

Information Technology Policies

[Home](#) / [College Policies](#) / [Technology](#) / Acceptable Use Policy

Acceptable Use Policy and User Agreement

INFORMATION TECHNOLOGY POLICIES

I. Justification and Statement of Policy

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 range of sanctions set forth in the College Life Manual and Student Code, Human Resource and College policies, as well as any applicable local, state, and federal laws. The College Infrastructure Committee reserves the right to modify this policy at any point in time, without notice to users.

employees, students, faculty, emeriti faculty, visitors, volunteers, third parties, alumni, 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.

III. Definitions

IV. Policy

Access to information and technology assets provided by the College is a privilege granted to the members of the College community. These assets are to be used for the activities for which they were designed. The College also recognizes that local, state, and federal laws relating to copyright, information security, and intellectual property are applicable to all members of the College community. The College reserves the right to limit or restrict computing privileges and access to its information and technology assets without notice.

Privacy

While the College 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 private messages, information, or files and there should be no expectation of privacy when using the College's network or systems.

On occasion, situations arise and scenarios occur that may require access to information stored within College systems. This may be prompted, for example, by legal action, health or safety concerns, or by urgent College business needs. Access may be provided with the approval of the following College officer.

Constituency


College Officer

Students

Vice President for Student Affairs

Faculty

Provost


[Admission](#) [Academics](#) [Student Life](#) [About F&M](#) [Success Beyond F&M](#) [Give](#)

President Chair, Board of Trustees

Staff AVP for Human Resources

Internet Use

Users must observe the protections outlined in 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 data.

Risks that users accept when accessing the Internet include:

- Lack of confidentiality and/or integrity of information accessed, sent, or received.
- No privacy protections.
- Web site operators and other third parties may collect, store, and share information about users who visit their sites or use their services.

Email accounts

All College email accounts and all data transferred or stored using the College's email system are the property of the College and are considered College records.

College email accounts:

- are to be used solely for College related activities and business.
- are not to be used to create or sign into any third-party service that has not been provisioned by the College, unless these services are being used exclusively on behalf of the College.

- are prohibited from being used for official College business.
- are encouraged to be used with personal services such as social media or online shopping.

Inappropriate Use of Email

Sending inappropriate email that violates any College policy is prohibited. Users receiving inappropriate email should immediately contact the ITS Help Desk at 717-358-6789 or helpdesk@fandm.edu. In the case of serious risk or potential harm, users should contact the Office of Public Safety at 717-358-3939 immediately.

Selected examples of inappropriate use include:

- harassing, obscene, or threatening messages
- the unauthorized exchange of sensitive or confidential data
- sending non-College sanctioned advertisements, solicitations, or chain letters
- sending malware or a message which is intended to mislead the recipient into performing an action
- misrepresenting the identity of the sender of a message
- using or attempting to use the accounts of others without their permission

Network Access

The College reserves the right to determine the information security level of any non-College owned or non-College managed systems that connect to the College network or systems. A baseline level of security must be met before being granted access to the College network. Users are responsible for their personally

are commonly used for copyright infringement.

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. Some contracted services, College network tenants, shared services organizations, etc., may inquire for exemption to this "Conflicting Network Services" section by contacting the ITS department before installing any software, systems, or equipment and receiving written permission.

User Prohibitions

User accounts or user device access or services may be suspended:

- for actions negatively impacting any College provided information or technology asset.
- for obstructing others from accessing College resources.
- for violating College licensing or contractual agreements.

Users are prohibited from:

- Distributing copyrighted material such as images, music, software, movies, electronic books, journals, or any other digital content for which the user does not have appropriate rights.
- Storing information for or producing physical items that could be considered weapons of any kind.
- Using College resources to offer goods or services of a commercial nature not sanctioned by the College.

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 current and 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 Maintenance

The College Infrastructure 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 Maintained by: Information Technology Services, Vice President and Chief Information Officer

Original Effective Date: September 1, 2019

Last Reviewed: September 14, 2022



Admission
FRANKLIN & MARSHALL COLLEGE & Aid

Academics

Student
Life

About
F&M

Success
Beyond
F&M

Give



Explore
Programs »



AID
Apply Now »



Plan Your
Visit »



accessibility in mind and incorporates many accessible features. If you are experiencing difficulty accessing a College website, or content located on a College website (video, document, etc.), please contact us at websters@fandm.edu. The College does not make representations with regard to the accessibility of third-party websites and is not able to remediate accessibility barriers on such websites.

© 2023 Franklin & Marshall College
 P.O. Box 3003,
 Lancaster, PA 17604-3003
 717-358-3911



[PRIVACY POLICY](#)

- [Careers](#)
- [Contact](#)
- [Nondiscrimination](#)
- [Privacy](#)
- [Fields of Study](#)
- [F&M Bookstore](#)
- [Stories](#)
- [Diversity, Equity & Inclusion](#)
- [Events](#)
- [MyDiplomat](#)