Technology Policies

Acceptable Use Policy and User Agreement

SEE ALL ARTICLES OF THE TECHNOLOGY POLICIES CHAPTER

This policy defines the acceptable use of Franklin & Marshall (F&M) information and technology assets. Those users who violate this policy are subject to the full range of sanctions set forth in the College Life Manual and Student Code, the Employee Policy Guide, as well as any applicable local, state, and federal laws. The College Information Technology Committee reserves the right to modify this policy at any point in time, without notice to users.

Information security requires participation and support from every member of the F&M community who has access to College systems and data. It is the responsibility of every member of the F&M community to help ensure the confidentiality, integrity, and availability of all information and technology assets.

Audience

This policy applies to all members of the F&M community, which includes employees, students, visitors, volunteers, third parties, contractors, consultants, clients, temporaries, and others (collectively known as "users"), who have access to, support, administer, manage, or maintain F&M information and technology assets.

Policy Maintenance

The College Information Technology Committee will review this policy on an annual basis. All revisions will be presented to the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) for approval.

Policy Statement

In support of its mission of teaching, research, and public service, F&M provides access to a wide variety of information and technology assets for its users. Access to these information and technology assets is a privilege granted to the members of

the F&M community and is vital to performing their daily tasks. Therefore, proper use and protection of F&M's information and technology assets is essential to the operation of the College.

It is each user's responsibility and obligation to ensure that all information and technology assets are used only for their intended purpose and that information contained or transmitted via these resources is protected from unauthorized access, modification, or destruction. F&M also recognizes that local, state, and federal laws relating to copyright, information security, and intellectual property are applicable to all members of the F&M community. The College reserves the right to limit or restrict computing privileges and access to its information and technology assets.

User Responsibility

Those who use F&M's information and technology assets must act responsibly. Every user is responsible for the integrity of these resources. All users must respect the rights of other users, respect the integrity of the physical facilities and controls, and respect all pertinent license and contractual agreements.

F&M information and technology assets are to be used for the College-related activities for which they are designed. The College provides each member of the College community with ample file and web space to disseminate legal content. Under no circumstances shall these resources be used to distribute copyrighted material whether it is images, music, software, movies, electronic books, journals, or any other digital content for which the user does not have appropriate rights. Under no circumstances shall these resources be used to produce physical items or disseminate materials in violation of the College's **weapons policy** (https://www.fandm.edu/college-policies/safety-security/weapons-policy). The use of College-provided network, file, or web services to offer goods or services of a commercial nature not sanctioned by the College is strictly forbidden.

Internet Use

Internet access is made available to members of the F&M community. Users must be familiar with the risks associated with accessing the Internet, including the lack of confidentiality or integrity of information accessed or sent via the Internet. Users must be aware that accessing the Internet through the College's network does not afford expanded privacy protections, and that web site operators or other third parties routinely collect and share information about their visitors.

Users must use discretion when posting information using College email addresses on public Internet sites or through social media. Users must observe the protections outlined by the **College's Data Classification Policy** (www.fandm.edu/college-policies/technology/data-classification-policy) before using any internet service to transmit, store, or process Confidential or Sensitive College data.

Network Admission Control & Anti-Virus Software

As part of F&M's ongoing efforts to deliver the most reliable network services network, the College reserves the right to determine the information security health of any non-College owned or non-College managed systems that connect to the College network, and to require a baseline level of security, including up-to-date operating system patches, anti-virus/anti-malware software, and/or other requirements before granting access to the College network. This may include a security scan to determine the security posture of your device before being granted access.

You are responsible for the state and behavior of your personally owned devices while they are used at F&M. Accordingly, every member of the College community and their guests have agreed not to use the network in any way that diminishes the effectiveness of the network or interferes with the reasonable use of those systems by others. Any device that adversely affects the College network or attempts to circumvent College security measures will be isolated from the network without advance notice.

Conflicting Network Services

Users may not connect systems to the College network which emulate, spoof, replicate, or interfere with existing information technology services provided by the College. Prohibited systems include but are not limited to DHCP servers, DNS servers, and wireless access points/personal hot spots. F&M reserves the right to disconnect without warning any systems which are found to be interfering with the ability of other members of the community to connect to or use information and technology resources provided by the College.

Electronic mail (email) and other Electronic Messaging

All F&M email accounts and all data transferred or stored using F&M's email capabilities are the property of the College. As such, email messages are considered part of F&M records and, upon legal request, are subject to review, monitoring, auditing, and discovery. Therefore, when composing email messages, users must comply with all policies regarding the acceptable use of F&M's information and technology assets.

F&M email addresses are not to be used to create or sign into any third-party cloud services that have not been provisioned by the College. Members of the community should use a personal email account to interact with services such as social media or online shopping unless these services are being used exclusively for work being performed on behalf of the College.

Inappropriate Use of Email or other Electronic Messaging

Any inappropriate email, as defined below, is prohibited. Users receiving such email should immediately contact the ITS Help Desk at 717-358-6789 or helpdesk@fandm.edu. In the case of serious risks or harm, users should contact the Office of Public Safety at 717-358-3939. Examples of the inappropriate use of electronic messaging include:

- The creation and exchange of messages which are harassing, obscene, or threatening;
- The unauthorized exchange of sensitive or confidential data;
- The creation and exchange of advertisements, solicitations, or chain letters.
- The knowing transmission of a message containing a computer virus or a message which is intended to trick or mislead the recipient into performing an action;
- The misrepresentation of the identity of the sender of a message; and
- The use or attempt to use the accounts of others without their permission.

Privacy

While F&M respects an individual's use of computing resources, it should be noted that there are no facilities provided for sending, receiving, storing, or otherwise manipulating confidential messages, information, or files and there should be no expectation of privacy when using the College's network or systems.

The College may monitor transmissions should a violation of this policy be alleged. Authorized personnel may also monitor transmissions in the course of performing routine maintenance or troubleshooting problems. System administrators or other authorized personnel may examine or make copies of files that are suspected of misuse or that have been corrupted or damaged.

Any file may be subject to search by law enforcement agencies under court order if such files contain information which may be used as evidence in a court of law. Information Technology Services staff may access college-owned computers to

perform system maintenance either on-site or using remote tools as necessary without prior notification.

User Agreement

I agree to the user obligations described above and agree not to use F&M's information and technology assets in any way that diminishes the effectiveness of those assets or interferes with the reasonable and individual use of those systems by others. I acknowledge the right of Franklin & Marshall College, and its designated staff, to inspect, when necessary as a function of responsible system management, all files stored or data transmitted through the College's information and technology assets.

I understand that upon violation of the terms of this agreement, the College retains the right to deny future computing privileges. I understand that I may also be subject to further disciplinary action by the College and/or legal action arising from the violation of any federal, state, or local laws.

Policy Maintained by: Information Technology Services, Vice President and Chief Information Officer

Last Reviewed: 18 September 2017