



Bar-Ilan University

Policy on Usage of IT Resources

CONTENTS

1. Statement of Purpose	2
2. Rules of Use.....	2
User Ids and Passwords.....	2
Using Bar-Ilan University's Computing System	3
Linking up to the Computing System	4
Data and System Security	4
Major Data and System Security Guidelines	4
Proper Conduct on the Network.....	5
Criminal and Civil Violations	5
Inflammatory Publishing.....	6
Copyright and Licensing Violations	6
Mass E-mailings.....	6
Spamming.....	6
Commercial Activity	7
Databases Containing Personal Details.....	7
Distribution Lists.....	7
3. Guidelines to Web Site Construction.....	8
Accurate and Updated Data.....	8
Identifying the Content Provider.....	8
Data Security of the Web Site	8



1. Statement of Purpose

- This document defines Bar-Ilan University's policy regarding the use of the University's Information Technology resources. It applies to the University's academic and administrative staffs, students, as well as to anyone having access to these services via Bar-Ilan University.
- Bar-Ilan University provides IT facilities, including LAN networks, access to the Internet, servers, computerized labs and classrooms. It does so in order to advance the University's objectives and to support teaching, research, community services and administrative processes – in accordance with the University's unique character. All computing activity must be consistent with these purposes. Users and Webmasters are equally bound by all existing University policies and the law.
- This document is accessible to the public, so that lack of knowledge cannot be claimed as a reason for failing to adhere to the policy.
- Bar-Ilan University's IT resources are available only to those who have received the proper authorization.
- All users of Bar-Ilan University's computers and infrastructures are obligated to act in accordance with the University's procedures as delineated in this "Bar-Ilan University Policy on Usage of IT Resources" document, to adhere to the policy and comply with the rules. Breaking these rules comprises a disciplinary violation; additionally, it may also be a criminal or civil offense.

Bar-Ilan University reserves the right to revoke use of computer resources if these resources are misused or abused.

2. Rules of Use

User Ids and Passwords

A user id is granted to an individual. That individual is solely responsible for any use made of the user id account.

It is a violation of policy to use a computer user id that is not assigned to that individual or to share the personal user id with others.



- Access to Bar-Ilan University's computers requires a user id and password. A secure password must be used (for instructions, see: [Secure Passwords](#)).
- Regulations require users to change their passwords at least once every six months. Any attempt to crack another person's password is strictly forbidden.
- Users may access only Bar-Ilan University computers or networks, to which they have received authorization. They may not access or attempt to access computerized systems for which they have not received authorization.

Using Bar-Ilan University's Computing System

- Do not try to render the computing system inoperative in any way.
- Eavesdropping on network traffic in any way, is not permitted. Only individuals who have received specific authorization to do so from the Data and Systems Security Manager, may "sniff" traffic on the network.
- The University's computing equipment is intended for University purposes only.
- The main computer room and telecommunication equipment storage closets located throughout the University are out of bounds. Entry is allowed only to authorized Center for IT Infrastructure & IS employees.
- Every new project or computer system must receive permission from the Committee for Systems Security, while still in the planning stage. The Committee, headed by the Data and Systems Security Manager, meets for the purpose of studying the project and granting authorization. The meeting is attended by a regular panel of CITIS experts, and the University representatives initiating and heading the project. To request a meeting, please download the following form: [Requesting a Meeting of the Committee for Systems & Data Security](#).



Linking up to the Computing System

- A computer or any other piece of communication equipment may not be linked up to the network without the written approval of a CITIS, Dept. of Communications and Networking, authorized representative.
- To link a laptop to the University network, the user must fill in the following form: [Laptop User's Network Connection Commitment Form](#) and give it to his department's computer support person.

Data and System Security

Virus attacks, spam mail, spyware and other threats to public and private computer systems have become increasingly widespread. The following instructions were written for all the University's computer network users, for the purpose of coping with these threats.

These dangers can enable negative elements to steal personal information, individual identities, and malign the reputation of the individual, the University, or its institutions.

Major Data and System Security Guidelines

- The user is solely responsible for his/her personal computer. He/she must act in accordance with the instructions publicized by the University, and ensure that the level of security of his/her computer is satisfactory.
- The user will carry out a virus check on all media (such as disks, CDs and USB flash drives) before connecting it to the computer.
- The user will comply with security rules publicized on the University web site.
- The user may not install software that enables someone else to gain control over his/her computer. If technical support is required, the University Customer Support personnel may install such software, upon receipt of the user's authorization. In special cases in which the user would like to install such software, he/she must receive written authorization to do so from the University Data and Systems Security Manager.



- University policy requires every user to shutdown his computer at the end of the workday. This rule serves 2 purposes:
 1. Increased data and system security, by preventing an attack on the computer while on;
 2. Energy saving.

Note: To prevent the possibility of forgetting to turn off the computer at the end of the workday, we recommend installing an automatic shutdown program. "Poweroff" is an example of such a system. Information and instructions can be found at the following links: (pre Win 7) [Poweroff Instructions](#) or: [Automatic Shutdown - Windows 7](#) .

Proper Conduct on the Network

Users must abide by acceptable rules of conduct on the Internet, known as "Netiquette", as can be found in [The Core Rules of Netiquette](#).

Criminal and Civil Violations

- Users may not exploit Bar-Ilan University's computing resources in violation of the law.
- Bar-Ilan University computing resources may not be used to support any illegal activity. Examples may include: drugs, gambling, pornography, prostitution, theft, spreading computer viruses, code cracking software, violating software licenses, illegal credit card trade and crimes.
- Infringements include, but are not limited to: violation of personal privacy, vandalism and pranks that incapacitate, compromise or destroy University resources and/or violate State laws; use of the network to send/receive a message that is inconsistent with the University's "Policy on Usage of IT Resources", as defined above.
- Furthermore, it is forbidden to connect to servers that violate these laws.
- The above is a generalized description and applies to any violation of the law. For purposes of illustration, and without adding to, or detracting from the above, a number of issues are detailed below. They require particular vigilance by users.



Inflammatory Publishing

- Without detracting from the generality of the above-mentioned, users, authors and webmasters must abide by the laws relating to libel.
- Users and webmasters must adhere to existing laws forbidding the defamation of others. Writing, displaying or transmitting incitement, threatening or racist material, or material that includes obscene or threatening language, are strictly forbidden. Users are particularly warned against sending provocative messages, whether political or otherwise. Those in doubt regarding specific material (as to whether or not it can be considered as incitement) must check with the University's Data and Systems Security Manager.

Copyright and Licensing Violations

- It is forbidden to use material displayed on the Internet and protected by copyrights or any other type of license, without receiving the prior consent of the author or other authorized body.
- Software that has not been legally purchased, or without permission of the lawful owners of the rights, may not be installed on the computer.
- One may transfer files only for administrative, academic or research purposes. The use of file sharing software, such as KaZaa, eMule, BitTorrent and the like, is forbidden.

Mass E-mailings

- Use of Internet resources is permitted within the University, or via dial-up access services from home, so long as such use does not disrupt, or distract from the proper, continuous management of the University's needs.

Spamming

- The term spamming refers to sending mail that is unwanted or has not been requested, to a single user or to multiple users. The mail may deal with any topic. As long as the addressee did not request it or did not leave his/her address for use, this mail is covered by the term spamming, which is forbidden by law. Needless to say, Bar-Ilan University's "Policy on Usage of IT Resources" forbids spamming.



- In keeping with the changes made to the Communication Law, the Knesset approved an amendment that "prohibits the delivery of advertisements using mobile text messaging, email, fax or automatic dialing systems without first obtaining the recipient's explicit written consent." (Link to: [Amendment to Communications Law, 2008](#) .)
- The University's policy in this regard, was outlined in letters sent by the offices of the Director General and Legal Advisor. The changes in the law are of particular importance to University information providers and database users.

Commercial Activity

- Use of computing resources, and the Internet in particular, for personal financial gain, including commercial advertising, is strictly forbidden, unless authorized by the University management.
- The University's name may not be used for advertising purposes, nor can its name be indicated as a user of any product or service, or as a source of research information upon which a commercial program or advertisement is based, unless authorized by the University management.

Databases Containing Personal Details

- Users are required to protect privacy. Users who manage, maintain or have access to databases containing personal information (personal details alongside names and/or ID numbers) may not lawfully transfer this information (in whole or in part) to any other person or body, other than as defined in the Privacy Law.
- A user in doubt as to whether or not the Privacy Law applies to specific material, must check with the University's Data and Systems Security Manager.

Distribution Lists

- Anyone receiving a distribution list must undertake to use it only within the framework of his/her function, and for the purposes for which the list had been prepared.



3. Guidelines to Web Site Construction

Accurate and Updated Data

To remain functional over time and to present an image consistent with Bar-Ilan University's position as an academic institution, information must be timely and accurate. Content providers are responsible for periodic reviews of the information contained (at least once a year), and revising content based upon relevancy, accuracy, and accessibility.

Identifying the Content Provider

The content provider must identify him/herself on the web site. Departments and/or organizational units and users are responsible for the information they disseminate via the Internet. Each page shall also list the most recent date on which the information was modified.

Data Security of the Web Site

All webmasters responsible for web sites must ensure the data and system security of their computers. Access to the site from outside the University will only be permitted after receipt of a commitment regarding security from the webmaster. (See: [Instructions and Commitment Form for New Web Site on a Dedicated Computer](#) .)

This document was prepared by Data and Systems Security – Center for IT Infrastructure & IS, in coordination with the Office of the University Legal Adviser.

Updated: November 8, 2011