


CPUT Acceptable Usage Policy			
Policy Group(s): Delete categories that are not relevant	A: Governance and Administration (Registrar) B: Teaching & Learning C: Finance D: Human Resources E: Student Affairs F: Technology, Partnerships, Research and Planning G: Operations		
Type: Tick document category	Policy <input checked="" type="checkbox"/> Procedure <input type="checkbox"/>	Guideline <input type="checkbox"/> Regulation <input type="checkbox"/>	
CPUT Statute and/or Regulation Reference no. and date:	<ul style="list-style-type: none"> Number - 46382 Volume - 1039 Date – 20/05/2022 		
Relevant Legislation and/or Policy, Codes of practice, Professional authorities:	<ul style="list-style-type: none"> The Electronic Communications and Transactions Act (Act No. 25 of 2002). The Promotion of Access to Information Act (Act No. 2 of 2000). The Protection of Personal Information Act (Act No. 4 of 2013). The Regulation of Interception of Communications and Provision of Communication Related Information Act (Act No. 70 of 2002). 		
Relevant Institutional Policies/ documents/manuals/ handbooks:	<ul style="list-style-type: none"> Electronic Communications Policy CTS Data Centre Policy IT Access Control policy Information Security Policy IT Incident Management Policy 		
Policy Reference and Version no.:	<ul style="list-style-type: none"> 5/1/P (Reference Number) 1.0 (Version Number) 		
Consultation Process To be verified and signed off before approval	<ul style="list-style-type: none"> Registrar's Office CTS Management CTS Policy Working Group Business ICT Committee Management Committee IT Governance Committee Council Approval 		
Policy Owner:	Deputy Vice Chancellor: Operations		
Compliance Officers:	Senior Director CTS CPUT Compliance Managers		
Certification of Due process:	<div style="border-top: 1px solid black; height: 20px; width: 100%;"></div>		

To be verified and signed once approved by the relevant authority		Vice Chancellor 		Date 12/04/2023	
Approval Date		Commencement Date		Review Date	

REVISION HISTORY: Only applicable to amended or reviewed Policies. Record details of amendments/revision.					
Version No.	Approved/ Rescinded	Date	Approving Authority	Resolution Number/ (Minute number)	Date for next review (start date for review process)
	Approved	25/03/2023	Council	5.1.3.3	25/03/2026

For office use only	
Policy Group (Broad Policy field)	Governance and Administration
Subject (Policy sub-field)	Policies
Reference Number	5/1/P
Version Number	1.0
Key Words:	Acceptable Usage

POLICY STATEMENT	
1.0 Intent	1.1. The purpose of this policy is to define and promote the responsible use of computing resources at CPUT.
2.0 Scope	2.1 This policy applies to all CPUT staff, students, guests, and contractors as well as any other CPUT affiliate(s) attempting to access or use CPUT computing resources.
3.0 Objective(s)	3.1 The objective of this policy is to govern the acceptable use on all computing resources including university owned, licensed, or managed resources. 3.2. Access to and usage of information technology resources necessitate certain expectations and responsibilities for all CPUT users.
4.0 Definitions and Acronyms	4.1 Access – Any mechanisms by which individuals gain legitimate access to information and information systems. 4.2 Computing Resources – Computer and network resources including all electronic communication systems and equipment.

	<p>4.3 CPUT – Cape Peninsula University of Technology.</p> <p>4.4 CPUT User – CPUT Staff, student or guests who are legally allowed to access the university computing resources.</p> <p>4.5 Core University Functions – activities that underpin institutional processes that include, but are not limited to, Teaching and Learning, Research, Community Engagement, Institutional Development, Finance, Marketing and Advancement.</p> <p>4.6 CTS – Computer and Telecommunication Services department of CPUT.</p> <p>4.7 Digital Device – is an electronic device that can receive, store, process or send digital information.</p> <p>4.8 ICT – Information and Communication Technology.</p> <p>4.9 Information – Information includes data stored on computers, transmitted over computer networks or stored on storage devices.</p> <p>4.10 Information Systems - an integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products.</p> <p>4.11 Institutional data - Information created, collected, maintained, transmitted, or recorded by or for the university to conduct university business.</p> <p>4.12 Network - A group of two or more computers or other electronic devices that are interconnected for the purpose of exchanging data and sharing resources.</p> <p>4.13 Personal Information as defined in the POPIA, means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:</p> <p>4.13.1. 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;</p> <p>4.13.2. information relating to the education or the medical, financial, criminal or employment history of the person;</p> <p>4.13.3. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;</p>
--	---

	<p>4.13.4. the biometric information of the person;</p> <p>4.13.5. the personal opinions, views or preferences of the person;</p> <p>4.13.6. 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;</p> <p>4.13.7. the views or opinions of another individual about the person; and</p> <p>4.13.8. 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.</p>
5.0 Policy/Procedure Principles	<p>5.1 Guiding Acceptable Use Principles</p> <p>5.1.1 CPUT computing resources are for CPUT faculty staff, students, guests and service providers (where necessary) to use for Core University Functions.</p> <p>5.1.2 All CPUT users accessing resources are responsible for seeing that computing resources are used in an effective, efficient, ethical, and lawful manner.</p> <p>5.1.3 CPUT users must behave in a manner consistent with CPUT's staff and student code of conduct and comply with all applicable laws, regulations, and CPUT policies.</p> <p>5.1.4 CPUT users must be considerate of the needs of other users by making every reasonable effort not to impede the ability of others to use CPUT computing resources and show restraint in the consumption of shared resources.</p> <p>5.1.5 Unauthorized access or use of university computing resources or data is strictly prohibited.</p> <p>5.1.6 The use of CPUT computing resources is a revocable privilege to all CPUT staff, students and guests that utilise CPUT computing resources.</p> <p>5.2. Access Requirements</p> <p>The following statements govern access to the CPUT computing resources:</p>

	<p>5.2.1 All access to CPUT computing resources (including computer and network access) is denied unless expressly granted.</p> <p>5.2.2 Access will only be granted for Core University Functions</p> <p>5.2.3 Accounts are assigned to current registered students and employees of CPUT and are not to be shared unless specifically authorized by the CTS department. Each CPUT user is solely responsible for all functions performed from accounts assigned to them.</p> <p>5.2.4 It is a violation of this policy for any CPUT user to allow others (including other users within the CPUT network) to use or have access to their account. Intentionally or negligently revealing one's password is prohibited.</p> <p>5.2.5 CPUT users are responsible for ensuring that they comply with all IT policies, including those related to keeping the CPUT network secure such as the Information Security Policy as well as the IT Access Control Policy and/or any other CPUT governance policies.</p> <p>5.3. Fair share of Resources</p> <p>5.3.1 The CTS department, and other university departments which operate and maintain computers, network systems and servers, must ensure that frivolous, excessive, or inappropriate use of the resources by one person or a few people does not degrade performance for others.</p> <p>5.3.2 The campus network, computer clusters, mail servers and other central computing resources are shared widely and have limited capacity, requiring that resources be utilized with consideration for others who also use them.</p> <p>5.3.3 The university may choose to set limits on an individual's use of a resource through quotas, time limits, and other mechanisms to ensure that these resources can be used by anyone who needs them.</p> <p>5.4. Prohibitions</p> <p>The following activities are specifically prohibited:</p> <p>5.4.1 CPUT users may not disguise their identity, the identity of their account or the machine that they are using.</p> <p>5.4.2 CPUT users may not impersonate another person or organization.</p>
--	--

	<p>5.4.3 CPUT users may not use CPUT assigned Internet number space (domain name) for their own personal domain without the prior express permission of the university management.</p> <p>5.4.4 CPUT users may not intercept, monitor, forge, alter or destroy other CPUT users' communications.</p> <p>5.4.5 CPUT users may not read, copy, change, or delete another CPUT user's data or communications without the prior express permission of the owner as well as the CTS department.</p> <p>5.4.6 CPUT users may not engage in actions that disrupt or interfere with the legitimate use by other CPUT users of any computing resources.</p> <p>5.4.7 CPUT users may not possess, distribute, or send unlawful communications of any kind, including but not limited to threats of violence, obscenity, child pornography and/or harassing communications (as defined by law), or participate or facilitate communications in furtherance of other illegal activities that may bring the establishment into disrepute.</p> <p>5.4.8 CPUT users should not bypass computer or network security mechanisms, without the prior express permission of the CTS department as well as the data or system owner.</p> <p>5.4.9 CPUT users must obey all established guidelines for any computers or networks used, both inside and outside of CPUT.</p> <p>5.4.10 CPUT users may not use the CPUT network for private business, commercial or political activities, fundraising, or advertising on behalf of non-CPUT organizations, unlawful activities or uses that violate other CPUT policies.</p> <p>5.4.11 CPUT users may not violate any laws or ordinances, including, but not limited to, copyright, discrimination, harassment, and/or export controls. CPUT may contact local law enforcement authorities to investigate any matter at its sole discretion.</p> <p>5.5 University Rights</p> <p>5.5.1 The university reserves the right to access, monitor, review, and release the contents and activity of an individual CPUT user's account(s) as well as that of personal Internet account(s) used for the processing of university information</p>
--	---

	<p>5.5.2 The university reserves the right to access any university owned resources on university property, connected to university networks, or containing university data.</p> <p>5.5.3 By accessing and using the Universities Information Systems, staff, students, and guests as well as any other CPUT affiliate who is authorized to access institutional data are consenting to such monitoring and information retrieval by law enforcement and for other purposes.</p> <p>5.5.4 CPUT reserves the right to update or revise this policy or implement additional policies in the future. CPUT users are responsible for staying informed about CPUT policies regarding the use of computer and network resources and complying with all applicable policies.</p> <p>5.6. Policy enforcement Consequences and Sanctions</p> <p>5.6.1 Failure and/or refusal to abide by the rules principles and procedures detailed in this policy shall be deemed as misconduct and CPUT may initiate the appropriate investigation and disciplinary action against such CPUT users.</p> <p>5.6.2 Penalties for violating this policy may include restricted access or loss of access to the CPUT network, termination and/or expulsion from CPUT and in some cases, civil and/or criminal liability.</p>
6.0 Responsibility	<p>6.1 Faculty Deans, HOD's and Divisional Heads</p> <p>6.1.1 Advise new staff/students, guests and service providers who have access to the university network about the Acceptable Usage Policy.</p> <p>6.2. CPUT IT Staff (including Faculty IT Coordinators, CTS Staff, etc.)</p> <p>6.2.1 Report breaches of this policy to respective line managers and CTS Management.</p> <p>6.3. CTS Management</p> <p>6.3.1 Report serious staff breaches to Human Capital Department for processing via the Staff Disciplinary Code.</p> <p>6.3.2 Report serious student breaches to the Department of Student Affairs.</p> <p>6.4. Human Capital Department</p> <p>6.4.1 Processing staff disciplinary processes.</p> <p>6.5. Department of Student Affairs</p> <p>6.5.1 Processing student disciplinary processes.</p>

7.0 Accountability and Authority:

Implementation:	CTS Department
Compliance:	All CPUT users
Monitoring and Evaluation:	Senior Director: CTS, Senior Director: Human Capital, Dean of Students
Development/Review:	Senior Director: CTS, CTS Policy Working Group
Approval Authority:	Council
Interpretation and Advice:	Senior Director: CTS

8.0 Who should know this Policy?

This policy applies to all CPUT staff, students, guests, and contractors as well as any other CPUT affiliate(s) attempting to access or use CPUT computing resources.

9.0 Policy/procedure implementation plan	<p>9.1 The CTS Director, in conjunction with relevant institutional stakeholders, are required to develop the policy implementation plan.</p> <p>9.2 The implementation plan will include:</p> <p>9.2.1 Processes and mechanisms to ensure that compliance to this policy is monitored, managed, and reported on</p> <p>9.2.2 Mechanisms include: Policy awareness campaigns (via electronic communications platforms, such as email, social media, CPUT websites); Policy compliance audits; Dedicated channels for reporting non-compliance incidents</p>
10.0 Resources required	10.1 Human as well as technology resources to develop and implement the policy implementation plan.

11.0 Answers to FAQ	<p>11.1 What is Acceptable Usage? Acceptable usage refers to the responsible use of computing resources at CPUT.</p> <p>11.2 What is Fair Use CPUT computing resources must be utilized with consideration for others who also use them.</p> <p>11.3 What are consequences for non-compliance to this policy Penalties for violating this policy may include restricted access or loss of access to the CPUT Network, termination and/or expulsion from CPUT and in some cases, civil and/or criminal liability.</p>

EFFECTIVENESS OF THE POLICY

Performance Indicator(s):	<p>Number of non-compliance incidents reported.</p> <p>Number of policy awareness campaigns launched.</p> <p>Existence of policy compliance processes implemented.</p> <p>Maturity of policy compliance processes implemented.</p>
----------------------------------	--