

# **AMERICAN INTERNATIONAL COLLEGE (AIC)**

## **TECHNOLOGY USE POLICY**

### **Definition of Terms**

Account: Any ID and password combination issued by AIC for access to electronic communication systems or computer resources.

User: Any person who uses the AIC electronic communication system or computer resources.

Electronic resources: Computer files and software, including but not limited to those that reside on disks and other storage media, individual computers, networked servers, or other electronic communications systems.

Electronic communications systems: Computers and networks [systems] used in communicating or posting information or material by way of electronic mail, bulletin boards, web pages, or other such electronic resources. Also includes, but is not limited to, direct connections to the campus network.

System administrator: A person responsible for managing and operating an electronic communication system for the use of others.

### **General Statement of Principles**

American International College encourages the creative and innovative use of information technology to enhance its teaching, research, and public service mission. Users will not have their right to access denied or abridged due to the individual's race, color, religion, sex, sexual orientation, national origin or citizenship status, age, disability, or veteran's status. AIC respects the intellectual labor and creativity of others and seeks to protect the free and peaceful expression of ideas. All members of AIC share responsibility for maintaining an environment within which actions are guided by mutual respect, integrity, and reason.

AIC expects all members of its community to use network systems with proper regard for the rights of others and AIC. Abuse of these privileges will be subject to disciplinary action, as established by the operating policies and procedures of AIC. AIC reserves the right to limit access in response to evidence of violations of AIC policy or federal, state or local laws. All members of the AIC community are bound by federal, state and local laws relating to civil rights, harassment, copyright, security, pornography, privacy, and other statutes relating to electronic media. It should be understood that this policy does not preclude enforcement under the laws and regulations of the United States of America, the Commonwealth of Massachusetts or local communities.

### **Who is covered by this Policy**

All users of AIC electronic communications systems are subject to the provisions of this policy, including those who rely on off-campus access to these systems.

Use of these systems implies consent with this policy, as well as other applicable AIC policies and local, state and federal laws. For individuals whose network accounts are primarily for representing units or special projects, further policies may apply as governed by the needs of the unit or project.

### **Individual Privileges**

The following individual privileges are extended to all users of electronic communication systems. However, it is understood that each of these privileges is conditional pending acceptance of the accompanying responsibilities.

1. Free Expression: There shall be no restrictions placed on the fundamental rights to free speech except those necessary to protect the rights of others and to preserve the order necessary for AIC to function as an institution of higher learning. Given the diverse cultural backgrounds of users, AIC cannot protect individuals against exposure to materials that they may consider offensive. Nevertheless AIC reserves the right to take restrictive actions in response to complaints that posted material creates a hostile environment for individuals or classes of individuals. AIC also has the responsibility to take restrictive action when a user violates AIC policy or federal, state or local laws.

2. Privacy: Users may expect to keep personal electronic mail correspondence reasonably confidential. Users should be sensitive to the inherent limitations of shared network resources in protecting privacy. Some examples of this may include printing personal messages on a shared printer, leaving a message or account open on a computer in an open office space or public area, etc. Specific personal electronic communications and computer files will not be searched deliberately to seek evidence of malfeasance except in an emergency or as part of a formal investigation by an authorized authority.

### **Individual Responsibilities**

Users of AIC's network systems accept responsibilities that include, but are not limited to, the following specific examples.

1. Respect for Intended Use of Resources: Users are responsible for all actions taken on their network account. Individual password security is the responsibility of the user and he/she should take precautions against others obtaining unauthorized access to his/her personal account. If the user allows another individual access to his/her account, the user assumes full

responsibility for the actions of this individual while logged into his/her account. AIC's electronic communication systems are to be used for the furtherance of AIC's mission and not for personal benefit.

2. Respect for Privacy of Others: Users shall not access anyone else's electronic resources, including files and mail, without specific permission from the owner. Permission does not include sharing account information as designated above, but allows for collectively reading e-mail and sharing files using network services. The user shall not take advantage of another's inexperience or negligence to gain access to any computer account, data, software, or file for which he or she has not received explicit permission to access.

3. Respect for Shared Nature of Resources: Users will not encroach on others' use of AIC's computers and network facilities. No user should attempt to modify AIC system or network facilities or to crash systems. Users should avoid activities that unreasonably tax systems resources, including but not limited to: sending an excessive number of messages, either locally or over the Internet; participating in electronic chain letters, frivolously printing multiple copies of documents, files or data; excessive game playing; modifying system facilities, operating systems, or disk partitions; or damaging or vandalizing AIC computing facilities, equipment, software, or computer files.

4. Respect for Rights of Others: AIC computing resources will not be used to harm or threaten to harm the safety or environmental health of another individual or individuals. The user must comply with AIC policies and federal, state and local laws regarding discriminatory harassment. Examples of violations include, but are not limited to: harassment; defamation, violation of privacy; intentionally placing a person or persons in reasonable fear of imminent physical harm; giving or causing to be given false reports of fire or other dangerous conditions; or harassment or discrimination based on race, color, religion, sex, sexual orientation, national origin or citizenship status, age, disability, or veteran status.

5. Respect for Intellectual Property: Respect for intellectual labor and creativity is vital to the academic discourse and enterprise. This principle encompasses respect for the right to acknowledgment, right to privacy, and right to determine the form, manner, and terms of publication and distribution. Examples of violations include, but are not limited to: copying copyrighted software without express written permission of the copyright owner; failing to obtain necessary licensing for software or to adhere to all licensing provisions (installation, use, copying, number of simultaneous users, term of license, etc.); plagiarism or inadequate attribution of the intellectual property of others; posting of texts, images or audio works in disregard of copyright restrictions; or unauthorized publication or distribution of another's work or writing.

6. Respect for Integrity of System or Network: Accounts shall not be used for unauthorized access and/or attempts to access computers, computer software, computer data or information, or networks without proper authorization, regardless of whether the computer, software, data, information, or network in question is owned by AIC. Abuse of networks or computers at other sites using AIC resources will be treated as an abuse of computing privileges at AIC. Users are prohibited from attempting to circumvent or subvert any system's security measures.

### **Reporting Violations**

If a user believes that a violation of this policy or criminal act has occurred, the user should contact Computing Services. AIC officials will take appropriate action in accordance with established AIC procedures. Infractions that may be violations of federal, state, or local laws will be reported by AIC officials to the appropriate authorities.

If a situation occurs in which a user feels that her/his personal health or safety is in jeopardy or that of another person (i.e., death threat, physically threatening message, or suicide threat), the police should be contacted by dialing 911.

If a user has violated any policies above, s/he may be subject to a process as defined in the Student or Employee Handbook.

In some situations, it may be necessary to suspend account privileges to prevent ongoing misuse while the alleged violation is under investigation. The system administrator reserves the right to immediate temporary suspension of the account(s) of anyone suspected of a violation, pending the outcome of investigation by the appropriate office listed above.

### **Administration and Implementation**

Systems administrators will manage network systems in a manner that is consistent with the system's importance for campus communication and the need for privacy of personal electronic mail messages. In connection with their responsibilities, professional staff members may on occasion need access or monitor parts of the system and thereby be given access to the contents of certain electronic mail messages. System administrators will respect the privacy of personal communications encountered on the systems. However, if, during the course of routine duties, a system administrator encounters information that indicates that a breach of this policy or criminal act has been or is about to be committed, the administrator will report the existence and source of this information to the proper authorities.

Administrators are not responsible for monitoring user activity or content on any network system. However, when they become aware of violations, either through the normal course of duty or by a complaint, it is their responsibility to refer the matter to the appropriate authority for investigation and possible discipline. To forestall an immediate threat to the security of a system or its users, system administrators may immediately suspend access of the people involved in the violation while the incident is being investigated. They may also take other actions to preserve the state of files and other information relevant to an investigation. Specific personal electronic communications and computer files will not be searched deliberately to seek evidence of malfeasance except when the appropriate authorities feel it is necessary in order: to enforce policies regarding

harassment and the safety of individuals; to prevent the posting of proprietary software or texts, images, or audio works in disregard of copyright restrictions or contractual obligations; to safeguard the integrity of computers, networks, and data either at AIC or elsewhere; and to protect AIC against seriously damaging consequences.

In general, electronic mail is considered the private information between the sender and recipient account holder. There may be exceptional circumstances where AIC may release electronic mail to other parties. These situations may include, but are not limited to, the death of the account holder, when an absent or terminated employee has received mail associated with his/her job responsibilities, or during the course of a criminal investigation by authorized legal authorities.

AIC recognizes that all network system users are bound by federal, state, and local laws relating to civil rights, harassment, copyright, pornography, privacy, security and other statutes relating to electronic media. Nothing in this policy should be interpreted as precluding enforcement of the laws and regulations of the United States of America, State of Massachusetts or any locality in the Commonwealth of Massachusetts.

### **Guidelines for Acceptable Use**

The account issued to you by the Office of Information Technology shall be used only in the manner described below. Violations of these rules may be cause for referral of the matter to the appropriate AIC administrative department.

1. The account shall be used only by the person to whom it is issued. You are responsible for the actions of anyone using your account.
2. All passwords issued are to be held privately and securely. Be responsible for all use of your accounts and for protecting each account's password. In other words, do not share computer accounts. If someone else learns your password, you must change it.
3. The account shall be used for academic or administrative purposes pertaining to AIC. You may send and receive electronic mail and maintain personal information (letters, resumes, etc.) as long as you observe the rules of etiquette, including refraining from obscenities and profanity.
4. The account shall not be used for unauthorized access and/or attempts to access computers, computer software, computer data or information, or networks without proper authorization, regardless of whether the computer, software, data, information, or network in question is owned by AIC. (That is, if you abuse the networks to which AIC belongs or the computers at other sites connected to those networks, AIC will treat this matter as an abuse of your AIC computing privileges.)
5. The user shall not take advantage of another's inexperience or negligence to gain access to any computer account, data, software, or file for which he or she has not received explicit permission to access.
6. The user shall not send fraudulent computer mail, break into another user's electronic mailbox, or read someone else's electronic mail without his or her permission.
7. The user shall not use AIC's computing resources to harass or threaten other users.
8. Software, other than freeware/shareware, may NOT be copied without permission of the system administrator.
9. The user is responsible for maintaining the security of his or her own data and for making back-ups of such data.
10. The user shall not encroach on others' use of AIC's computers (e.g., disrupting others' computer use by excessive game playing; by sending excessive messages, either locally or off-campus [including but not limited to electronic chain letters]; printing excessive copies of documents, files, data, or programs; modifying system facilities [including attaching devices to the network such as routers, switches, or servers], modifying operating systems, or disk partitions; attempting to crash or tie up an AIC computer; damaging or vandalizing AIC computing facilities, equipment, software, or computer files)
11. The user should report any abuse of the above to the appropriate dean, director, instructor, supervisor, system administrator, or other AIC authority.