INTERNET USAGE POLICY
of Saint Joseph University of Beirut

This Policy was approved by the University Board during its 223rd meeting on February 19, 2025

SCOPE

This Policy applies to all of the University staff, teachers and students.

ROLES

CISO (Chief Information Security Officer)

The CISO is responsible for developing and updating this Policy.

STI (IT Department)

The IT Department is responsible for the technical management of this Policy.

Table of Contents

DETAILS

1. Introduction

This Policy covers access to all Internet services that are provided by *Université Saint-Joseph de Beyrouth* (USJ – Saint Joseph University) hereunder referred to as 'USJ' or 'University' for the purpose of conducting and supporting official business activity through USJ's network infrastructure and all mobile devices.

This document describes how you may use the Internet when access is provided by USJ or as part of your work. It also outlines your personal responsibilities and informs you of what you must and must not do.

Access to the Internet from company devices is made available for the business purposes of USJ. A certain amount of personal use is permitted in accordance with the statements contained within this Policy.

It is acknowledged that it is impossible to define precise rules covering all Internet activities and adherence should be undertaken within the spirit of the Policy to ensure productive use of the Internet.

Non-compliance with this Policy could have a significant effect on the efficient operation of USJ and may result in financial loss and an inability to provide necessary services to our customers. If any user is found to have breached this Policy, they will be subject to disciplinary measures. If a criminal offense is considered to have been committed, further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this Policy or how it may apply to you, seek advice in the first instance from your immediate manager.

The following policies and procedures are relevant to this document:

- Acceptable Use Policy
- Electronic Messaging Policy
- Mobile Device Policy
- Software Installation Policy
- Social Media Policy

2. Internet Access Policy

2.1 Business Use of the Internet

Your Internet access must be used in accordance with this Policy for tasks reasonably related to your work including:

- Access to information and systems that are pertinent to fulfilling USJ's business obligations
- The capability to post updates to organization-owned and/or maintained websites and social media accounts
- An electronic commerce facility (e.g. purchasing equipment for USJ)
- Research

2.2 Personal Use of the Internet

USJ permits personal use of the Internet in your own time (for example during your lunch break), provided it does not interfere with your work. Any exception to this is at the discretion of your line manager.

USJ is not, however, responsible for any personal transactions you enter into - for example with respect to the quality, delivery or loss of items ordered. You must accept responsibility for, and keep USJ protected against, any claims, damages, losses or the like that might arise from your transaction, for example in relation to payment for items or any personal injury or damage to property they might cause.

2.3 Internet Access, Security and Monitoring

USJ will provide secure access to the Internet from your business device, a desktop computer or laptop for example. The IT Department is responsible for the technical management of this access.

You are responsible for the security provided by your account username and password. Only you must know your password and you must be the only person who uses the Internet whilst logged on with your account.

You must not use anyone else's user account to access the Internet.

The provision of Internet access is owned by USJ and all access is recorded, logged and interrogated for the purposes of:

- Monitoring total usage to ensure business use is not impacted by lack of capacity
- Monitoring all access for reports that are produced for line managers and auditors

2.4 Prohibited Uses of the Internet

Except where it is strictly and necessarily required for your work, IT audit activity or other investigations for example, you must not use the Internet access provided by USJ to:

- Create, download, upload, display or knowingly access, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive.
- Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files.
- Subscribe to, enter or utilize real-time chat facilities such as chat rooms, text messenger or pager programs.
- Subscribe to, enter or use online gaming or betting sites.
- Subscribe to or enter "money making" sites or enter or use "money making" programs.
- Run a private business.
- Download any software that does not comply with the USJ's Software Policy.

The above list gives examples of "unsuitable" usage but is neither exclusive nor exhaustive. "Unsuitable" material will include data, images, audio files or video files, the transmission of which is illegal, and material that defy the rule, essence and spirit of this and other organizational policies.

USJ will take steps to block the following categories of websites:

- Illegal
- Pornographic
- Violence
- Hate and discrimination
- Offensive
- Weapons
- Phishing
- Malicious proxies
- Gambling
- Dating
- Games

If you have inadvertently attempted to access such a site, you should inform the IT Department immediately.