Computer Use and Internet Access

Acceptable Use Policy for Technology Resources

The College provides technology resources for use by students, faculty, staff, and the general public. This technology includes but is not limited to, all College computing equipment, software, systems, networks, electronic mail, web site, and Internet access. These resources are the property of the College and are provided to the campus community to support the College's mission and institutional goals. The College reserves the rights to grant, restrict, or deny privileges and access to technology resources.

Use of the technology resources must be consistent with the stated mission, goals, policies, procedures, and priorities of the College. Use of College resources is a privilege and requires that users agree to abide by all relevant College policies and procedures, as well as all applicable federal, state, and local laws. Users are expected to conduct themselves in a responsible and ethical manner at all times.

Any use of College technology resources for illegal, inappropriate, or obscene purposes, or in support of such activities, is prohibited. Respect for intellectual property or copyright, ownership of data, security measures, and personal rights and privacy must always be demonstrated.

It should be clear that all personal use of computers to access pornographic websites will result in appropriate disciplinary action and may result in civil and criminal penalties for users. Personal use of computers for business purposes is prohibited and may constitute violation of the Alabama Ethics law. It is illegal to download music through the College computer network system. Employees who are found to be illegally downloading music will be subject to federal and state laws pertaining to such acts.

Email Monitoring

Gadsden State Community College may monitor all information stored, transmitted, received, or contained in the College email systems. Workplace files, internet use, and email may be monitored by the College. Information flowing through or stored on computers within the network is not considered confidential and is subject to monitoring by network administrators.

Personal Blogs and Websites

This policy is also applicable to content that you publish on the internet (e.g. your contributions to blogs, message boards and social networking or content-sharing sites) even if created, updated, modified or contributed to outside of working hours or when using personal IT systems.

When you post content to the internet that identifies you as an employee of the College and discusses your work, the College, or employees of the College, it is expected that you will conduct yourself appropriately and in a manner that is consistent with the policies of the College and the Alabama Community College System.
If you already have a personal blog or website which indicates in any way that you work for the College, or you intend to create a personal blog or website that will identify you as an employee of the College, you should report this to your immediate supervisor. Any blog or posting that clearly identifies that you work for the College in which you express any idea or opinion should also include a disclaimer stating that the views expressed are personal and do not represent the views or opinions of the College. Online publications which do not identify the author as an employee of the College and does not mention the College and are purely concerned with personal matters will normally fall outside the scope of this policy.

Violation of College and Alabama Community College System policies on internet sites is subject to investigation and sanctions within this policy and other applicable policies.

**Computer Hardware/Software**

Any personally-owned computing property or peripheral equipment (including wireless devices) brought to the College cannot be connected to the College administrative network without the approval of the employee’s Supervisor and Information Technology Services. No prior approval is needed to connect personal devices to the internet-only wireless networks; GSCC-SA and GSCC-FS. Personally-owned software cannot be loaded onto a College-owned computer unless it is directly related to the job position and is approved by the Supervisor. If any approved personally-owned computer software is loaded onto a College-owned computer, the license and documents must remain with the College computer on campus in the event of an audit. Computer software may be audited by Information Technology Services and others.

*Complete Policies on Computer Use and Internet Access may be found in the Catalog & Student Handbook.*

**Computer and Network Security**

Computer and network security is not solely an Information Technology Services responsibility. Each employee has certain responsibilities for securing their Gadsden State systems and access to those systems. The following are links to four policies that apply to all employees. Please review them and be sure your area of responsibility is in compliance. If you encounter any difficulties in complying, please contact the Chief Information Officer or the Information Technology help desk (256.549.8341) to schedule assistance.

**Laptop and Portable Device Encryption Policy**

1. **Purpose**
   The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained by Gadsden State Community College.

2. **Scope**
   This policy applies to all Gadsden State Community College (GSCC) employees, students,
vendors, contractors and others that may use a computer and/or servers that contain or may potentially have access to GSCC confidential or and personally identifiable information (PII).

3. **Policy**
   Sensitive information belonging to Gadsden State Community College should be stored on portable devices and/or removable media only when absolutely required in the performance of your assigned duties or when providing information required by state or federal agencies. Portable devices include but are not limited to laptop computers, tablets, smartphones, jump-drives, etc. When sensitive information is stored on a portable device or removable media, it **MUST be encrypted** in accordance with a currently approved encryption standard. Approved encryption standards will be maintained by the IT department.

   Sensitive information belonging to Gadsden State Community College should never be stored on personal portable devices and/or removable media. Additionally, portable devices and/or removable media containing sensitive information belonging to Gadsden State Community College may not be connected to, or used with, personal computers and other personally owned devices.

4. **Policy Compliance**
   4.1 **Compliance Measurement**
      The Information Technology (IT) department help desk may be contacted for assistance in selecting the appropriate encryption. The IT staff will verify compliance to this policy through various methods, including but not limited to, periodic walk-thru, business tool reports, internal and external audits, and feedback to owner of the device.

   4.2 **Enforcement**
      The Chief Information Officer is authorized to mitigate any non-compliance with this policy at any time either directly or through delegation to staff.

   4.3 **Exceptions**
      Any exception to the policy must be approved by the Chief Information Officer.

5. **Revision History**
   Date: August 2018
   Description: Revised

---

**Smartphone and Tablet Email Security**

1. **Purpose**
   The purpose of this policy is to minimize the risk of loss or exposure of sensitive information communicated via email on behalf of Gadsden State Community College.

2. **Scope**
   This policy applies to all Gadsden State Community College (GSCC) employees, students, vendors, contractors and others that may use an administrative GSCC email account on a portable device such as a smartphone or tablet.

3. **Policy**
   Gadsden State Community College email accounts may be used on smartphone and/or tablet devices to facilitate official duties associated with GSCC. If email is to be stored in an account on the device, GSCC requires the use of an appropriate PIN or password. The College reserves the right to remotely wipe the contents of any device reported lost, stolen or maliciously using a
GSCC email account. Users may use a web-browser on a smartphone or tablet to access email without an associated PIN requirement if emails are not stored on the device. Alternatively a user may use the Microsoft Outlook Web Access (OWA) app, in which case the college reserves the right to remotely wipe the contents of the OWA app but not the entire phone in the case of a lost, stolen or maliciously used GSCC email account.

4. Policy Compliance
   4.1 Compliance Measurement
   Appropriate settings will be maintained on GSCC email servers to enforce a PIN requirement of smartphones and tablets.

   4.2 Enforcement
   The Chief Information Officer is authorized to mitigate any non-compliance with this policy at any time either directly or through delegation to staff.

   4.3 Exceptions
   Any exception to the policy must be approved by the Chief Information Officer.

5. Revision History
   Date: August 2018
   Description: Revised

Workstation Security Policy

1. Purpose
   The purpose of this policy is to provide guidance for workstation security at Gadsden State Community College in order to ensure the security of information both on the workstation and information the workstation may have access to. The primary intent is to appropriately protect confidential and personally identifiable information (PII) in employees’ and students’ records.

2. Scope
   This policy applies to all Gadsden State Community College (GSCC) employees, contractors, students, vendors and all others that access GSCC confidential and/or sensitive information.

3. Policy
   Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including personally identifiable information (PII) and that access to sensitive information is restricted to authorized users.

   3.1 Users of GSCC affiliated workstations shall consider the sensitivity of the information, including PII that may be accessed and minimize the possibility of unauthorized access.

   3.2 Gadsden State Community College will implement physical and technical safeguards for all workstations containing or having access to PII and restrict access to authorized users.

   3.3 Appropriate measures include but are not limited to:
   - Restricting physical access to workstations to only authorized personnel.
   - Securing workstations (i.e., screen lock or logout) prior to leaving the area to prevent unauthorized access. The IT department is authorized to enforce a 15-minute screen inactivity timeout on the MIS domain workstations via
electronic policy updates. Locking the workstation will not close documents or logout of work sessions but will require entering the workstation password to resume the session.

- Ensuring workstations are used for authorized business purposes only.
- Never installing unauthorized software on workstations.
- Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.
- Complying with the Laptop and portable Device Encryption Policy.
- Installing privacy screen filters or using other physical barriers to alleviate exposing data.
- Exit running applications and close open documents when leaving for extended periods of time.
- Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).

4. **Policy Compliance**
   4.1 **Compliance Measurement**
   ITS staff will verify compliance to this policy through various methods, including but not limited to, periodic walk-thru, automated monitoring, internal and external audits, and provide feedback to the workstation owner.
   
   4.2 **Enforcement**
   The Chief Information Officer is authorized to mitigate any non-compliance with this policy at any time either directly or through delegation to staff.

   4.3 **Exceptions**
   Any exception to the policy must be approved by the Chief Information Office.

5. **Revision History**
   Date: August 2018
   Description: Revised

**Server Malware Protection Policy**

1. **Purpose**
   The purpose of this policy is to outline which server systems are required to have anti-virus and/or anti-spyware applications.

2. **Scope**
   This policy applies to all servers connected to any Gadsden State Community College (GSCC) network. This explicitly includes any system for which the Information Technology Services (ITS) department has the responsibility to administer. This also includes all server systems setup for use at any GSCC campus or facility, regardless of whether the ITS department retains administrative obligation or not.

3. **Policy**
   ITS staff will adhere to this policy to determine which servers will have anti-virus and/or anti-spyware applications installed on them and to deploy such software and/or hardware appliances
as appropriate.

3.1 Anti-Virus
All servers not explicitly exempted MUST have an anti-virus application installed that offers scanning protection to files and applications running on the target system if they meet one or more of the following conditions:
- Non-administrative users have remote access capability
- The system is a file server
- Microsoft Share access is open to this server from systems used by non-administrative users
- HTTP/FTP access is open from the Internet
- The Director of Computer Systems or Chief Information Officer determines that the system warrants the installation of anti-virus.

3.2 Mail Server Anti-Virus
Mail servers MUST have either an external or internal anti-virus scanning application or appliance that scans all mail destined to and from the mail server.

3.3 Anti-Spyware
All servers MUST have an anti-spyware application installed that offers real-time protection to the target system if they meet one or more of the following conditions:
- Any system where non-technical or non-administrative users have remote access to the system and ANY outbound access is permitted to the Internet
- Any system where non-technical or non-administrative users have the ability to install software on their own
- The Director of Computer Systems or Chief Information Officer determines that the system warrants the installation of anti-spyware.

3.4 Notable Exceptions
An exception to the above standards will generally be granted with minimal documentation if one of the following notable conditions apply to this system:
- The system is a dedicated SQL server
- The system is used as a dedicated mail server
- The system is not a Windows based platform

4. Policy Compliance
4.1 Compliance Measurement
The Director of Computer Systems will monitor compliance to this policy through various methods, including but not limited to, manual inspection of servers, monitoring tool reports, internal and external audits, and provide feedback to the Chief Information Officer upon request.

4.2 Enforcement
The Chief Information Officer is authorized to mitigate any non-compliance with this policy at any time either directly or through delegation to staff.

4.3 Exceptions
Any exception to the policy must be approved by the Chief Information Officer.