COLLEGE of COASTAL GEORGIA

CITATION REFERENCE

Official Title: Acceptable Use Policy
Abbreviated Title: AUP
Volume: CCGA Policies
Responsible Office:
Originally Issued: June 14, 2022
Effective Date: June 14, 2022
Revised: June 14, 2022

Acceptable Use Policy

Policy Statement

Appropriate use of College of Coastal Georgia's Information Technology (IT) resources is an institution-wide undertaking necessitating all users promote responsible behavior and create safeguards against the abuse of IT resources. Guidelines regarding developing the Appropriate Use Policy (AUP) are established to provide an environment that encourages the free exchange of ideas and sharing of information.

Reason for Policy

This policy outlines the general standards for the appropriate use of IT resources, which include, but are not limited to, equipment, software, networks, data, and telephones, whether owned, leased, or otherwise provided by the College of Coastal Georgia. All users are expected to use IT resources responsibly, respecting the public trust through which these resources have been provided, the rights and privacy of others, the integrity of facilities and controls, state and federal laws, and USG policies and standards. Access to IT resources is a privilege and must be treated with the highest standard of ethics. Therefore, all users are obliged to abide by the following general standards.

Entities Affected by This Policy

This policy applies to all users including, faculty, staff, students, contractors, guests, external organizations, and individuals accessing IT resources.

Who Should Read This Policy

All faculty, staff, students, contractors, guests, external organizations, and individuals of the College of Coastal Georgia should read and understand this policy.

Contacts

Contact	Phone	E-Mail
Alan Ours	912-279-5762	aours@ccga.edu
Matt Hanak	912-279-5763	mhanak@ccga.edu

Website Address for This Policy

Related Document/Resources

None

Definitions

IT - Abbreviation for Information Technology which may be used to describe technology systems or resources. IT may also be used in lieu to reference the Technology Services Department.

Overview

Preserving access to IT resources is an effort that requires all users to act responsibly and guard against abuses. Users must abide by the following standards of appropriate and ethical use:

- Use only those IT resources for which you have authorization.
- Protect the access and integrity of IT resources.

- Abide by applicable local, state, federal laws, organizational policies, and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted material and University System of Georgia (USG) information.
- Use IT resources only for their intended purpose.
- Respect the privacy and personal rights of others.

College of Coastal Georgia and its users accept the following responsibilities and guidelines when using the College of Coastal Georgia's IT resources. This is put forth as a minimum set of standards for all areas of the College of Coastal Georgia and may be supplemented with specific departmental or organization-level guidelines. However, such additional guidelines must be consistent with this document and cannot supersede this document. These guidelines include 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 IT resources is granted based on acceptance of the following specific responsibilities: Use only those computing and 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 purposely look for or exploit security flaws to gain system or data access.

Protect the access and integrity of computing and IT resources. For example, it is a violation:

- To use excessive bandwidth.
- To release a virus or malicious program that damages or harms a system or network.
- To prevent others from accessing an authorized service.
- To send an email that may cause problems and disrupt service for other users.

- To attempt to degrade performance or deny service deliberately.
- To corrupt or misuse information.
- To alter or destroy information or resources without authorization.

Abide by applicable laws and College of Coastal Georgia policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software. For example, it is a violation:

- To download, use or distribute copyrighted materials, including pirated software, music, videos, or games.
- To not adhere to the College of Coastal Georgia licensing agreements has with its vendors and contractors.
- To make more copies of licensed software than the license allows.
- To operate and participate in pyramid or Ponzi schemes.
- To upload, download, distribute, or possess pornography.
- To upload, download, distribute, or possess child pornography.

Use computing and IT resources only for the intended purposes. 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 use College purchased software or devices for personal use or gains.
- To connect any personal computer or device to any College of Coastal Georgia domain network.
- To send a forged email.
- To misuse Internet Relay Chat (IRC) 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.

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 other individuals' passwords 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 USG Guidelines.
- To misrepresent one’s identity or relationship to the College of Coastal Georgia when obtaining or using a computer, network, or administrative privileges.

Email Use and Protection

College of Coastal Georgia email is provided as a tool to assist and facilitate state business, communications with students, faculty, and its representatives to conduct official business on behalf of College of Coastal Georgia. This section establishes a standard for the appropriate use and protection of College of Coastal Georgia email systems.

- The College of Coastal Georgia authorization and access control and password protection policies and standards shall govern access to email.
- Email passwords shall be encrypted and not be stored or passed in clear text.
- Email systems shall be protected from viruses, interception, and malicious intentions.

- Use of College of Coastal Georgia email systems for creating or distributing of any disruptive or offensive messages is prohibited.
- Users shall not distribute mass mailings about viruses or other malware warnings.
- All email monitoring of current employees must be reviewed and approved by the College of Coastal Georgia Technology Services or USG Legal Affairs.
- Unauthorized email forwarding is prohibited. Email forwarding must be approved by the email account user or the College of Coastal Georgia executive management.
- It is the responsibility of every College of Coastal Georgia employee with access to email to promptly report phishing, and spam messages to Technology Services.

File Sharing and Document Management

College of Coastal Georgia provides its faculty, staff, and students multiple ways to store, access, and share files and documents relating to business operations and education. All individuals utilizing technology resources must comply with the College of Coastal Georgia's Institutional Data Management Standards Policy. This policy has been created to protect sensitive data, including the personal data of students and employees. It is essential for compliance with federal, state, and the University System of Georgia data security regulations. The document management solutions available at the College of Coastal Georgia do not monitor compliance with the Institutional Data Management Standards Policy.

Technology Services does not monitor for sensitive data on prohibited third-party resources (Dropbox, Google Drive, etc.), as such it is prohibited to store sensitive/confidential information on these resources. It is the individual’s responsibility that data stored using these available tools adhere to the policy and legal requirements.

The acceptable resources provided by the College of Coastal Georgia that are available to store, access, and share documents and data are as follows. Any other service or resources to store USG data is prohibited unless approved by Technology Services.

- OneDrive
- SharePoint
- Share File System (U: Drive. R: Drive)

- MoveIt (files.usg.edu)

Cybersecurity Caveat

Be aware that although Technology Services and IT providers are charged with preserving the integrity and security of resources, security sometimes can 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 regularly.
- Promptly reporting any misuse or violations of the policy.
- Using virus scanning software with current updates.
- Using personal firewall protection.
- Installing security patches promptly.

Every user of the College of Coastal Georgia's IT resources has an obligation to report suspected violations of the above guidelines. Reports should be directed to the office, division, department, school, or administrative area responsible for the particular system involved.

Policy Compliance

Compliance Measurement
IT will verify compliance to this policy through various methods, including but not limited to, business tool reports and internal/external audits.

Exceptions
IT must approve any exception to the policy in advance.

Non-Compliance
Failure to comply with the appropriate use of these resources threatens the sharing of information, the free exchange of

ideas, and the secure environment for creating and maintaining information property, and subjects one to disciplinary actions. Any user of the College of Coastal Georgia found using IT resources for unethical and inappropriate practices has violated this policy and is subject to disciplinary proceedings, including suspension of system privileges, expulsion from school, termination of employment and/or legal action as may be appropriate.

Although all members of College of Coastal Georgia expect privacy, if a user is suspected of violating College of Coastal Georgia policy, their right to privacy may be superseded by the USG's requirement to protect the integrity of IT resources, the rights of all users, and the property of College of Coastal Georgia, the USG, and the state. College of Coastal Georgia thus reserves the right, upon approval by the Information Security Officer (ISO), the Chief Information Officer (CIO), for immediate action, and Human Resources, for investigative actions, to examine material stored on or transmitted through its resources if there is cause to believe that the standards for appropriate use are being violated by an organization, user, or a trespasser onto its systems or networks.

Responsibilities

The Responsibilities each party has in connection with this policy are:

Party	Responsibility

Forms

Appendices