Acceptable Use Policy
Information Technology

Purpose

Stetson University makes available to its community members computing and network resources, including shared information technology resources to deliver information. These resources are to be used in a manner consistent with University policy and the law.

Scope

The Acceptable Use Policy for Stetson University Information Technology applies to all active members of the University community, including faculty, students, staff, and affiliates, and to authorized visitors, guests, and others for whom University technology resources and network access are made available by the University

A. POLICY STATEMENT

1. Institutional Use

Use of all University information technology and digital resources should be for purposes that are consistent with the non-profit educational mission and the policies and legal requirements (including license agreements and terms of service) of the University, and not for commercial purposes.

2. Prohibited Use

Use of the University's information technology and digital resources should not violate applicable federal, state, and local law, including U. S. copyright law, or applicable University policies, and, if travel is involved, the laws of the relevant nation or state. These include for example, the laws on libel, privacy, copyright, trademark, obscenity, and child pornography; the Florida Computer Crimes Act (Fl. Stat. Ch. 815), the Florida Security of Communications Statute (F. Stat. Ch.934), the Electronic Communications Privacy Act (18 U.S.C. §§ 2510 et seq.), and the Computer Fraud and Abuse Act (18 U.S.C. §1030 et seq.) From any location, University resources may not be used to transmit malicious, harassing, or defamatory content.

The following actions are considered unacceptable behavior:

- Users may not participate in any malicious behavior that harms or interferes with others' use of resources.
- Users may not use resources or information for commercial purposes without prior authorization.
- Users may not disrupt network services or tamper with software protections or restrictions.
- Accounts and passwords should not be shared or used by persons other than those to whom they have been assigned.

- Users must refrain from speaking on behalf of the University without proper authorization to do so.

3. Access and Privacy

In general, and subject to applicable law, the University reserves the right to access and copy information and files (including e-mail and voice messages) residing on University-owned equipment, systems, and in storage contracted by the University from outside enterprises. This includes access without notice, where justified by the University's operational and/or legal needs and consistent with applicable laws.

If business-related information or files (including e-mail and digitized voice messages) must be accessed based on business need or where required by law, they may be accessed by the University after consultation with the Business Office and among the appropriate University offices.

The University may, in its discretion, disclose the results of any such individual or general monitoring, including the contents and records of individual communications, to appropriate College or law enforcement personnel, subject to the Family and Educational Rights and Privacy Act (20 U.S.C. §1232(6)) and other applicable laws.

4. Violations and Penalties

Violations of the policy may result in disciplinary action, including dismissal from employment, expulsion from further study and termination, or suspension of network privileges.

B. QUESTIONS REGARDING THIS POLICY

If you have questions or concerns regarding this policy or other Information Technology Security Policies, please contact the Office of Information Technology.

Stetson Office of Information Technology
386-822-7045
support@stetson.edu