

Information Systems Policy and Procedures

The information systems—including computers, network accounts, microcomputers, printers, networks, software, electronic mail, video, telephones, long distance, and voicemail accounts—at Adelphi are provided for the purpose of enhancing the mission of scholarship, research, and education. All students, faculty, and staff who are provided access to these systems are responsible for seeing that these information systems are used in an effective, efficient, ethical, and lawful manner. The use of information systems is a privilege, not a right, which may be revoked at any time for misuse, including but not limited to violation of the policy and procedures contained herein. Adelphi University reserves the right for authorized personnel to access and examine the contents of its information systems for business and/or security reasons. The following policies relate to information system use and the University reserves the right to modify this policy at any time. This Acceptable Use policy is also available on Adelphi's Office of Information Technology & Resources website.

1. The information systems are owned by Adelphi and are to be used for University-related activities only. All access to central information systems, including issuing of accounts, must be approved through the Office of Information Technology & Resources (OITR). Access to school, institute, college, or departmental information systems must be approved by authorized personnel.
2. Information systems are to be used only for the purpose for which they are assigned and are not to be used for commercial, non-University, or solicitous activities. Information systems are to be used in accordance with all federal, state and local laws.
3. Computer programs, email, voicemail, and electronic files are presumed to be private and confidential unless there is suspected misuse or they have been explicitly made available to authorized individuals. Authorized OITR personnel may access others' files when necessary for the maintenance and security of information systems. When performing maintenance, every effort will be made to insure the privacy of a user's files. However, if violations of policy are discovered, they will be reported to the appropriate Vice President and either the Assistant Vice President for Human Resources and Labor Relations (for employees) or the Dean of Student Affairs (for students).
4. Fraudulent, harassing, illegal, or obscene messages or materials are not to be sent, printed, requested, or stored. Chain letters and other forms of Internet mass mailings are not allowed. University-wide broadcasts must be approved by the Director of IT.
5. A computer account, email account, or voicemail account assigned to an individual must not be used by others without explicit permission from the instructor or administrator requesting the account. The individual to whom the account is assigned is responsible and will be held responsible for the proper use of the account, including proper password protection.
6. Information system accounts that expire will be deleted, along with any files within the expired accounts. Accounts expire in accordance with the terms of the account. Email and voicemail messages that are older than the limit set by the system administrator will be deleted. For active employees, and others who have an ongoing relationship with the University, such as emeritus professors, accounts will not be closed and files will not be deleted without every effort being made to contact the account holder. The OITR will assist in whatever way possible to help account holders to archive their files.
7. Software systems that allow access through the network to the contents of microcomputer files will not be installed on a microcomputer without the approval of the faculty or staff member to whom the microcomputer is assigned, and if installed, will not allow access to the contents of files except under the direct control of that faculty or staff member.
8. Special support software may be installed by OITR personnel on University computing systems in order to support resource usage accounting, security, network management, hardware and software inventory, updating functions, and personnel.
9. No one may deliberately attempt to degrade the performance of the information systems or to deprive authorized personnel of resources of access to any University Information system.
10. Loopholes in information systems security or knowledge of special password must be reported to the OITR as soon as possible and are not to be used to damage information systems, obtain extra resources from another user, gain access to systems or use systems for which proper authorization has not been given.
11. Copyrighted software is not to be copied from or into the campus information systems, excepted as permitted by law and by the contract or license agreement with the owner of the copyright. Campus information systems are not to be used to replicate copyrighted software. The use of the software on a local area network or on multiple computers must be in accordance with the license agreement.
12. The OITR staff is responsible for dealing with primary violations of this policy. Repeated or serious violations will be referred to the University Student Judicial Officer, Vice Provost for Faculty and Staff Relations, or the Associated Vice President for Human Resources and Labor Relations.

Only those who complete and sign the Panther Account Request form and return the form to Customer Services will be considered for the creation of a Panther account.