Acceptable Use Policy for IT Services

Menlo College
Updated: March 3, 2014

This Acceptable Use Policy (AUP) governs appropriate behavior with respect to Menlo College networking and IT services. The scope of this AUP includes, but is not limited to:

- Academic and social activities on the College wired and wireless network
- Use of College-owned computing equipment, including printers, and all associated connectivity, wires, and accessories

This AUP applies to all users of the College’s information technology (IT) resources, regardless of the access device (personal computers, smartphones, and tablets, College-owned computers and printers, all relevant accessories, etc.).

**Intersection with the Student Code of Conduct**

In all cases, students should behave in a manner consistent with the Code of Conduct as outlined in the Student Handbook. This is an IT-specific addendum to that document. As with the Code of Conduct, this AUP is subject to change as circumstances require.

**Rights & Responsibilities**

By using Menlo College’s IT resources, students accept the policies set forth in this AUP. Violation of the guidelines can lead to the revocation of access to some or all of these services.

College IT resources are shared with the entire community. Users shall not engage in any activity that affects the ability of other users to access network resources. The Office of IT will use available tools to help maintain a balance between a high quality of service and the ability to gain access to priority resources. This means that we generally permit more access by more users, versus less access by fewer users. It is the responsibility of the user to avoid negatively impacting others.

For residential students, the Office of IT acknowledges that the social aspect is an important component of the higher education experience. As such, while the primary purpose of IT services is to support academic/instructional needs, efforts are made to provide quality of service for media
streaming and other social/entertainment capabilities within the confines of avoiding negative impact on other users.

Menlo College ensures the quality of service for all users in all contexts through general monitoring of all available tools. Users should not expect any universal right of privacy with respect to the College’s IT services. We do not actively monitor communication or traffic from any specific users or group of users, but system administrators may access files or accounts of suspected unauthorized use with appropriate justification as per the Code of Conduct and other College policies. Email accounts will be accessed only via court order or under direction of the Office of Risk Management.

**General Expectations**

- No student shall provide his or her Menlo credentials (username/password) to another individual at any time, for any purpose

- All students shall make reasonable efforts to maintain a secure workstation. Examples include utilizing an anti-virus application, making sure operating systems are fully up to date, and avoiding installation of suspicious software.

- Students must utilize the Password Manager system as provided by the Office of IT. The Password Manager system allows students to reset passwords or unlock accounts themselves.

Version 1.0 by Allan Chen March 3, 2014