



# Student Device Handbook

## GCS Strategic Plan

*“Use technology as an amplifier for learning, creating, making, connecting, communicating, collaborating and problem solving.”*



## Table of Contents

GCS Goals for Student Use.....	2
Access to Information .....	2
Board Policy and Procedure:.....	2
Digital Citizenship Education.....	2
Unacceptable Uses.....	3
Monitoring .....	3
Filtering .....	3
Damaged/Lost/Stolen Device and/or Accessories.....	3
Security .....	4
Vandalism/Intentional Damage .....	4
Personal Technology Device (PTD) Rules.....	4

Access to the GCS network, the Internet, and electronic devices is a privilege provided to students solely to support student education, research, and career development, and is therefore subject to certain restrictions as set forth by the Board of Education and/or the Superintendent. The below regulations apply to all students and include all aspects of network use, whether via desktop or laptop computer, or personal technology device owned by GCS or the individual student, parent, or other third party.

### **Agreement**

**All students must accept the terms of the Certification of Review and Agreement prior to accessing the GCS network and checking out a device for home use. Parents must sign the form stating they have read the Student Handbook.**

### **GCS Goals for Student Use**

- To support the implementation of local curricula and the North Carolina Standard Course of Study;
- To enhance learning opportunities by focusing on the application of skills in information retrieval, searching strategies, research skills, critical thinking, communication, collaboration, and creativity;
- To encourage appropriate career development; and
- To promote life-long learning.

### **Access to Information**

Students will be able to access information that may include:

- Information, news, and resources from businesses, libraries, educational institutions, government agencies, research institutions, GCS online school media center catalogs, online textbooks and tutorials, other digital media content, and a variety of other sources;
- Public domain and shareware software; and
- Telecommunications with individuals and groups around the world.

### **Board Policy and Procedure**

- [JCDAE / JCDAE-P](#) – Harassment by students
- [EFE / EFE-P](#) – Acceptable use of electronic transmission capabilities

### **Student Handbook**

The student handbook can be found on the Guilford County Schools website or by [clicking here](#).

### **Digital Citizenship Education**

GCS will provide [digital citizenship education](#) to all students that addresses appropriate online behavior, including interactions with other individuals online, as well as cyberbullying awareness and response.

### **Digital Citizenship Rules**

Students shall be taught the importance of appropriate, safe behavior when using the GCS network to access information over the Internet. Users must abide by [iSafe Digital Citizenship rules](#), which include, but are not limited to:

- Students must be polite; rudeness will not be tolerated;
- Students must use appropriate language; use of profanity, vulgarities, abusive, or inappropriate language will not be allowed;
- Students must practice appropriate online behavior
- In any electronic communications, students must not reveal any personal information about others, such as full name, personal address, or phone numbers.

## **Penalties for Unacceptable Uses**

Students who violate any of the following rules are subject to disciplinary consequences set forth in the Code of Student Conduct, which may include suspension or expulsion from school as well as possible criminal prosecution or civil penalties under federal or state law.

## **Unacceptable Uses**

Transmission of material in violation of any federal or state law, regulation, or GCS policy or regulation is prohibited. Unacceptable uses include, but are not limited to, the following types of conduct:

1. Taking any actions that may disrupt the GCS network;
2. Knowingly introducing or attempting to introduce viruses or other malware into the network;
3. Unauthorized access (“hacking”) into computer systems or networks;
4. Logging into the network on a personal account and allowing others to access that account, unless permitted by an instructor for collaboration purposes;
5. Accessing proxy avoidance sites;
6. Encouraging or committing unlawful acts, violations of the GCS Code of Student Conduct, or using the GCS devices and/or network to promote illegal activities;
7. Accessing or using threatening or obscene material;
8. Accessing pornography;
9. Using discriminatory, defamatory, offensive, or harassing statements or language including disparagement of others based on their race, color, ancestry, national origin, sex, sexual orientation, socioeconomic status, academic status, gender identity or expression, age, disability, religious, or political beliefs through any means including phone, online, or other digital communications;
10. Sending or soliciting abusive or sexually oriented messages or images;
11. Accessing material that is harmful to minors;
12. Violating copyright laws, including duplication of software or plagiarism;
13. Utilizing the GCS network for commercial purposes;

## **Monitoring**

GCS will monitor the online activities of students. Activity by users is not confidential or private.

## **Filtering**

GCS will maintain centralized software in order to provide Internet control and filtering. The filtering software is intended to allow valuable online Internet access while, to the extent possible, inhibiting access to content that is obscene, pornographic, harmful to minors, or whose purpose is to promote, encourage or provide the skills to commit illegal activities, including gambling, use of illegal drugs, hate speech, or criminal skills. The filtering software is also intended to prohibit access to sites for online merchandising, alternative journals, and games. GCS will make every effort to update the filtering software on a daily basis.

## **Ownership**

The device is permanent property of Guilford County School District.

## **Damaged/Lost/Stolen Device and/or Accessories**

Student(s) should notify school staff as soon as possible if their GCS issued device is damaged, lost, or stolen. If a student’s device is stolen, the student should file a police report and share the case number with the school. Devices stolen outside of school should be reported to the local police. Devices stolen at school should be reported to the SRO at the school.

## **Privileges**

Use of the GCS network and electronic devices is a privilege, not a right. Inappropriate use or other violation of the provisions of this regulation may result in limitation or cancellation of user privileges and possible

disciplinary actions under appropriate federal or state statutes or the GCS Code of Student Conduct. Activity by users is not confidential or private.

### **Additional School-Specific Policies**

Principals are authorized to develop and implement additional rules for the use of devices on school campuses under their control. Any such rules shall be communicated to the students.

### **Security**

Security on the GCS network is a high priority. Attempts to tamper with the network, individual user accounts, software applications, to access the network using the name and password of another user, or to share a password may result in cancellation of user privileges. Email and search history is not private; system administrators have access to all email and device data. Email messages relating to or in support of illegal activities will be reported to the authorities, and appropriate disciplinary action will follow. Guilford County Public Schools has safeguards in place to protect your child. **GCS complies with the filtering requirements mandated by the Children's Internet Protection Act (CIPPA) and Children's Online Privacy Protection Act (COPPA).**

### **Vandalism/Intentional Damage**

Vandalism will result in cancellation of user privileges and disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy network or computer equipment and/or data of anyone connected to the network. This includes, but is not limited to, uploading, creating, or transmitting computer viruses or worms. Vandalism of networks and computer systems, including unauthorized access, may be a violation of criminal law. Parent/Guardian will be responsible for paying for the damage or replacing the device (\$525 if Lenovo).

### **Personal Technology Device (PTD) Rules**

To encourage growth, creativity, collaboration, and higher achievement, the Superintendent may authorize the use of PTDs during school hours by students at selected high schools. Students at those schools will be permitted to use PTDs for educational purposes only.

## Footnotes

1. A personal technology device (“PTD”) is a portable Internet accessing device designed to transmit communications by voice, written characters, words, or images, share information, record sounds, process words, and/or capture images, such as a laptop, tablet, smart-phone, cell-phone, PDA, or e-reader.
2. Unless otherwise stated, references to “parents” include one or both parents, legal guardian, or legal custodian of a student, or person acting in loco parentis to the student.
3. Student behavior guidelines are set forth in the Code of Student Conduct, which is updated and made available to students each year.
4. Cyberbullying is the use of information and communication technologies, including but not limited to email, cell phones, text, still photograph or video messages, instant messaging, defamatory personal web sites, and online personal or public web sites or journals, to convey an offensive, racial, derogatory, bullying, or obscene message to another person, including but not limited to references to race, color, ancestry, national origin, gender, socioeconomic status, academic status, gender identity or expression, sexual orientation, religion, physical or sensory disability, and/or physical appearance.
5. The term malware, another word for malicious software, means “computer software designed to be destructive or disruptive, such as computer viruses and worms.” (Black’s Law Dictionary).
6. “[A proxy] builds a firewall, which prevents attackers from gaining access to private information. It also protects users against harmful websites containing viruses.” Proxy avoidance sites “allow users to bypass the proxy and view any sites they wish. This allows users access to restricted sites. ([www.ehow.co.uk](http://www.ehow.co.uk)).
7. The term harmful to minors means “any picture, image, graphic image file, or other visual depiction that: 1) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; 2) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and 3) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.” (Children’s Internet Protection Act).
8. The Photo and Video Release form is available in the GCS Student Handbook that is distributed to every student at the beginning of the school year.
9. GCS is not responsible for acquiring, using, servicing, or maintaining devices or data plans.
10. GCS property means all property owned or operated by the Guilford County Board of Education, including school campuses and buildings, athletic fields, playgrounds, parking lots, bus stops, District-owned vehicles including school buses and activity buses, and any other properties owned or controlled by GCS.