PROCEDURE:
3.3.4p1. Acceptable Computer and Internet Use

Revised: *August 2008; September 2009; September 16, 2010; September 21, 2011; September 19, 2012; September 18, 2013; September 17, 2014; September 16, 2015; September 21, 2016; August 16, 2017; August 15, 2018; August 21, 2019*
Last Reviewed: *August 2008; September 2009; September 16, 2010; September 21, 2011; September 19, 2012; September 18, 2013; September 17, 2014; September 16, 2015; September 21, 2016; August 16, 2017; August 15, 2018; August 21, 2019; August 19, 2020; August 17, 2021; August 17, 2022; August 15, 2023*
Adopted: *August 2007*

I. PURPOSE

In making decisions regarding access to the Internet and use of its computers, the College considers its own stated educational mission, goals, and objectives. Electronic information research skills are now fundamental to preparation of citizens and future employees. The College expects faculty to blend thoughtful use of the Internet throughout the curriculum and provide guidance and instruction to students in its use. As much as possible, access from Technical Colleges to Internet resources should be structured in ways that point students to those resources that have been evaluated prior to use. While students shall be able to move beyond those resources to others that have not been previewed by staff, they shall be provided with guidelines and lists of resources particularly suited to learning objectives. Students and employees utilizing Technical College-provided Internet access are responsible for good behavior on-line just as they are in a classroom or other area of the college.

The purpose of College-provided Internet access is to facilitate communications in support of research and education. To remain eligible as users, students' use must be in support of and consistent with the educational objectives of the College. Access is a privilege, not a right. Access entails responsibility.

II. RELATED AUTHORITY

TCSG Procedure 3.3.4p. Acceptable Computer and Internet Use
TCSG Information Security Standards
State Board Policy 3.2.1. Intellectual Property
Ogeechee Technical College Procedure 3.3.4p2. Email Use
Ogeechee Technical College Procedure 3.3.4p3. Privacy Notice to Computer Users
Ogeechee Technical College Procedure 3.3.4p4. Remote Access
Ogeechee Technical College Procedure 3.3.4p5. Laptop Computer
The Gramm-Leach-Bliley Act
The Federal Trade Commission (FTC) Standards for Safeguarding Customer Information; Final Rule (16 CFR Part 314)
Ogeechee Technical College Marketing and Community Relations Plan
O.C.G.A. § 20-4-11 – Powers of the Board
O.C.G.A. § 20-4-14 – TCSG Powers and Duties

III. APPLICABILITY

This procedure applies to all employees and students of Ogeechee Technical College.

IV. DEFINITIONS

None.

V. ATTACHMENTS

Acknowledgement of Acceptable Computer & Internet Use

VI. PROCEDURE

Scope

This procedure is posted on the College intranet, and it is distributed to each new employee during orientation. When updates occur, the Vice President for Technology and Institutional Support will advise employees via email. It is the responsibility of each employee to return the "Acknowledgement" form to Human Resources (HR). HR is responsible for ensuring that each employee's file contains a signed acknowledgement form.

General

Using a computer without permission is theft of services and is illegal under state and federal laws. Federal law prohibits misuse of computer resources.

In addition, the following specific computer crimes are prohibited by state law in Georgia (O.C.G.A. § 16-9-90 et seq.):

1. Computer theft (including theft of computer services, intellectual property such as copyrighted material, and any other property);
2. Computer trespass (unauthorized use of computers to delete or alter data or interfere with others' usage);
3. Computer invasion of privacy (unauthorized access to financial or personal data or the like);
4. Computer forgery (forgery as defined by other laws, but committed on a computer rather than on paper);
5. Computer password disclosure (unauthorized disclosure of a password resulting in damages exceeding $500 - in practice, this includes any disclosure that requires a system security audit afterward); and
6. Misleading transmittal of names or trademarks (falsely identifying yourself or falsely claiming to speak for a person or organization by using their name, trademark, logo, or seal).
7. Malware (malicious software programs and applications designed to damage or cause other unwanted actions on a computer system).

Users should not expect files stored on College-based computers to be private. Electronic messages and files stored on College-based computers shall be treated like other College premises that are temporarily assigned for individual use. Administrators may review files and messages in an effort to maintain system integrity and in an effort to ensure that users are acting responsibly. Moreover, College officials shall cooperate

with law enforcement officials who are properly authorized to search College computers and computer systems.

All information created, stored or transmitted by College computers or networks is subject to monitoring for compliance with applicable laws and policies.

Users are prohibited from maintaining written lists of electronic accounts and passwords on or near workstations or work areas.

In addition to the computer crimes delineated in O.C.G.A. 16-9-93, the following uses of College-provided computers, networks and Internet access are not permitted:

a. To create, access or transmit sexually explicit, obscene, or pornographic material;
b. To create, access or transmit material that could be considered unlawful conduct based on race, color, creed, national or ethnic origin, gender, religion, disability, age, genetic information, political affirmation or belief, disabled veteran, veteran of the Vietnam Era or citizenship status addressed directly to any individual or group that has the purpose or effect of unreasonably and objectively interfering with that individual or group's: (1) performance, (2) work or educational environment or (3) ability to participate in an educational program or activity;
c. To violate any local, state or federal statute;
d. To vandalize, damage, or disable the property of another individual or organization;
e. To access another individual's password, materials, information, or files without permission;
f. To violate copyright or otherwise use the intellectual property of another individual or organization in violation of the law, including software piracy;
g. To conduct private or personal for-profit activities. This includes use for private purposes such as business transactions, private advertising of products or services, and any activity meant to foster personal gain;
h. To knowingly endanger the security of any College computer or network;
i. To willfully interfere with another's authorized computer usage;
j. To knowingly connect any computer to any of the College networks unless it meets technical and security standards;
k. To create, install, or knowingly distribute a computer virus, "Trojan horse," or other surreptitiously destructive program on any College computer or network facility, regardless of whether any demonstrable harm results;
l. To modify or reconfigure the software or hardware of any College computer or network without proper authorization;
m. To conduct unauthorized not-for-profit business activities;
n. To conduct any activity or solicitation for political or religious causes;
o. To perform any activity that could cause the loss, corruption of, prevention of rightful access to, or unauthorized distribution of College data and information;
p. To create, access, or participate in online gambling. Occasional access to information or websites of the Georgia Lottery Corporation shall not constitute nor be considered inappropriate use; and

q. To capture and/or record network traffic without authorization;
r. To knowingly transmit copyrighted material using peer to peer file sharing technology;
s. To knowingly evade Internet content filtering or other traffic monitoring tools using VPN, Proxy Services, or similar technologies.

Occasional personal use of Internet connectivity and e-mail that do not involve any inappropriate use as described above may occur, if permitted by the College. Any such use should be brief, infrequent, and shall not interfere with User's performance, duties and responsibilities. Refer to Procedure 3.3.4p2. Email Use for more information regarding electronic mail usage.

Users of College computers and computer systems are subject to the College's procedure on the development of Intellectual Property.

Users of College computers and computer systems or hosted services are subject to the Information Security Standards. The College makes no warranties of any kind, express or implied, for the computers, computer systems and Internet access it provides. The College shall not be responsible for any damages users suffer, including but not limited to loss of data resulting from delays or interruptions in service. The College shall not be responsible for the accuracy, nature or quality of information gathered through College diskettes, hard drives servers, or other storage devices; nor for the accuracy, nature or quality of information gathered through College-provided Internet access. The College shall not be responsible for personal property used to access its computers or networks or for College-provided Internet access. The College shall not be responsible for unauthorized financial obligations resulting from College-provided access to the Internet.

Penalties
Violations of these policies incur the same types of disciplinary measures as violations of other System or technical college policies or state or federal laws, including criminal prosecution.

VII. RECORD RETENTION

All related documents generated or collected pursuant to this procedure shall be maintained in a manner consistent with the Georgia Archives' Retention Schedule for State Government Paper and Electronic Records