography, obscenity, vulgarity, nudity, defamation, personal attacks, emails that violate the privacy of UWC staff and/or their families, emails that include promotion of events, groups, pages, web sites, organisations and programs not related to or affiliated to UWC.

3.1.1.3 Email spoofing: Users will not construct and send emails under the pretense of being someone else.

3.1.1.4 Internet content filtering: UWC reserves the right to filter content to prioritise educational, teaching, learning, research and other associated sites.

3.1.1.5 Infringe on the proprietary, privacy and copyright: Users must not infringe on the proprietary, privacy and copyright of others when using the Internet to download material.

3.1.1.6 Posting or exfiltration of classified information: Users are strictly prohibited from posting or exfiltrating sensitive or confidential information such as usernames, passwords, security or server-specific information, UWC email addresses or distribution lists, which could assist third parties to gain unauthorised access to UWC Systems or expose UWC to cyber threats and any possible reputational damage.

3.1.1.7 Personal email accounts: Users are prohibited from sending UWC classified information to their personal email accounts.

3.1.1.8 Misaddressed email: Any email received in error must be deleted by the recipient after notifying the sender that the email was received in error. If the user is uncertain as to whether the email should be deleted, then IT must be contacted for assistance.

3.1.1.9 Disclaimer: All emails transmitted outside of UWC will automatically contain the standard disclaimer as issued by UWC Management from time to time.

3.1.2 Access to ICT resources

3.1.2.1 Responsible use of data: Data must be used responsibly and only for its intended purpose and the privacy of data must be respected.

3.1.2.2 Secure handling of data: All data owned or processed by UWC, whether primary or secondary, must be handled in accordance with its security classification as defined in the Data Classification Standard.

3.1.2.3 Access to UWC classified data by external parties: Will be governed by a signed Non Disclosure Agreement (NDA).

3.1.2.4 Personal information: Users who process personal information on behalf of UWC are required to do so in accordance with POPIA and must notify the UWC Information Officer of details of their processing.

3.1.2.5 Disclosure of information: Users must take care not to disclose information to unauthorised individuals or third parties.

3.1.2.6 Personal use of ICT resources: ICT resources will not be used for the purposes of running a personal business, including promotions or advertising. ICT resources are primarily made available to enable the academic programme and any incidental personal use will be permitted within reason. The onus is on the user to ensure that personal use of ICT resources does not:

- interfere with productivity and the performance of administrative operations and the academic programme;
- incur unwarranted expenses on the University;
- have a negative impact on the University in any way;
- compromise the confidentiality, integrity and availability of the University's systems and information assets.

3.1.3 Security

3.1.3.1 Password management: All passwords must comply with the UWC Password Policy.

3.1.3.2 Misuse of or tampering with ICT resources: Unauthorised access and use of accounts, programs and/or data (including copying, configuring, corrupting or deleting), all forms of hacking, deliberate introduction of malware and circumventing antivirus or malware protection installed on ICT resources are prohibited.

3.1.3.3 Incident reporting: Any warning, suspicion or occurrence of a computer virus, hoax, persistent spam/phishing, denial of service or hacking attempt must immediately be reported to IT.

3.1.3.4 Antimalware software: Users must ensure that their devices are up to date with the latest antimalware software.

3.1.3.5 Backups: Users are responsible for their own data security and backups.

3.1.3.6 Information Security awareness and training: Users must attend and complete all mandatory awareness and training provided by the University, especially where it relates to information security.

3.1.4 Visitor WIFI

3.1.4.1 Eduroam WIFI: Eduroam WIFI is available to all UWC users. Visitors from eligible institutions may access the Eduroam WIFI using their home institution's login credentials. In such cases their home institution's Acceptable Use Policy will apply in addition to this policy.

3.1.4.2 Guest WIFI: A separate guest WIFI has been made available for guests and will be managed by the relevant faculty.

3.1.5 Software

3.1.5.1 Software installation: Measures will be implemented to restrict users from installing any software on UWC devices.

3.1.5.2 Compliance with software license agreements: Users must ensure that they comply with the terms and conditions of software license agreements.

3.1.6 Rights in content reuse

3.1.6.1 Users must refrain from using third party text, images, sounds, trademarks or logos in materials such as emails, documents and web pages without the consent of the rights holder.

3.1.7 Bring Your Own Device "BYOD"

3.1.7.1 BYOD policy: It is permissible for users to connect their personally-owned devices to the University's wireless network. Users must adhere to the minimum requirements outlined in the *BYOD Policy*.

3.1.8 Physical security

3.1.8.1 Access cards: Users must not share their access cards. Lost or stolen cards must be reported to the Risk, Safety & Compliance department.

3.1.8.2 Securing unattended devices: Users must not leave their computers, laptops or mobile devices unattended, and if left unattended they need to ensure that it is secured. Users are encouraged to use screensavers or log out of a session to prevent unauthorised access to their devices.

3.1.9 Monitoring usage

3.1.9.1 Monitoring of internet and email usage: UWC reserves the right to monitor the use of ICT resources including bandwidth usage, websites visited and email traffic on the UWC network.

3.1.9.2 Reporting of unauthorised use: Any unauthorised use of UWC's ICT resources must immediately be reported to the IT service desk.

3.1.9.3 External Disclosure: Whilst respecting a user's right to privacy, UWC may, for legitimate purposes, disclose a user's content to relevant third parties as required. Any information collected during the course of the monitoring will be held securely in accordance with the POPIA requirements.

3.2 Staff-specific requirements

3.2.1 Office security: Staff must ensure that their offices are secured whilst unattended.

3.2.2 Contract negotiation: Staff should note that it is possible to form contracts electronically, without any hard copy confirmation from the user. Special care should be taken to obtain appropriate authority before purporting to commit the University to any contractual obligations (which may include clicking 'I agree' to an online dialogue box) and the wording 'subject to contract' should be used on emails where appropriate.

3.2.3 Staff transactions on behalf of UWC: Staff may not transact on behalf of UWC via the Internet or email (i.e. purchase of goods or services) without receiving the necessary authority and adhering to the UWC Procurement Process.

3.2.4 Staff meeting protocols: Meetings are confidential and are to be attended by the invitee only. Log-in details may not be shared with 3rd parties nor may 3rd parties be present during virtual meetings. Other than by persons authorised to do so by the University, meetings may not be recorded by audio or video means. Meeting pack(s) should not be distributed to unauthorised persons.

3.3 Student-specific requirements

Within UWC, Research, Student Computer Laboratories, Campus Residences and CIECT may have specific requirements as it pertains to their respective areas and as a result need to formulate specific operational procedures aligned with the overarching Acceptable Use policy.

4. Policy Compliance

Compliance Measurement

IT will take proactive measures to assess compliance to this policy internally through periodic control assessments.

Non-Compliance

Contraventions of this policy may be subject to the UWC Code of Conduct and Disciplinary Processes for UWC staff, Council members and students and legal action may be taken for third parties and guests. Examples of what constitutes a breach to this policy include:

- UWC staff, student or third party negligence in fulfilling their information security duties, e.g.
    - Sharing of user account login details and/or access cards;
    - Sharing UWC classified information with a third party without obtaining prior authorisation;
    - Sending UWC classified information to a personal email account.
- Misuse or abuse of ICT resources for personal use and gain.

Exceptions

Where it is not possible or practical to apply or enforce any part of this policy, a formal request must be submitted with business justification to the IT Service Desk (servicedesk@uwc.ac.za). Policy exceptions will be granted in the form of a risk acceptance, only once the Risk Owner has signed off on the associated risks. Risk acceptances must only be granted for specified periods of time and must be reviewed annually.

5. Roles & Responsibilities

Key responsibilities in respect of this policy	*IT GRC	*IT Dept	*HR Dept	Legal	Users	Audit	*EMC	*ICT Portfolio SteerCom	*ICT GC	Council
Maintain (review and update) this policy.	R	C	C	C						
Approval of this policy.							R	R	R	R
Communicate and create awareness of this policy and any subsequent changes.	R		R				C	C	C	C
Establish standards, processes, procedures and controls to support this policy.		R								
Ensure implementation of policy.	C	C	C	C	R		C	C	C	C
Risk assessments – assess risks associated with this policy and track the management and remediation of risks.	R	C	C				C	C	C	C
Policy compliance measurement – assess compliance to this policy.	R	C	C				C	C	C	C
Audit key controls and report on the design and effectiveness of the control environment.	C	C	C			R				

*GRC = Governance, Risk and Compliance *IT = Information Technology, *Dept = Department, HR = Human Resources, EMC = Executive Management Committee, SteerCom = Steering Committee, GC = Governance Committee, R = Responsible, C = Consulted

6. Related internal documents, industry standards and legislation

- **Internal documents:** Information Security Incident Management Procedure, Data Classification Standard, BYOD Policy (2021/03), Password Policy (2005/3), Password Creation Management & Protection Procedure.
- **Industry standards:** ISO/IEC 27001:2013
- **Legislation:** Protection of Personal Information Act 4 of 2013, Electronic Communications and Transactions Act 25 of 2002.

7. Revision History

Version	Date of change	Summary of Change	Changed by
1	Sep 2004	Initial Policy Formulation and Council Approval	Mike Lewis
1.1	Oct 2007	Updates – Terminology, structure, content	Anver Natha
1.2	Nov 2008	Updates – Terminology, structure, content	Anver Natha
1.3	Mar 2013	Updates – Terminology, structure, content	Anver Natha, Conrad Tiflin
1.4	Jun 2013	Updates – Terminology, structure, content	Anver Natha, Conrad Tiflin
1.5	Sep 2014	Updates – Terminology, structure, content	Anver Natha, Conrad Tiflin
1.6	Dec 2015	Updates – Terminology, structure, content	Anver Natha, Conrad Tiflin
1.7	Apr 2016	Updates – Terminology, structure, content	Anver Natha, Conrad Tiflin
1.8	Jul 2016	HR and Legal Review	Karlene Mercuur and Tamima Taliep
1.9	Feb 2017	Updates – Content	Anver Natha, Conrad Tiflin
1.10	Apr 2017	Updates – Content	Anver Natha, Conrad Tiflin
1.11	May 2017	Updates – Content	Anver Natha, Conrad Tiflin, Tamima Talip
1.12	May 2017	Updates based on IT Portfolio Steercom sitting	Anver Natha, Conrad Tiflin, Tamima Talip
1.13	December 2020	• Renamed the policy from “Computer, Internet and Email Use policy” to “Acceptable Use policy”. • Updated the structure and contents of the policy in line with industry standards and legislative requirements as listed in Related internal documents, industry standards and legislation. • Aligned the policy with the ‘IT policy framework and guideline’ to ensure standardisation across all IT policies.	Ilhaam Gihwala
1.14	February 2021	• Updated statements 3.1.8.2 and 3.3 of the Acceptable Use Policy • Deleted 3.1.8.3	Gail Francke
1.15	February 2021	• Added 3.2.4 Meeting protocols	Gail Francke
1.16	May 2021	• Updated the policy cover page to reflect stakeholder consultation	Gail Francke
1.17	May 2021	• Updated the ‘circulated to’ section in the cover page table to be in date order sequence • Updated Senate date from 23 Feb to 25 May 2021 • Replaced ‘will’ with ‘may’ and added ‘Council members and guests’ in the	Gail Francke

		Non-Compliance section on page 10: ‘..Processes for UWC staff, Council members and students and legal action may be taken for third parties and guests’ • Removed business from ‘business justifications’ in Exceptions section • Changed ‘may’ to ‘must’ in Exceptions section: Risk acceptances ‘must’ only be granted	