GNTC Acceptable Computer Use Guidelines

The following is meant to serve as clarification of the Technical College System of Georgia policy "Acceptable Computer and Internet Use" as it applies to computer use on Georgia Northwestern Technical College campuses. GNTC does not attempt to articulate all required or unacceptable behavior by its users. Therefore, each user's judgment on appropriate conduct must be relied upon. To assist in such judgment, and assure adherence to state policy, the following guidelines have been created.

1. Security: (reference subsections h. and o. of TCSG Acceptable Computer and Internet Use Policy)
   1.1. An access account assigned to a user must not be used by any other individual. Users are responsible for the proper use of their accounts, including proper password protection.
      1.1.1. Proper use of an account would prohibit activities such as: obtaining another user's password, or allowing friends, family, co-workers, or any other individual use of your account.
      1.1.2. Proper password protection would prohibit activities such as: storing passwords in an unlocked desk drawer, or on sticky notes hidden under keyboard, monitor, etc…

   1.2. For user protection and for the security of campus computing resources, users must exit any networked applications that requires a password (e.g. Banner, Peoplesoft, Secure Shell, etc…) and logout or lock the computer console before leaving a networked computer or your office computer.

   1.3. All written passwords should be kept in a locked and secure location.

   1.4. The user is responsible for maintaining the security of his/her own data and for making backups of such data unless arrangements for the backup of such data is stored on servers maintained by the department of Technology Services

   1.5. You should never give out your password via email or unsolicited phone call. GNTC Technology Services personnel will never ask for your username/password over the phone or via email correspondence

2. Access: (reference subsections j. and o. of TCSG Acceptable Computer and Internet Use Policy)
   2.1. GNTC computer systems are made available and accessible for use in research and education by the faculty, staff, and students of the college. Authorized access levels for specific users will be determined by the divisional vice president in conjunction with the director or assistant director of Information Technology. Banner access levels will be determined by the appointed data steward and submitted to the database administrator for review and implementation.

   2.2. Attachment of any device to a network port in any GNTC facility is not permitted without inspection, and approval by Technology Services personnel. Such devices include, but are not limited to: computers, tablets, access points, routers, gaming devices, etc.

2.3. Use of classroom instructor or podium computers is limited to the following:
   2.3.1. GNTC employees who possess a valid login username
   2.3.2. Authorized guests who are directly supervised by a full-time GNTC employee
   2.3.3. Part-time Continuing Education instructors who have received a temporary login account, and written instructions from the Office of Economic Development regarding proper use of the system
   2.3.4. Instructor supervised students who use the classroom computer system for the purpose of in-class presentations

2.4. Authorized visitors, GNTC students, faculty, and staff are permitted to connect via open wireless to the networks provided. (some of which are unsecured wireless networks) PUI or CUI should never be transmitted over a non-secured wireless network.

3. Software and Copyrighted Material: (reference subsections a., b., d., f., l., and o. of TCSG Acceptable Computer and Internet Use Policy)
   3.1. All GNTC computer users are required to follow all copyright laws (see TCSG Policy). Downloading, reproduction, and/or distribution of licensed materials is prohibited without proper authorization from the author or creator. Users must not publish information, messages, graphics, or photographs from any web page, without the express permission of the author or creator.

   3.2. Peer-to-Peer file sharing resulting in file-sharing, downloading, or uploading substantial parts of a copyrighted work without authority constitutes a violation of copyright laws. For more information, visit the US Copyright Office. GNTC blocks P2P file sharing on the web content filter in compliance with the Higher Education Opportunity Act. (HEOA).

   3.3. A copy of the license agreement for all software purchased and used by any department or division on the GNTC campus must be submitted to the Director Of Information Technology prior to software installation. It is the shared responsibility of the department of Technology Services and the end user to ensure that all license provisions (including copyright, use, duplication, simultaneous installations, etc.) be honored. Use of any personal software or hardware on GNTC computers must be authorized by the director or assistant director of Information Technology prior to installation or use.

   (Installation of freeware/shareware and other software which constitutes the "Instructor guide" for a course offering is permitted without prior authorization. However, users are responsible for following all licensing restrictions for any such software.)

   3.4. Requests for installing software in a computer laboratory environment should be submitted in writing using the helpdesk support system at least 10 working days prior to the start of the next instructional period. The department of Technology Services may also work with instructional staff in allowing alternative installation procedures when emergency situations arise.

4. Desktop System Integrity: (reference subsection l. of TCSG Acceptable Computer and Internet Use Policy)
   4.1. Users may not install hardware or change equipment configurations on desktop computer systems without prior approval of the department of Technology Services.

   4.2. Food or drink may be restricted in student lab areas. Specific lab policies will apply. Check the specific policies posted in the lab area.

5. Laptop System Integrity: (reference subsections h., l., and o. of TCSG Acceptable Computer and Internet Use Policy)

5.1. All GNTC laptops must be initially configured by the department of Technology Services to meet appropriate technical and security specifications. (e.g., anti-virus, anti-spyware, operating system patches, etc…).

5.2. Assigned users of GNTC laptops will be instructed on the proper procedure and intervals to maintain the security configuration.

5.3. GNTC laptops are subject to the software provisions detailed in section 3 at all times.

6. Internet Access/Use: (reference subsections a., b., c. of TCSG Acceptable Computer and Internet Use Policy)

6.1. Internet access is provided for all GNTC employees and students. This access is contingent on use of an authorized user account for login purposes.

6.2. Occasional personal use of Internet connectivity and/or email is permitted. Such use should be brief, infrequent, and shall not interfere with the user's performance, duties, or responsibilities.

6.3. Like most colleges and businesses, GNTC has limited Internet bandwidth. To preserve adequate bandwidth for legitimate educational activities, do not download or stream high bandwidth content which is not directly related to the educational goals and mission of GNTC. This would include, but not be limited to: internet radio, videos, movies, games, etc.

6.4. For security purposes, all Internet access is governed by appropriate firewall access rules. This is to protect the security and integrity of GNTC systems from possible Internet based threats. If a user at GNTC is denied access to a vital Internet site or service based on firewall access rules, the director or assistant director of Information Technology will make every effort to allow access without compromising campus security or traffic flow.

6.5. Internet content delivered to the GNTC campus is also filtered for content whereby the filter guidelines will be agreed upon and reviewed. GNTC is not responsible for discriminatory, offensive, sexually explicit, or obscene material which may circumvent filter settings. If filter rules block legitimate, necessary content from entering the campus, the department of Technology Services will make every effort to allow the needed content without compromising overall filter functionality.

7. Email:

7.1. All employee email at GNTC is archived per TCSG email archive policy for a period of 5 years.

7.2. Employees of GNTC are not to use wide scale distribution lists such as ALL_GNTC, WCC_GNTC, FCC_GNTC, etc. to send emails containing any information, pictures, or other content which is not directly related to GNTC college goals or mission statements.

7.3. The use of '**Reply All**' when responding to an email should be considered carefully on a case-by-case basis as it is very possible to expose Personally Identifiable Information (PII), Confidential User Information (CUI), or other information to unintended recipients!

7.4. All business email correspondence must utilize GNTC provided email systems. This includes all email correspondence with students.

8. Portable Storage and Transmittal of Confidential User Information (CUI) or Personally Identifiable Information (PII)

8.1. Information not intended for public dissemination (ie. CUI or PII) that is stored on any type of portable

media or computing device at a minimum must be encrypted using an industry standard symmetric key encryption algorithm such as AES 128 or AES256. This includes information stored on, but not limited to, notebook PCs, hard drives, smartphones, CDs, DVDs, Flash Memory Devices (USB drives), etc. Information not intended for public dissemination that exists in any electronic form stored anywhere other than on a non-portable computer located at a GNTC site **must** be encrypted using the minimum specified encryption standard, and physical security of that device maintained.

8.2. All transmission of email to portable devices such as smartphones, tablet, etc. must use TLS 1.2 or higher. No clear text transmission of GNTC faculty/staff email to any portable device is permitted. Non-encrypted text messaging of PUI or CUI is prohibited.

8.3. If there is a need to mail Confidential or Personally Identifiable Information stored on digital media, then the digital media must be encrypted using the minimum specified encryption standard, and the mail package must be trackable to ensure that it is delivered to the intended recipient.

Additional Computer Security Policy and User Resources:

- Technical College System of Georgia Acceptable Computer and Internet Use Policy
- User Security Awareness Videos
  - The Best Free 1 Hour Security Awareness Training
  - Mobile Device Security

Important: If you are viewing a printed copy of the GNTC Acceptable Computer Use Guidelines, then please be sure to visit: http://www.gntc.edu/fullpanel/uploads/files/computeruseguidelines.pdf for the most current changes, updates, and revisions.

GNTC does not discriminate on the basis of race, color, creed, national or ethnic origin, gender, religion, disability, age, political affiliation or belief, veteran status, or citizenship status (except in those special circumstances permitted or mandated by law).

Revised 2/22/2018 – dt