Title:	**Guidelines for Interpretation & Administration of the South Georgia State College Appropriate Use Policy for Information Technology (IT) Resources**
Status:	**Final**
Effective Date:	**2013-Oct-01**
Last Revised:	**2016-Nov-16, Reviewed 2017-Jan-18**
Policy Point of Contact:	**Chief Information Officer, Information and Instructional Technology**
Synopsis:	South Georgia State College guidelines for interpreting the appropriate use of information technology resources.

These guidelines are meant to assist South Georgia State College in the interpretation and administration of the South Georgia State College Appropriate Use Policy. The guideline outlines the responsibilities users accept when using South Georgia State College computing and IT resources. South Georgia State College, as a member institution of the University System, is subject to the USG Appropriate Use Policy and Guidelines for Interpretation and Administration. This document is provided as institution-level guidance on South Georgia State College's Appropriate Use Policy, along with any additional expectations on the part of South Georgia State College. This guideline includes the use of information systems and resources, computers, telephones, Internet access, electronic mail (email), voice mail, reproduction equipment, facsimile systems, and other forms of electronic communication.

User Responsibilities

Use of South Georgia State College IT resources is granted based on acceptance of the following specific responsibilities:

Use only those IT resources for which you have authorization.

For example, it is a violation:

- To use resources you have not been specifically authorized to use
- To use someone else's account and password or share your account and password with someone else
- To access files, data, or processes without authorization

- To purposefully look for or exploit security flaws to gain system or data access

Protect the access and integrity of IT resources.

For example, it is a violation:

- To use excessive bandwidth
- To release a virus or a worm that damages or harms a system or network
- To prevent others from accessing an authorized service
- To send email that may cause problems and disrupt service for others
- To attempt to deliberately degrade performance or deny service
- To corrupt or misuse information
- To alter or destroy information without authorization
- To connect personally owned systems and equipment to the South Georgia State College primary network or South Georgia State College computers without the prior approval of the Chief Information Officer.
    - If such approval is granted, the user has a responsibility to ensure the security and integrity of the personally owned (or managed) systems and equipment, as well as data accessed through such systems.

Abide by applicable federal, state, and local laws; adhere to USG and South Georgia State College policies; respect the copyrights and intellectual property rights of others, including the legal use of copyrighted material.

For example, it is a violation:

- To download, use or distribute copyrighted materials, including pirated software, music, videos, or games
- To make more copies of licensed software than the license allows
- To operate or participate in pyramid schemes
- To upload, download, distribute or possess pornography
- To upload, download, distribute or possess child pornography

Use IT resources only for their intended purpose.

For example, it is a violation:

- To use computing or network resources for advertising or other commercial purposes
- To distribute copyrighted materials without the express permission of the copyright holder
- To send forged email
- To misuse software to allow users to hide their identity, or to interfere with other systems or users
- To send terrorist threats or “hoax messages”
- To send chain letters
- To intercept or monitor any network communications not intended for you
- To attempt to circumvent security mechanisms
- To use privileged access for other than official duties
- To use former privileges after graduation, transfer or termination, except as granted by South Georgia State College
- To upload, download, distribute or possess materials depicting pornography, gratuitous nudity, sexually explicit content, or of an obscene nature

Respect the privacy and personal rights of others.

For example, it is a violation:

- To use electronic resources for harassment or stalking other individuals
- To tap a phone line or run a network sniffer or vulnerability scanner without authorization
- To access or attempt to access another individual’s password or data without explicit authorization
- To access or copy another user’s electronic mail, data, programs, or other files without permission
- To disclose information about students in violation of South Georgia State College or USG guidelines

Use of mobile payment card readers over the SGSC wireless network is prohibited.

For example, it is a violation:

- To use your mobile device as a credit card transaction system on the institution's wireless network
- To use products such as Square, Clover Go, PayPal Here, and InnerFence on the institution's wireless network

System and Network Administrator Responsibilities

System administrators and providers of South Georgia State College IT resources have the additional responsibility of ensuring the confidentiality, integrity, and availability of the resources they are managing. Persons in these positions are granted significant trust to use their privileges appropriately, for their intended purpose, and only when required to maintain the system. Any private information seen in carrying out these duties must be treated in the strictest confidence, unless it relates to a violation or the security of the system.

Security Caveat

Be aware that although computing and IT providers at South Georgia State College, and throughout the USG, are charged with preserving the integrity and security of resources, security can sometimes be breached through actions beyond their control. Users are therefore urged to take appropriate precautions such as:

- Safeguarding their account and password
- Taking full advantage of file security mechanisms
- Backing up critical data on a regular basis
- Promptly reporting any misuse or violations of the policy
- Using virus scan software with current updates
- Using personal firewall protection
- Installing security patches in a timely manner

Violations

Every user of South Georgia State College resources has an obligation to report suspected violations of the above guidelines or of the Appropriate Use Policy for IT Resources. Reports should be directed to Information and Instructional Technology at South Georgia State College.
Last Revised: 2013-Oct-07