


PROCEDURE

Subject:	Acceptable Use	Number: 2.60.05
Source:	Vice President, Planning and Institutional Effectiveness	Reference (Rule #) 6HX14-2.60
President's Approval/Date:	 4/10/18	

PURPOSE: This Procedure defines general user responsibilities. Its purpose is to outline acceptable uses of State College of Florida (SCF) information resources (e.g., computer equipment, electronic messaging systems (EMS), and the Internet).

SCOPE: This procedure applies to:

- Users, systems, and locations;
- Employees, contractors, service providers, visitors;
- Applies to all facilities; and
- Students

POLICY STATEMENT: Information Protection, Use, Access, and Handling

- SCF information shall be protected consistently in a manner commensurate with its sensitivity, value, and criticality (see SCF Data Classification Guidelines)
- Access to sensitive SCF information (i.e., non-public) shall be based on a need to know, and shall be limited to access required for one's job function.
- Procedure Exceptions
- Requests for exceptions to the information security Procedures and Rules are thoroughly reviewed by the Data Custodian or Information Technology (IT) management; and are approved by the Presidential Advisory Committee.
- Other exceptions may be defined by management, such as business justified internet sites (e.g., YouTube internet site, streaming audio sites).

Electronic Messaging System (EMS)

- The SCF EMS encompasses all aspects of electronic communication, including, but not limited to, Microsoft Exchange, Microsoft Outlook, Microsoft Lync, faxes,

voicemail, text messaging, social media, and any other form of electronic messaging system approved for use by SCF.

- SCF owns the EMS and all related hardware and software. Employees and contractors shall use the EMS for SCF business or management approved purposes. Business use includes a reasonable amount of personal use by employees (e.g., to communicate with their families while traveling on SCF business).
- Employees shall not use the EMS for non-SCF business (limited exceptions may be approved by management), political purposes, or any activity or purpose that is illegal, dishonest, in violation of any SCF procedures; or to conduct any form of business outside normal SCF business.
- The EMS shall not be used to send confidential or proprietary information to third parties outside of SCF without management approval and adequate protection (e.g., strong encryption with good key management practices). Discretion shall be exercised when using the EMS to send highly sensitive and confidential information to other employees within SCF.
- Under no circumstances shall credit card information be sent by the EMS.
- All email and messages remain the property of SCF, and SCF reserves the right to review a user's electronic messages at any time without prior notice to the user. A user shall not expect any privacy in anything that they create, store, send, or receive on the EMS.
- Electronic messages may be programmatically or randomly selected for monitoring or review.
- Users shall not log in to or otherwise access another user's account without IT Management approval.
- Users shall not attempt to mislead other users or EMS regarding their identity.
- The EMS shall not be used to send or receive obscene, pornographic, or other inappropriate materials.
- The EMS shall not be used to discriminate based on sex (including pregnancy), race, religion, age, national origin/ethnicity, color, marital status, disability, genetic information or sexual orientation.
- Users shall not resend or forward an email chain letter received from any source.
- Users receiving an email message containing suspicious content or links shall immediately contact the SCF Help Desk at (941) 752-5357. The user shall not, under any circumstances, click on links or open attachments contained within such emails or forward them to other users.
- Users of the EMS shall take reasonable steps to ensure that material coming from outside SCF does not breach SCF's

harassment or discrimination policies. If there is uncertainty in this regard, the material shall be deleted and management notified.

Internet / Intranet Usage

- Users shall be responsible for exercising good judgment regarding the reasonableness of personal use of the Internet / Intranet. Should there be any uncertainty regarding appropriate Internet or Intranet usage; SCF staff shall consult their manager.
- Under no circumstances shall users download or attempt to download or install software using a SCF Internet connection; this includes, but not limited to, running or attempting to run any form of executable file.
- Users shall not access websites containing pornographic, violent, or illegal content.
- Users shall not change or attempt to change any preinstalled SCF settings or configurations pertaining to proxies, web-browsers, anti-virus software, or security controls of any kind.
- Intentional efforts to circumvent filtering software are not acceptable.
- Users shall exercise extreme caution when navigating to new or unknown websites.
- When a user is unclear of the security policies, standards, and procedures governing any aspect of SCF Internet usage, the user shall contact their manager or the Help Desk at (941) 752-5357 for instruction or clarification.

NONCOMPLIANCE:

Any employee/contractor found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment. Service providers found to have violated this procedure may be subject to financial penalties, legal action, and including termination of contract.

Any student found to have violated this procedure may be subject to disciplinary action in accordance with the Student Code of Conduct.