


Category	IT Infrastructure and Services	Policy Number	SUP-ITS-101	 جامعة زايد ZAYED UNIVERSITY
Distribution	External	Version	2.1	
Responsible Office	CAFO	Policy Owner	IT Department	
Date Approved	27 April 2021	Effective Date	27 April 2021	
Date Last Reviewed	27 April 2021	Due Date for Next Review	27 April 2024	

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. Policy

3.1 Zayed University will be a leading institution in the effective use of information technology for the enhancement of student learning, university management, research and outreach.

3.2 The computing resources that Zayed 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.

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

- a) clear expectations and guidelines;
- b) adequate how-to training;
- c) ample professional development opportunities;
- d) prompt technical support;
- e) a fast and efficient network.

3.4 Violations

Violations of computing resource rules and policies may result in university disciplinary action, which may have serious consequences. Individuals who violate license agreements and copyright may be subject to legal action from external parties (publishers/vendors/copyright holders). 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. With prior notice and written warning, access to computing resources may be restricted by the university when actions interfere with reasonable use by other members of the university

community. In all cases, the individual will be notified of the reason and duration of the access restriction as soon as possible. Access will be restored when the situation has been resolved.

3.5 Blackboard

3.5.1 Blackboard is intended to support the teaching, learning and research of Zayed University faculty, staff and students and facilitate communication and the sharing of information and resources among the university community and beyond. Zayed 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;
- d) clubs and societies.

3.5.2 All courses are expected to have a significant Blackboard presence.

3.5.3 All current employees and students are automatically given Blackboard accounts. All persons affiliated with Zayed University will use their network password to access Blackboard. Access to Blackboard for persons not employed by or attending Zayed University may be requested by members of the Zayed University community. Such a request must be approved by a Dean or Director of a unit.

3.6 Email

3.6.1 Email is a key mechanism for official communication within Zayed University.

3.6.2 All faculty, staff and students are provided with an official Zayed University email account upon entrance to the university. Cancellation of this email account will occur once the association with the university has been severed. Any exception to keep an email address active requires Dean/Director approval.

3.6.3 Faculty, staff, and students are expected to check their email on a regular basis in order to stay current with university-related communications.

3.6.4 Users are expected to change their email password from the default setting immediately after the account has been received. This password should remain private.

3.6.5 There is no guarantee of privacy for email. In the event of complaints, it may be necessary for the university to view email communication.

3.6.6 Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of Zayed University or any unit of Zayed University unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer will be included unless it is clear from the context that the author is not representing Zayed University.

3.7 Mass Email

3.7.1 Mass mailings are defined as mailings to large groups of faculty, staff, and/or students. Only messages that pertain directly to university business are acceptable.

3.7.2 Students and student groups/organizations are prohibited from mass mailing faculty or staff directly. In order to send mass emails, individual students or

student groups/organizations may have the email sent through a representative from the Student Affairs Office.

3.7.3 Faculty and staff are expected to use this function with discretion.

3.8 Network Resources

3.8.1 Network resources include items such as internet bandwidth and shared or personal remote drives.

3.8.2 Zayed University Information Technology Department 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.

3.8.3 While the Information Technology Department is responsible for monitoring the use of computer systems, it is also the responsibility of all individuals in Zayed 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 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 Information Technology Department.

3.9 Password

3.9.1 The authentication mechanism that controls access to network resources is a user identification and password. User authentication is a means to control who has access to any network resource in Zayed University. Access gained by a non-authorized entity can cause loss of information confidentiality, integrity and availability that may result in loss of revenue, liability, loss of trust, or embarrassment to Zayed University.

3.9.2 The password procedures associated with this policy establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the Zayed University user authentication mechanism. To ensure a safe and secure network, it is essential that users follow defined network password security measures and protocols.

4. Related Policies and Laws

UNI-LEG-301 Copyright

UNI-LEG-302 Intellectual Property

5. Administration

This policy is administered by the Information Technology Department. Any questions can be directed to the Director of the Information Technology Department.

6. Revision History

Date	Revision
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.
15 April 2021	Added Internal Distribution
6 January 2020	Updated the policy number to SUP-ITS-09 from ACA-INF-05.
17 January 2018	Minor revisions and non-substantive changes approved by the President.
12 April 2007	New policy replacing ACA-INF-05 External Access to Blackboard approved.