


Category	IT Infrastructure and Services	Policy Number	SUP-ITS-101	 جامعة زايد ZAYED UNIVERSITY
Classification	Public	Version	2.2	
Responsible Office	CAFO	Policy Owner	ITD Director	
Date Approved	22 April 2025	Effective Date	22 April 2025	
Date Last Reviewed	25 November 2024	Due Date for Next Review	22 April 2028	

POLICY

Computing Resources

1. Purpose

This policy outlines the use of computing resources by students, faculty, staff, and, where appropriate, users external to the Zayed University community.

2. Scope of Application

This policy applies to all Zayed University users and external users where appropriate.

3. Definitions

CAFO	Chief Administration and Finance Officer
ITD	Information Technology Department
University	Zayed University
University Community	Zayed University employees and students

4. Policy

4.1 Zayed University (“**University**”) is committed to being a leading institution in the effective use of information technology for the enhancement of student learning, University management, research, and outreach.

4.2 The computing resources that the University provides are for the educational, research, and administrative endeavors of its students, faculty, and staff. It is expected that the computer resources be utilized in the achievement of these core institutional activities. Under no circumstances may faculty, students, or staff use University computing resources in ways that are illegal, unethical, or that interfere with reasonable use by other members of the University community.

4.3 In order to achieve the goals of the University with regards to computing resources, faculty and staff can expect to be provided with:

- a) clear expectations and guidelines about University computing resources,
- b) adequate training about University computing resources,
- c) ample professional development opportunities,

- d) prompt technical support, and
- e) a fast and efficient network.

4.4 Violations

- 4.4.1** Violations of computing resource rules and policies may result in University disciplinary action.
- 4.4.2** Individuals who violate license agreements and copyright may be subject to legal action from external parties (publishers/vendors/copyright holders).
- 4.4.3 Access Restriction**
 - a) Access to computing resources may be restricted by the University without prior notice and without the consent of the user when required by and consistent with law.
 - b) Access to computing resources may be restricted by the University with prior notice and written warning when actions interfere with reasonable use by other members of the University community.
 - c) In all cases, the individual(s) concerned will be notified of the reason and duration of the access restriction as soon as possible.
 - d) Access will be restored when the situation has been resolved.

4.5 Blackboard

- 4.5.1** Blackboard is intended to support the teaching, learning and research of University faculty, staff, and students and facilitate communication and the sharing of information and resources within the University community and beyond. University faculty and staff may use Blackboard for:
 - a) courses they teach,
 - b) committees engaged in academic endeavors,
 - c) academic organizations of which they are a member, and/or
 - d) clubs and societies.
- 4.5.2** All courses are expected to have a significant Blackboard presence.
- 4.5.3** All current employees and students are automatically given Blackboard accounts. All persons affiliated with the University will use their network password to access Blackboard.
- 4.5.4** Access to Blackboard for persons not employed by or attending the University may be requested by members of the University community. Such a request must be approved by the Dean or Director of the relevant College/Department.

4.6 Email

- 4.6.1** All faculty, staff, and students are provided with official University email accounts for communication.
- 4.6.2** Users are expected to adhere to the University's email usage guidelines, which include maintaining the security of their accounts and using email for University-related purposes only.
- 4.6.3** Detailed rules and responsibilities regarding email usage are outlined in the Email Security Policy.

4.7 Password Security

- 4.7.1** Users must safeguard their credentials to prevent unauthorized access to University systems.
- 4.7.2** Password creation, management, and security requirements are outlined in the Password Security Policy.

4.8 Network Resources

- 4.8.1** Network resources include items such as internet bandwidth and shared or personal remote drives.
- 4.8.2** The University Information Technology Department (“**ITD**”) reserves the right to allocate resources in different ways in order to achieve maximum usage. To accomplish this, the system administrators may suspend or terminate privileges of individuals without notice if malicious misuse or use inconsistent with this policy or any other University policy is discovered. Privileges may also be suspended, without notice, to meet time-dependent, critical operational needs. System administrators may also limit the number of messages or files that each user has in order to keep the system functioning.
- 4.8.3** While ITD is responsible for monitoring the use of computer systems, it is also the responsibility of all individuals in the University to urge their peers and colleagues to use the network and systems appropriately. This is the only way that the integrity and availability of the network and systems can be ensured for everyone. Each member of the University community is responsible for using only those accounts or computers for which he or she has authorization and is responsible for protecting all passwords. Individual responsibility includes respecting the rights of other users and of copyright holders. Individuals are urged to report unauthorized use of computers, networks, or other computer service facilities on campus to the ITD.

5. Related Policies and Laws

- SUP-ITS-104 Acceptable Usage
- SUP-ITS-105 Internet Usage
- SUP-ITS-202 Internet Content and Management Control
- SUP-ITS-205 Password Security
- SUP-ITS-206 Email Security
- SUP-ITS-501 Electronic Learning Management System
- SUP-ITS-601 Equipment and Software Technical Support
- SUP-HR-11 Disciplinary Measures
- UNI-LEG-301 Copyright
- UNI-LEG-302 Intellectual Property

6. Administration

This policy is administered by the Client Services Unit, ITD.

7. Revision History

Date	Revision	Ver.
22 April 2025	Approved by the CAFO.	2.2
25 November 2024	Non-substantive changes: <ul style="list-style-type: none">• Updated the formatting.• Reworded the Email and Password Sections because the details are outlined in other policies.• Updated the Related Policies and Laws Section.	
11 February 2023	Administrative change: <ul style="list-style-type: none">• Updated the information header and policy numbers to be in line with the new format.• Updated the policy number from SUP-ITS-09 to SUP-ITS-101.	
27 April 2021	Non-substantive changes approved by the Vice-President as Acting CAFO.	2.1
6 January 2020	Updated the policy number to SUP-ITS-09 from ACA-INF-05.	
17 January 2018	Minor revisions approved by the President.	2.0
12 April 2007	New policy replacing ACA-INF-05 External Access to Blackboard approved.	1.0