October 2011

8.101 Acceptable Use of Electronic Resources

Type of Policy ■ ***University*** □ ***Campus*** □ ***Department/Unit*** □ **Interim**	**Acceptable use of Electronic Resources** **Policy 8. 101**
Information Technology Policies	**Effective date: June 7, 2008**

Policy History:	Approved by:	Resolution #	Date
Approved	Board of Governors	6.7.08:5	June 7, 2008
Revised	Chancellor	N/A	June 5, 2015
Revised (Non-substantive)	Office of University Counsel	N/A	May 31, 2017
Responsible Office	Responsible Administrator:	Contact information	Applies to:
University Chief Financial Officer	University Chief Financial Officer	937-769-1304	All Faculty , Visiting Faculty, Staff , Students and all external persons or organizations and individuals accessing external network services, such as the Internet and Intranet.

I. Introduction and Purpose

Antioch University (AU) values technology as a means of communicating information and ideas to the AU community and the world. In keeping with AU's commitment to utilizing technology in teaching and learning, this policy provides direction in the appropriate use of all forms of electronic resources. This document articulates the AU Policy on Acceptable Use of Electronic Resources, provides example violations, and outlines procedures for reporting policy violations.

II. Scope

This policy applies to use of all electronic resources utilized, owned, managed, or contracted by AU including, but not limited to:

A. Networks – The complete mechanism by which computers and peripherals are connected including connections to the Internet.

B. Computers – All computers including desktop and laptop computers assigned to individuals or available for shared use, and computers that are used for hosting applications and/or data in a central location (commonly referred to as servers),

C. Software – Any software whether it is loaded on a desktop or laptop computer or on a server.

D. Data – Any data stored on the networks or computers described above, or data utilized or owned by AU stored on portable devices or other media.

III. Persons Covered by this Policy

This policy applies to all users of electronic resources utilized, owned, managed, or contracted by AU including, but not limited to: AU faculty and visiting faculty, staff, students, external persons or organizations and individuals accessing external network services, such as the Internet and Intranet.

IV. Access

A. Access to computing resources and network capacity is a privilege generally available to all AU faculty, staff, and students. Access may also be granted to individuals outside AU for purposes consistent with the mission of AU; however, there will be no anonymous access allowed to any electronic resources.

B. In general:

1. Faculty and staff are given access to computing resources (e.g. email accounts as well as financial, human resources, and student information systems) once they have been offered and accepted a position and set up as employees in the University's human resources information system. Access is revoked when an employee no longer holds a position with AU. The level of access they are granted depends on their role within AU and may vary during their employment.

2. Students are given access to computing resources (e.g. email account, learning management system account) when they have applied and have been accepted at AU and their status has been entered into the University's student information system. Student access is revoked when they are no longer a student, except when a student graduates. Alumni access to email accounts will not be revoked.

C. The above paragraphs are the general rules for granting access to AU computing resources. More specific rules may be found within Policies or Procedures dealing with specific resources (e.g. the Email Policy). There may also be exceptions to the general rules which will be handled on an individual basis, for example, when people need accounts created before their status has been entered into the human resources information system (e.g. adjunct faculty who often need access before their contracts are finalized).

V. General Policies

A. While the use of AU electronic resources may be a requirement for coursework and work, access and use may be restricted or revoked in cases of misuse or repeated abuse.

B. AU reserves the right to limit access to its electronic resources when applicable AU policies, state and/or federal laws or contractual obligations are violated.

C. AU does not, as a rule, monitor the content of materials transported over AU's network or information posted on AU-owned computers and networks, but reserves the right to do so. Although AU does not typically block access to online content, it reserves the right to do so in cases where online content or activity diminishes the capacity of the AU network, where there is a threat to AU or its core academic mission, or where there is a reasonable cause to suggest a violation of AU or campus policy or local, state, or federal laws.

D. AU provides reasonable security against intrusion and damage to files stored on the central computing facilities, but does not guarantee that its computer systems are secure. AU is not responsible for unauthorized access by other users, nor does AU guarantee protection against media failure, fire, floods, or other natural or man-made disasters.

VI. Censorship

A. Free expression of ideas is central to the academic process. AU computer system administrators will not remove any information from individual accounts unless the system administrator finds one or more of the following:

1. The presence of the information involves illegality (e.g., copyrighted material, software used in violation of a license agreement).

2. The information in some way endangers computing resources or the information of other users (e.g., a computer worm, virus, or other destructive program).

3. The information is inconsistent with, interferes with, or disrupts the mission, policies, or functions of the University.

4. The information involves the use of obscene, bigoted, or abusive material, or is intended to harass or defame another individual.

B. Users whose information is removed will be notified as soon as is feasible, unless such notice is contrary to the interests of AU.

VII. Institutional Purposes

A. AU electronic resources and network capacity are provided for purposes related to AU's mission of education, research, and public service. All users will access electronic resources and network capacity primarily for purposes related to studies, instruction, the discharge of duties as employees, official business with AU, and other AU-sanctioned activities. Incidental personal use of electronic resources and network capacity is allowed only if that use does not interfere with the primary purpose of the system, does not interfere with the individual's primary job function, and does not cause any appreciable additional or direct cost to AU.

B. The use of AU computing resources and network capacity for personal monetary gain or commercial purposes is not permitted without prior written permission from the Vice Chancellor for Administration/CFO.

VIII. Security

A. Federal, state, and other governmental departments, entities or agencies (hereinafter, "agencies") impose independent conditions on Antioch University and Antioch University employees for access to and utilization of electronic resources. Antioch University employees who are granted access to any federal, state, or other governmental electronic resources (including but not limited to the Title IV Federal Financial Aid National Student Loan Data System (NSLDS), the Common Origination and Disbursement system (COD), and the Financial Aid Administrators Access to Online Central Processing System (CPS)), must comply with all conditions of access to and utilization of those resources as imposed by the relevant agency, in addition to complying with the requirements of Antioch policy. Violation of conditions of access to or utilization of electronic resources is a serious matter and may adversely impact the employee, the campus, and the entire University. Any employee in violation of this policy and/or the conditions of access to and utilization of federal, state or governmental resources is subject to University disciplinary sanctions, up to and including immediate termination of employment, and is subject to sanctions from the agency, including possible fines and prosecution.

B. The user is responsible for maintaining the security and confidentiality of information stored on relevant systems and computers. For example:

1. Users must not share computer accounts, passwords, and other types of authorization assigned to them with others.

2. The user should select account passwords that cannot be easily guessed or "cracked." Passwords should be changed regularly or immediately if the user feels the password may have been compromised.

3. For sensitive information on computers and systems, the user should supplement security with additional passwords or encryption.

4. The user should be aware of computer viruses and other destructive computer programs, and take steps to avoid them or passing them on to others.

C. Portable electronic devices such as laptops, PDAs or flash drives must not be used for storing confidential information about individuals (especially social security numbers) unless that information is encrypted.

IX. Lawful Usage

Computing resources and network capacity may not be used for unlawful purposes. Examples of unlawful purposes include but are not limited to:

A. Intentional harassment of other users.

B. Intentional destruction of or damage to equipment, software, or data belonging to AU or other users.

C. Intentional disruption or unauthorized monitoring of electronic communications.

D. Unauthorized copying of copyrighted material.

X. Ethical Usage

Computing resources and network capacity should be used in accordance with the high ethical standards of the AU community. Examples of unethical use, some of which may also be unlawful, include but are not limited to:

A. Violations of computer system security.

B. Unauthorized use of computer accounts, access codes, or network identification numbers assigned to others.

C. Intentional use of computer systems in ways that unnecessarily impede the computing activities of others (e.g. randomly initiating interactive electronic communications or e-mail exchanges, or overuse of interactive network utilities).

D. Use of computing facilities for private business purposes unrelated to the mission of AU or University life.

E. Academic dishonesty (e.g. plagiarism, cheating).

F. Violation of software license agreements.

G. Violation of network usage policies and regulations.

H. Violation of another user's privacy.

XI. Facilitative Usage

AU computer users can facilitate computing in the AU environment in many ways. Collegiality demands the practice of facilitative computing. Users should practice good stewardship of resources in the following ways:

A. Regular deletion of unneeded files from workstations and systems.

B. Refraining from overuse of connect time, information storage space, printing facilities, or processing capacity.

C. Refraining from overuse of network capacity.

XII. Copyrighted Material and File Sharing

A. AU's systems and networks cannot be used to copy, store, display, or distribute copyrighted material in any medium, or to prepare derivative works of such material, without the express permission of the copyright owner, except as otherwise allowed under copyright law. In addition to sanctions by the institution, copyright violators could be subject to felony charges under state and federal law and may be sued by the copyright holder.

B. Under copyright law, unless you have express permission from the copyright holder to engage in the copying, downloading, and sharing of files, you are in violation of the law. Peer-to-peer programs have no provision to acquire permission. In practice, therefore, the use of peer-to-peer programs for downloading music and movies may put users in violation of AU's policy and the law.

C. AU does not intend to block peer-to-peer file-sharing programs, nor does it monitor the content of network traffic. However, Information Technology Services (ITS) does monitor traffic patterns in order to guarantee acceptable network performance for all users. If ITS becomes aware of policy violations or illegal activities in the course of investigating network congestion or determining problems, it will investigate by inspecting content stored or shared on its network.

D. This policy also prohibits activities that interfere with the ability of others to use AU's computing resources or other network-connected services effectively. This may apply to peer-to-peer file-sharing programs irrespective of copyright violations, as these programs consume huge amounts of network resources.

XIII. Sanctions

Violation of the policies described above for legal and ethical use of computing resources will be dealt with seriously. Violators will be subject to the normal disciplinary procedures of AU. Violations may result in the loss of computing privileges as well as other sanctions, up to and including immediate termination of employment. Illegal acts involving AU computing resources may also be subject to prosecution by state and federal authorities.

XIV. Reporting and Response to Violations

Members of the AU community who believe they have witnessed or been a victim of a violation of the AU Policy on Acceptable Use of Electronic Resources should file a complaint with the appropriate AU office as follows:

A. Students and faculty members should report suspected violations of this policy to the Academic Dean or Chief Academic Officer (CAO) on their campus. Staff should report violations to their supervisor.

B. If the campus Provost determines that a violation may have occurred, the circumstances should be reported to the Vice Chancellor of University Academic Affairs and/or the Vice Chancellor & CFO to determine whether or not a violation has occurred and the appropriate response in accordance with AU's established policies and procedures.

XV. Review Schedule

This policy will be reviewed annually by the Office of University Counsel.

Policy Cross Reference

Email Use Policy	Policy # 8.103