WEBSTER UNIVERSITY – ACCEPTABLE USE POLICY

Responsible Office: Information Technology
Last Updated: 01-25-2019

Webster University
Acceptable Use Policy

Policy Purpose

Webster University ("Webster") provides numerous information technology resources for use by the Webster community to support its educational mission. The use of these resources must be consistent with the goals of the University. This policy applies to all "users" of computing resources owned or managed by Webster University, including (but not limited to) Webster University faculty, staff, students, alumni, guests, agents of the administration, as well as external individuals and organizations accessing Webster's services and resources. Students, staff, administrators, faculty and others granted use of Webster University's computer network resources.

We encourage members of the Webster community to use Webster's information technology resources and online networks for Webster University educational and business purposes under the appropriate circumstances. While these resources help the university function, they also require responsible use from every user. Webster University users' actions can affect people all around the world. Therefore, users must use these technologies responsibly and with respect. Users are expected to follow Webster's guidelines, policies, and procedures in utilizing information technology and electronic networks accessed by such technology.

Definitions

For purposes of this policy the following definitions shall apply:

Approved Webster University devices shall mean computers, mobile devices and any other Webster University technology assets purchased by the information technology department and/or the University.

Electronic Communications shall mean and include the use of information systems

in communicating or posting information or material by way of messages, email, bulletin boards, the Internet, World Wide Web, or other such tools.

Information technology resources include computers, computer services, servers, and similar devices provided or administered by Webster and for which Webster is responsible. Information technology resources also include access to Webster's on-campus network, the Internet, World Wide Web and other online computer networks.

Networks shall mean and include video, voice and data networks, routers and storage devices.

Other shall include Webster guests and/or those who may use Webster University facilities for a specific event or period of time and are given specific technology access.

Personal Data is any information that relates to an **identified or identifiable living individual**. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data. Personal data that has been de-identified, encrypted or **pseudonymised** but can be used to re-identify a person remains personal data and falls within the scope of this definition.

Pseudonymisation is a process that takes the most identifying fields of personal data within a database and replaces them with artificial identifiers, or pseudonyms. For example, a name is replaced with a unique number. The purpose is to render the data record less identifying and therefore reduce concerns with data sharing and data retention.

Sensitive Data is any data that reveals: Racial or ethnic origin; Political opinions; Religious or philosophical beliefs; Trade union membership; Genetic data; Biometric data for the purpose of uniquely identifying a natural person; Data concerning health or a natural person's sex life and/or sexual orientation

Users shall mean all of Webster University's faculty, staff, students, alumni, guests, agents of the administration, as well as external individuals and organizations accessing Webster's services and resources.

Access and use

The following guidelines apply to all Users:

- Users may not use another individual's account or passwords. Password and account sharing are prohibited. Users are accountable for all activity associated with their user ID and password. Users must never share their login credentials with any other person.

- Users may not use Webster's computer resources for any illegal or criminal purpose.

- The transmission and/or posting of personal and/or sensitive data may only proceed if the individual who owns the personal and sensitive data has given authorization to do so.

- The university is bound by its contractual and license agreements respecting certain third-party resources: users are expected to comply with all such agreements when using such resources.

- If a user learns of a potential breach in the security of Webster's information technology resources, the user must report the potential security breach immediately to the Information Security Office at iso@webster.edu.

- Webster's information technology resources and networks shall not be used to gain unauthorized access to any computer, computer service, server or similar device, network, website, storage device or restricted data base(s).

- No one shall alter or delete software, hardware, communications, or data belonging to someone else without authorization. Users are prohibited from using or making unauthorized copies of software.

- The use of invasive software or malicious code is prohibited.

- Users must notify Webster University of any theft, loss, unauthorized access detection or similar Webster owned or of a personally owned computing device containing data or software application licenses belonging to Webster University. Users must cooperate with Webster University and its efforts to retrieve or protect any Webster University data or software on such Webster owned or personally owned computing device(s).

- Webster understands that users may want to download or install certain software onto approved Webster University devices to facilitate the user's ability to communicate or to perform his or her duties and responsibilities. In order to protect Webster's information technology resources, networks and devices, Webster must ensure that software downloaded or installed onto approved Webster University devices is safe, compatible and appropriate for use. For this reason, users must not knowingly download or install software onto approved Webster University devices unless allowed under applicable procedures or prior authorization has been received from the Office of the Chief Information Officer or designee. Users may complete the Request for Non-Standard Software and submit it to the Office of the Chief Information Officer.

- Using Webster's information technology resources to post or transmit sexually explicit images or any other content deemed to be offensive and inappropriate for academic use is prohibited. In addition, viewing, posting or transmitting sexually explicit material or any other content deemed to be offensive and inappropriate for academic use may constitute a violation of the Webster's *Policy on Sexual Assault, Harassment and Other Offenses* as discussed in the Civility and Liberty section below.

Acceptable Email Usage

- It is strictly prohibited to forward information that contains confidential or proprietary information to any personal email accounts, servers, storage media, mobile devices and other electronic systems. Confidential or proprietary information sent on behalf of Webster University to any third-party must follow Webster's privacy and security policies on the handling and transmission of protected information.

- Staff and full-time faculty may NOT forward their email to a non-Webster account. Staff and full-time faculty may forward their Webster email account to a third party email system that is operated by Webster University or is a part of the Webster University domain. For example, someone in Leiden may forward his/her *@webster.edu* email account to their *@webster.nl* account.

- Employees, staff, faculty and adjunct faculty are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct University business, to create or memorialize any binding transactions, or to store or retain email on behalf of the University. Such communications and transactions should be conducted through proper channels using University approved documentation.

- Sending chain letters or joke emails from a University email account is prohibited.

Civility and Liberty

Webster seeks to protect the civil, personal, and property rights of those properly using its information technology resources and seeks to protect the confidentiality of Webster's records stored electronically. Conduct which involves use of Webster's information technology resources to violate another's rights is subject to disciplinary action.

As an academic institution, we are committed to supporting the academic freedom of all members of the Webster community; as a social institution, we are committed to respecting the dignity of all members of our community. The standards and principles of intellectual and academic freedom developed for university libraries apply to

material received via computer news networks and by similar means. The standards of intellectual and academic freedom developed for faculty and student publication in traditional media apply to computer-generated publication.

There will be situations in which what one person understands to be free expression another person takes to be harassment, personal assault, or an assault on prevailing standards of decency. The Report of the Committee on Freedom of Expression at Yale University (January 8, 1975), states:

Shock, hurt, and anger are not consequences to be weighed lightly. No member of a community with a decent respect for others should use, or encourage others to use, slurs and epithets intended to discredit another's race, ethnic group, religion, or sex. It may sometimes be necessary in a university for civility and mutual respect to be superseded by the need to guarantee free expression.

The values superseded are nevertheless important, and every member of the university community should consider them in exercising the fundamental right to free expression. We have considered the opposing argument that behavior which violates these social and ethical considerations should be made subject to formal sanctions, and the argument that such behavior entitles others to prevent speech they might regard as offensive. Our conviction that the central purpose of the university is to foster the free access of knowledge compels us to reject both of these arguments. They assert a right to prevent free expression. They rest upon the assumption that speech can be suppressed by anyone who deems it false or offensive...They make the majority, or any willful minority, the arbiters of truth for all. If expression may be prevented, censored, or punished, because of its content or because of the motives attributed to those who promote it, then it is no longer free. It will be subordinated to other values that we believe to be of lower priority in a university.

The conclusions that we draw, then, are these: even when some members of the university community fail to meet their social and ethical responsibilities, the paramount obligation of the university is to protect their right to free expression. If a university's overriding commitment to free expression is to be sustained, secondary social and ethical responsibilities must be left to the informal processes of suasion, example, and argument.

Just as nothing in the present policy is to be understood as excusing users from compliance with federal or state law, nothing in this policy should be understood as withdrawing Webster's affirmation of statements in faculty and student policy handbooks in support of academic and intellectual freedom.

None of this, though, denies that harassment on the basis of sex is a violation of Title VII of The Civil Rights Act of 1964 and is also prohibited under Title IX of the Education Amendments of 1972. Webster's *Policy on Sexual Assault, Harassment and Other Offenses* defines sexual harassment as:

Unwelcome sexual advances, requests for sexual favors, and other verbal or physical

contact of a sexual nature constitutes sexual harassment when 1) submission to such conduct is made either explicitly or implicitly a term or a condition of an individual's employment or education or 2) submission to or rejection of such conduct is used as a basis for employment or academic decisions affecting that individual or 3) such conduct has the purpose or effect of unreasonably interfering with an individual's work or academic performance or of creating an intimidating, hostile, or offensive educational or employment environment.

Webster expects that users will respect the rights of others to freedom from harassment or intimidation. A user may violate this policy if he or she transmits or posts abusive or unwanted material causing the work or academic experience of others to be disrupted. In addition, a user violates this policy and may violate the law if he or she targets another person, group or organization to cause distress, embarrassment, injury, unwanted attention or other substantial discomfort. Webster's sexual harassment policy prohibits users from displaying sexually graphic materials that may interfere with the work or academic pursuits of members of the Webster community. Due to the public nature and/or location of some of Webster's computers, viewing and/or distributing sexually graphic or offensive materials may be a violation of University policy. Webster's information technology resources and systems are Webster property. Webster may override individual passwords and access electronic communications transmitted via its information technology resources and systems at any time.

Electronic communications, instant messages, or other information on Webster's computers and email systems are not private or confidential. Webster retains the right to retrieve, read and publish any information or message in its information technology resources and email systems. Deletion of electronic communications and information by individuals does not necessarily remove such messages form the system and, in some cases, deleted information and emails may still be accessed after deletion by an individual user. Accordingly, the use of Webster's information technology resources and systems should be prudent and consistent with the work and academic pursuits of Webster.

In the course of a legal matter and/or security incident investigation, the university reserves the right to inspect a personally owned computing device that may access or may maintain sensitive university data.

The University is not responsible for unofficial uses of computer resources. In particular, electronic communications, email and personal Web pages often express private opinions which do not reflect University positions.

Property

University computing and information resources are made available to individuals to assist in the pursuit of educational and other academic goals. It is expected that users will cooperate with each other and respect the ownership of work and information even though it is in electronic-- rather than more immediately tangible--form. Individuals and

organizations will be held no less accountable for their actions in situations involving computers and information resources than they would be in dealing with other media. Rules prohibiting theft and vandalism apply to software and data as well as to physical equipment. In particular:

- The purchase and/or installation of hardware, software and/or related devices connected to Webster University technology environment is specifically prohibited.
- Users must adhere to posted lab and system policies, procedures, or protocols, such as time or storage limits, where those policies, procedures, or protocols are consistent with this policy. Refusal may constitute failure to comply as defined in the Code of Student Conduct.
- Using Webster's information technology resources to damage or disrupt, or to attempt to damage or disrupt the operation of computer equipment, data communications equipment, or data communications lines is prohibited.

Privacy and Personal Rights

Webster seeks to protect the civil, personal, and property rights of those properly using its information technology resources and seeks to protect the confidentiality of Webster's records stored electronically. The University does not access information created and/or stored by individual user on its IT systems except when it determines that it has a legitimate operational need to do so. The University has the legal right to access, preserve and review all information stored on or transmitted through its electronic services, equipment and systems. Conduct which involves use of Webster's information technology resources to violate another's rights is subject to disciplinary action.

- All users of the university's computing resources are expected to respect the privacy and personal rights of others. The use of computing resources to libel, slander, or harass any other person is not allowed and could lead to university discipline.

- Electronic communications, instant messages, or other information on Webster's computers, email and web services are not private or confidential. Webster retains the right to retrieve, read and publish any information or message in its information technology resources and systems. Deletion of electronic communications and information by individuals does not necessarily remove such messages from the system.

- Use of Webster systems for non-Webster purposes, such as running an independent business, or volunteer work for some other organization, absent written authorization from an employee's supervisor may constitute theft of computer time. Activities by students related to their coursework or to the work of chartered student organizations, and by faculty or staff related to their contractual obligations are explicitly authorized by this policy

- Use of I.T. Systems, even when carried out on a privately-owned computer or other device that is not owned, managed or maintained by Webster University, is governed by this Acceptable Use Policy.

- In the course of a potential or ongoing legal matter, a security incident investigation and/or an internal University investigation, the University reserves the right to inspect a personally-owned computing device that may access or may contain sensitive and/or proprietary data. Documents must not be destroyed by the current University document destruction process currently in effect. They must instead be brought to the attention of the University Secretary and then properly secured.

Adherence with Federal, State, and Local Copyright Laws

A user of Webster's computing and network resources must:

- Abide by all applicable copyright laws and licenses. Webster University has entered into legal agreements or contracts for many of our software and services which require each individual using them to comply with those agreements.
- Observe the copyright law as it applies to music, videos, games, images, texts and other media in both personal use and in production of electronic information.
- Do not use, copy, or distribute copyrighted works (including but not limited to Web page graphics, sound files, film clips, trademarks, software and logos) unless there is a legal right to use, copy, distribute, or otherwise exploit the copyrighted work.

Adjudication

Violations of this policy could be subject to disciplinary action including, but not limited to, reprimand, discharge, denial of access privileges, probations, academic expulsion and/or legal action.