# University of Balamand

## The Ethical Use of Information Technology Policy

**Title:** The Ethical Use of Information Technology Policy

**Document Type**: Public

**Policy Owner:** Office of the President, Office of the Provost, Office of Information Technology

**Applies to:** Every member of the UOB community

**Effective date:** Immediately

**For More Information, Contact:** Office of the Provost, Office of Information Technology

**Contact Information:** Provoffice@balamand.edu.lb

06-930-250 Extension: 1633, 1511 or 4357

**Official Website:** https://www.balamand.edu.lb/AboutUOB/Pages/University-Policies.aspx

---

## Background

The University of Balamand (UOB) recognizes the pivotal role that Information Technology (IT) resources play in achieving its mission, vision and core values. Hence, the need for a policy to ensure the ethical and responsible use of IT while respecting the confidentiality of information and the privacy of the user.

## Purpose Statement

The purpose of this policy is to establish principles for the responsible, ethical, and secure use of IT resources within the academic and working environment at UOB by fostering a purposeful digital environment that promotes academic integrity, adheres to university policies, safeguards intellectual property and respects privacy.

**Applies to:**

This policy applies to all students, faculty, staff, visiting professors, researchers, postdoctoral fellows, and contractors.

**Definitions**

1. **Information technology (IT):** refers to the use, development, and management of computer-based systems, software, and networks to store, process, transmit, and retrieve information.
2. **Privacy:** refers to the right of individuals to control the access, use, and disclosure of their personal information, protecting it from unauthorized access or misuse.
3. **Security:** refers to the measures and practices implemented to protect information and technology resources from unauthorized access, use, disclosure, disruption, or destruction.
4. **Responsible behavior:** refers to the actions and conduct expected from individuals using information technology resources, including respecting the rights and privacy of others, adhering to legal and ethical standards, and using technology in a manner that promotes a positive and safe environment.
5. **Intellectual property:** defined as creations of the mind, which can be the result of academic scholarship such as the development of textbooks, literary works, artistic creations, artifacts, as well as any creation covered by a patent or copyright and including trademarks or trade secrets.
6. **Data protection:** refers to the regulation and practices governing the collection, use, and safeguarding of personal data about individuals within the university community.
7. **Acceptable use:** refers to the agreed-upon guidelines and rules for the proper and responsible use of technology resources, ensuring compliance with legal, ethical, and organizational standards.
8. **Unacceptable use**: refers to actions or behaviors that violate established policies, guidelines, or rules regarding the use of information technology resources within a university.

9. **Unauthorized use:** refers to accessing or utilizing IT resources without proper authorization. This can include bypassing security measures, using someone else's credentials, or accessing restricted areas.
10. **Unethical use**: refers specifically to actions that violate ethical principles, although they may not explicitly be prohibited by university policies.

## Policy Statement

This policy provides a foundational framework for the use of UOB information technology resources. The policy encompasses the use of information, data, any equipment, electronic and computing devices, and network resources among other digital platforms employed in the pursuit of UOB business.

Specifically, the policy emphasizes the ethical and responsible IT practices within the following areas:

### 1. Authorization and Security

All devices connecting to the UOB network must receive proper authorization through the IT department and maintain up-to-date with anti-virus protection. The use of USB devices (flash drives, external hard drives) for storing or transferring data is allowed for university academic, administrative, or research purposes. However, users should ensure that their devices are free from malware or other security threats.

This policy prohibits the use of USB devices to transfer or store unauthorized or pirated software, the sharing of USB devices containing university confidential data with unauthorized individuals, and the neglectful handling of USB devices that could result in university data breaches or security incidents. Furthermore, this policy forbids users from circumventing or disabling user authentication or security mechanisms of any UOB system, network, or account. Nonetheless, users are responsible for the protection of their own authentication credentials.

**2. Data Encryption**

All sensitive or confidential data stored on USB devices must be encrypted to prevent unauthorized access or disclosure. Users are responsible for implementing appropriate encryption measures and ensuring compliance with data protection regulations.

**3. Responsible Resources Use**

Users must avoid intentional waste of UOB resources. Examples of waste include excessive paper printing, unauthorized mass mailings, and running programs in a loop. The policy regards responsible use of resources as a mechanism for environmental sustainability and operational efficiency at UOB.

**4. Personal Use and Commercial Gain**

Occasional and responsible personal use of the UOB IT resources is allowed, provided it does not significantly consume UOB resources, disrupt job performance, or violate this or other university policies or procedures. However, this policy strictly prohibits any use of UOB IT resources for commercial gain.

**5. Compliance with Legal and Ethical Standards**

Any use of UOB IT resources for any activity that is illegal under national or international law is strictly prohibited. Users must adhere to all relevant laws, regulations, and ethical standards, including UOB bylaws while utilizing UOB information technology resources. Any data collected or stored using USB devices must also comply with applicable privacy laws and University policies. Users must obtain a written consent and adhere to data retention guidelines when collecting or storing personal or sensitive information.

**6. Network Infrastructure Modification**

Users may not modify the existing UOB network infrastructure. Possible modifications that are prohibited include, but are not limited to, installing network devices such as hubs, switches, routers, network firewalls, and installing wireless access points to the existing UOB network.

### 7. Copyright Compliance

This policy strictly prohibits unauthorized copying and downloading of copyrighted material. Examples include digitizing and distributing copyrighted photographs, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which UOB or the end user does not have an active license.

### 8. Data Mining and the Use of Emerging Trends on Campus

Data mining activities on campus networks must adhere to ethical guidelines and respect user privacy. Researchers must obtain proper approvals before conducting data mining activities using university resources.

### 9. Reporting Incidents

Users are required to immediately report any theft, loss, or unauthorized disclosure of UOB proprietary information to the IT department. Prompt reporting is essential to mitigate the risk of data breaches and protect sensitive information. Faculty members should also report such incidents to their deans, while staff should report to their immediate supervisors or directors in addition to the IT department.

## Enforcement

UOB seeks to provide a secure, yet open, network that protects the integrity and confidentiality of information while maintaining its accessibility. Nonetheless, each member of the UOB community is responsible for the security and protection of university information and information resources to which they have control over and/or access. Thus, any breach in security or any suspected breach must be immediately conveyed to the IT department via a phone call and an email.

Failure to comply with this policy may result in disciplinary actions taken by the university leadership that may range from the revocation of IT privileges to legal pursuit.