AMERICAN NATIONAL UNIVERSITY

Code of Computing Conduct

American National University Computing Facilities (ANUCF) are intended to support the academic mission and the administrative functions of the University. This Code of Conduct states the principles regarding the use of ANUCF. They complement and supplement rather than replace other policies concerning appropriate conduct of staff and students.

> The policies controlling acceptable behavior at American National University are implicitly extended to cover the use of the ANUCF. The impersonal aspect of computers should not be taken as an excuse or reason for people's interactions with others to be anything by well-mannered, ethical and legal.
>
> For example, if it is unacceptable to display a sexually explicit poster in a public room, it is similarly unacceptable to display such an image on a publicly visible computer screen. Unsolicited, wide distribution of mail or message should be carried out only if there is a reasonable expectation of interest by the recipients. Even in those cases, care must be taken to ensure that the messages do not overwhelm systems.

American National University Computing Facilities include any computer, computer-based network, computer peripheral, operating system, software or any combination thereof, owned by American National University or American National University Services, Inc. (ANUSI) or under custody or control of American National University or American National University Services, Inc.

> The ANUCF include stand-alone workstations and network-attached systems as well as central servers. This Code also specifically applies to access to ANUCF via telephone lines, the internet, or other remote access mechanisms.

The following principles apply to all American National University and ANUSI employees, students and other users of the American National University Computer facilities. Users shall:

1. Be responsible for using these facilities in an effective, ethical and lawful manner.

   This policy states that individual users are responsible for their own actions. For example, if a user transmits illicit materials or stores illegal software, that individual user is responsible for such actions and may be held accountable for all results and repercussions of such actions.

   Be aware that wasteful or inefficient use of resources may incur significant expense for American National University or result in a reduction in service to other users.

2. Use only those facilities for which they have authorization, whether these facilities are at American National University or at any other location accessible through a network.

Normally, ANUCF systems require explicit authorization. Authorization based on the provision of false or misleading information is not valid.

3. Take all reasonable steps to protect the integrity and privacy of the ANUCF including software and data. In particular, users shall not share with others the access codes, account numbers, passwords or other authorization which have been assigned to them.

   Users are encouraged to report any violations of this policy and any information relating to a flaw in or bypass of computing facility security, to the appropriate instructor, campus director, department head or to the UNUCF Information Systems department. Such security “holes” must not be “tested” without proper authorization. Turning a blind eye to potential violations or system flaw may allow your privacy or access to be jeopardized.

   In this and the following sections, “access code” represents the username, account, sign-on ID, password or whatever system-dependent mechanisms are used to gain access to particular facilities.

   By allowing your access code to be used by others, you risk compromising the security and integrity of the ANUCF. As described in several later sections, much software which American National University utilizes requires that all actions be identified and traceable. For these reasons, if you do allow your access code to be used by others, you are responsible for all usage and activities carried out with the code.

   Allowing unauthorized access to ANUCF indirectly is similarly prohibited (such as allowing access to a private computer at home, where this computer in turn provides access to ANUCF).

   A computer or terminal logged on and unattended in an accessible location is particularly vulnerable.

   Some system management functions require that all those responsible for such functions share a single access code. Similarly, specific access codes are at times allocated to allow several people performing common functions to receive email. The use of such shared codes must be restricted to the intended purpose. Other usage by the same people should be through single-user access codes.

4. Respect the copyrights of the owners of all software, media and data they use.

   Most of the programs made available on the ANUCF are copyrighted. Copyright law specifically prohibits copying of any software except as explicitly allowed in the usage agreement. Copyright law also provides similar protection for data and text.

   Unless the software explicitly states otherwise, ALL software is copyrighted, even those normally referred to as shareware or freeware. Individual license agreements detail the exact rights and limitations.

Media files such as music and video files are also subject to copyright protection. Unauthorized downloading of such files, including unauthorized peer to peer sharing of copyrighted material is specifically prohibited.

Unauthorized use, sharing or distribution of copyrighted material may subject the user to criminal and civil penalties, including fines, incarceration, money damages payable to the copyright owners, and attorney's fees. In addition, American National University may take disciplinary action against users who violate these prohibitions which may include suspension or termination of employees, and suspension or disenrollment of students.

5. Respect the policies established by the administrators of external networks such as GAPS, COD, ED Connect, WestLaw, and various virtual library networks when using such networks. They also respect the policies established by the administrators of local computing facilities at American National University.

   The use of networks external to American National University must comply with the policies of acceptable use promulgated by the organization responsible for those networks. This Code of Conduct hereby specifically incorporates these external policies. Adherence to this code ensure compliance with the policies of our associated networks.

6. Respect the privacy of others. This includes, but is not limited to, respecting the confidentiality of email, files, data and transmissions.

   Records containing information directly related to a student are confidential and protected from public disclosure by the Family Educational Rights & Privacy Act, 20 U.S.C. & 1232 g. No one shall access any such records maintained in an electronic format or disclose or distribute their contents in any manner inconsistent with federal and state law and the University regulations.

   The ability to access information does not imply permission to access it. Specifically, having read-access to a file does not mean that you may read it. You should not browse, view, print, copy or execute someone else's directories or files (either manually or program-assisted) without explicit permission. The also applies to floppy disks and tapes and similar storage media.

   There may be cases where supervisors must access an employee's mail or files to get specific job-related materials or conduct business. For example, an urgent memo must be sent, but the staff member who typed it is ill. The need to respond to business-related email is another example. In all cases, unless prior arrangements have been made, reasonable effort to ask the employee's permission must be made.

   Access codes allocated for specific purposes may be designate as "non-private." In such cases, no data stored under the code may be considered for the private use of the individual to whom the code is allocated. Prior notice of such designation must be given.

7. Refrain from using ANUCF for unauthorized commercial activities.

As with other University resources, the use of the ANUCF for private, commercially-oriented applications is forbidden without appropriate authorization. Use for University-related private activities is often permitted. For example, running an unauthorized business, doing tax returns or sending e-mail soliciting donations from a non-University-related entity are clearly not allowed. On the other hand, use by a student for writing a resume is quite acceptable. If in doubt, check with the appropriate instructor, campus director, department head, executive vice president or executive director.

8. Refrain from using ANUCF for any unauthorized or illegal purposes. Such purposes might include destruction or alteration of data owned by others, interference with legitimate access to computing facilities or harassment of users of such facilities at American National University or elsewhere, unauthorized disruption of ANUCF, attempts to discover or alter passwords or to subvert security systems in ANUCF or in any other computing or network facility.

   The law prohibits unauthorized use of computers; unauthorized access to information or programs; destruction or alteration of data or interference with lawful access to data and the use of a computer system with the intent to commit any of the above.

   Intentional introduction of any computer virus, Trojan horse, worm or similar software is an explicit violation of this principle.

   Any unauthorized action which intentionally denies or obstructs access for another legitimate user to ANUCF is forbidden.

9. Properly identify themselves in any electronic correspondence and provide valid, traceable identification if required by applications or servers within the ANUCF or in establishing connections from the ANUCF.

   All transmissions must be identifiable by American National University staff. That is, they must include your access code. Similar rules are imposed by many external networks. You are encouraged to ensure that your name (in addition to access code) is also attached to all applicable messages. It is specifically forbidden to attempt to mask your real identity or intentionally originate a message masquerading as someone else.

   By convention, most systems offering “anonymous FTP” services request that you enter your network address as a password. Users must comply with this convention.

   Users do not have a right to privacy when using ANUCF.

   University officials have the right to access electronic files, including e-mail files, for any purpose deemed reasonable by them in their sole discretion.

Any violation of this Code may be prosecuted in conformity with the relevant University policy (Code of Student Conduct, personnel policies, etc.) as well as applicable criminal and civil laws.