Bar-Ilan University

Policy on Usage of ICT Resources

1. Statement of Purpose

- This document defines Bar-Ilan University's policy regarding the use of the University's Information and Communication Technology (ICT) resources. It applies to the University's academic and administrative staff, students, as well as to anyone having access to these services via Bar-Ilan University.

- Bar-Ilan University provides ICT facilities, including local 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, except the Free Wi-Fi network.

- All users of Bar-Ilan University's computers and infrastructures, including the Free Wi-Fi network, are obligated to act in accordance with the University's procedures as delineated in this "Bar-Ilan University Policy on Usage of ICT 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 UserId is granted to an individual. That individual is solely responsible for any use made of the UserId account.

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

- Access to Bar-Ilan University's computers requires a UserId and Password. A secure password must be used (for instructions, see the "Good Password" appendix below).
- 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 ICT Division employees.

Introduction of new ICT systems and projects to Bar-Ilan University

- Every new computing 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 ICT division staff experts, and the University representatives initiating and heading the project. To request a meeting, please contact the Data and Systems Security Manager.

Linking up to the Computing System

- A computer or any other piece of communication equipment may not be linked up to the campus network without the written approval of a ICT Division authorized representative (except standard equipment listed and approved by the Purchasing Department).

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.

- 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. This should be accomplished by installing current security updates to the Operating System and the Anti-Virus software, by the user itself or by the competent support teams.

- The user will carry out a virus check on all mobile media (such as mobile disk drives and USB flash drives) before connecting it to the computer.

- 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 authorization to do so from the University Data and Systems Security Manager.

- The user will comply with security rules publicized from time to time by the University.

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 or publish links 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.

Incitement 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 Legal Advisor office.

Copyright and Licensing Violations

Copyright is one of the intellectual property rights. The court treats copyright as a basic human right and aggravates the punishment for violating it. The "Copyright Law 2007" allows for a claim for compensation of up to NIS 100,000 for any infringement of copyright, without proof of damage. Therefore:

- Any material appearing on the Internet - such as a picture, photo, article, book, song, website, YouTube video, Facebook post, app, game, software code, graphic design - should be treated as copyrighted or licensed material, and may not be used without prior permission from 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.

Massive use of Network or Internet resources

- Use of Network or Internet resources of the University is permitted within the University, or via remote access, as 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 (nr. 40 from 2008) 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."

- 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 Information Details

The University operates in accordance with the Privacy Protection Law-1981 and the regulations amended following it, the Privacy Protection (Information Security) Regulations, 2017.

The University's databases containing personal information are registered with the Registrar of Databases at the Ministry of Justice and a database administrator is appointed for each of them.

- Users are required to protect privacy. Users who manage, maintain or have access to databases containing personal information 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 or with the Data Protection Officer.

Distribution Lists

- Anyone managing or being a member of 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.

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 site operator.

Accessibility for the Handicapped

By law, any information site that provides a service to the public must be accessible to handicapped people.

In addition to making the site configuration accessible, its content must be accessible, including all documents on it (PDF, Word, etc.)

This document was prepared by Data and Systems Security – ICT Division, in coordination with the Office of the University Legal Advisor.

Updated: December 28, 2020

"Good password" Appendix

- Must be in English letters
- At least 8 characters long
- Must include at least one digit
- Must have at least one lowercase character
- Must include at least one uppercase character
- Do not include more than two identical characters
- Do not include part of your name or username

The site for resetting and changing a password at your own service:
https://sspr.biu.ac.il/sspr/public/ForgottenPassword