



## Policy 5.1 Information Technology Conditions of Use

**Responsible Official:** Enterprise CIO and Sr. Vice Provost for Library Services and Digital Scholarship

**Administering Division/Department:** LITS: Library & IT Services

**Effective Date:** March 31, 2007

**Last Revision:** July 07, 2017

### Policy Sections:

- I. Overview
- II. Applicability
- III. Policy Details
- IV. Related Links
- V. Contact Information
- VI. Revision History

### Overview

Computers, networks, and software applications are powerful tools that can facilitate Emory's core missions in teaching, learning, research, and service. Access and utilization of these tools is a privilege to which all University faculty, staff, students, and authorized guests are entitled. This policy documents the responsibilities that accompany this privilege.

Campuses, schools, colleges, departments, and other administrative units have considerable latitude in developing complementary information technology conditions of use policies, as long as they are consistent with this enterprise policy and any other applicable policies of the University. Such policies may be more restrictive than the enterprise policy, but must not be more permissive.

### Applicability

This policy applies to Emory faculty, staff, students, and retirees who have been issued computer accounts such as an Emory NetID and to visitors and guests who have been issued sponsored computer accounts. This policy applies to all Emory information technology resources, whether they are accessed from campus or from a remote location. This policy also applies to anyone who has been granted access to or connects any device to the Emory network or Emory IT resources.

### Policy Details

#### General Principles:

- Emory's information technology (IT) resources are provided for uses consistent with the University's missions of teaching, learning, research, and service or for related administrative support.
- The use of Emory's IT resources must be consistent with other University policies, government regulations and laws.
- IT resources are not to be used for private financial gain or for supporting non-Emory related businesses.
- Users of Emory IT resources are expected to read and abide by all relevant IT policies and standards and to complete any prescribed IT security training.

### **Information Security Requirements:**

- Users of Emory's IT resources may not:
  - Share their passwords or other access credentials;
  - Attempt to hack, bypass, or violate security controls or conduct unauthorized testing of IT resources for security vulnerabilities;
  - Access, modify, or share sensitive data or information obtained from any of Emory's systems without appropriate authorization;
  - Use access credentials issued to other individuals or attempt to impersonate another individual in order to access IT resources.
- Users of Emory IT resources must:
  - Implement reasonable and appropriate safeguards to protect sensitive or critical information that they create or maintain;
  - Dispose of sensitive information in a secure manner (e.g. shredding, physical destruction, disk wiping)
  - Report any IT security incidents or security policy violations;
  - Cooperate with authorized IT security investigations;
  - Cooperate with authorized requests to discontinue activities that threaten the confidentiality, integrity, or availability of IT resources.
  - Return all institutional data and IT resources to Emory upon termination of employment and securely delete all institutional data from personally owned devices/media.

### **Conduct:**

- Users of Emory's IT resources may not use those resources for any unethical or illegal purpose, including but not limited to the following:
  - Violating copyrights or license agreements for any type of intellectual property (e.g. software, music, audio/video recordings, photographs, illustrations, documents, media files, e-journals, e-books, databases) (see <http://web.library.emory.edu/research-learning/scholcomm-datamgmt/index.html> for more information on University guidelines for copyright and fair use);
  - Harassing other members of the Emory community;
  - Destroying or stealing equipment, software, or data belonging to others;
  - Intentionally damaging or destroying the confidentiality or integrity of IT resources or disrupting their availability;
  - Viewing or distributing content, to the extent that doing so violates any applicable Emory policy and/or state and/or federal law, regulation, or policy;
  - Monitoring or disrupting the communications of others.

### **Personal Usage:**

- Limited and reasonable personal use of Emory's IT resources is acceptable and allowed, as long as it does not:
  - Interfere with the fulfillment of an employee's responsibilities;
  - Adversely impact or conflict with any activities that support Emory's mission or operations;
  - Result in any measurable cost to Emory;
  - Violate any other applicable University policies.

### **Network Protection and Monitoring:**

- Authorized Emory staff may without notice:
  - Monitor, inspect, or copy network communications, IT resources, and the data they contain. Use of the Emory network and/or IT resources constitutes consent to such monitoring;
  - Assess IT resources connected to the Emory network for security vulnerabilities;
  - Take emergency protective actions such as restricting user access rights or access to IT resources or the network;
  - Block potentially malicious network communications;
  - Block the viewing, downloading, or distribution of any content to the extent that doing so is required by federal or state law, regulation, or policy, or is required to carry out Emory's mission or operations.

### **Sanctions:**

- Failure to comply with this policy may have legal consequences and may result in:
  - Suspension or termination of access;
  - Disciplinary actions (up to and including termination of employment) in accordance with applicable university policy.

## Related Links

- Current Version of This Policy: <http://policies.emory.edu/5.1>
- [Connecting to the Emory Data Network](http://policies.emory.edu/5.4) (<http://policies.emory.edu/5.4>)
- [Emory Network IDs \(NetIDs\) and Passwords](http://policies.emory.edu/5.5) (<http://policies.emory.edu/5.5>)
- [Peer-to-Peer File Sharing](http://policies.emory.edu/5.7) (<http://policies.emory.edu/5.7>)
- [Disk Encryption Policy](http://policies.emory.edu/5.12) (<http://policies.emory.edu/5.12>)
- [Automatic Forwarding of Email from the EmoryExchange Environment](http://policies.emory.edu/5.13) (<http://policies.emory.edu/5.13>)
- [Copyright, Publishing and Fair Use](http://web.library.emory.edu/research-learning/scholcomm-datamgmt/index.html) (<http://web.library.emory.edu/research-learning/scholcomm-datamgmt/index.html>)

## Contact Information

Subject	Contact	Phone	Email
Clarification of policy	Brad Sanford	404-727-2630	brad.sanford@emory.edu

## Revision History

- Version Published on: Mar 13, 2016 (*Incorporation of changes requested by OGC*)
- Version Published on: Mar 13, 2016 (*Updated web links*)
- Version Published on: Mar 15, 2011 (*Major Revision / Re-write*)
- Version Published on: Mar 29, 2007 (*Original Publication*)

*Emory University policies are subject to change at any time. If you are reading this policy in paper or PDF format, you are strongly encouraged to visit [policies.emory.edu](http://policies.emory.edu) to ensure that you are relying on the current version.*