George County School District's
Technology Handbook
2025-2026

I. Introduction

Welcome to the George County School District's (GCSD) Technology Handbook. This document serves as a comprehensive guide for all members of our school community—students, staff, and parents/guardians—regarding the effective, responsible, and safe use of technology resources within our district.

The GCSD is committed to providing a rich and engaging learning environment, and technology plays a vital role in achieving this goal. By embracing digital tools, we aim to:

- Enhance teaching and learning experiences.
- Foster critical thinking, creativity, and problem-solving skills.
- Prepare students for success in the technologically advanced world.
- Facilitate efficient communication and administrative processes.

This handbook outlines policies, procedures, and best practices to ensure that our technology resources are utilized respectfully, ethically, securely, and in alignment with our educational mission. All users are expected to familiarize themselves with and adhere to the guidelines presented herein.

II. Purpose and Scope of Technology Use

Technology resources, including but not limited to computers, networks, internet access, software, and peripheral devices, are provided primarily for educational and administrative purposes. These resources are an extension of the classroom and workplace, and their use is subject to the same standards of conduct expected in all other school environments.
Educational Use: Technology should be leveraged to support curriculum goals, facilitate research, enable collaboration, and enhance digital literacy.
Administrative Use: Technology aids in efficient school operations, communication, data management, and professional development.
Personal use of district technology should be minimal, not interfere with educational or administrative objectives, and always comply with all district policies.

III. Acceptable Use Policy (AUP) Summary

This Technology Handbook operates in conjunction with the district's official **Acceptable Use Policy (AUP)**. The AUP is a separate, more detailed document that all students, staff, and volunteers are required to read, understand, and sign before gaining access to district technology resources.

Key Principles of the AUP (Summarized):

- **Respect for Property:** Treat all district technology equipment with care.
- **Responsible Conduct:** Use technology ethically, legally, and in a manner that supports the educational environment.
- **Privacy and Confidentiality:** Respect the privacy of others and understand that district systems are monitored.
- **Digital Citizenship:** Engage in online interactions responsibly, respectfully, and safely.
- **Security:** Protect accounts, passwords, and the integrity of the network.

Users are strongly encouraged to review the full AUP document for complete details and specific regulations.

IV. Roles and Responsibilities

Effective technology integration requires collaboration and clear responsibilities from all stakeholders.

A. District Administration (Superintendent, Principals)

- Establish and enforce district-wide technology policies and procedures.
- Allocate resources for technology infrastructure, support, and professional development.
- Ensure compliance with federal and state regulations (e.g., CIPA, FERPA).
- Promote a culture of responsible technology use and digital citizenship.

B. Technology Department

- Manage, maintain, and secure the district's technology infrastructure (networks, servers, devices, software).
- Provide technical support and troubleshooting for staff and students.
- Ensure compliance with federal and state regulations (e.g., CIPA, FERPA).
- Implement and manage content filtering, security measures, and data backups.
- Research and recommend new technologies to support educational goals.
- Provide training and resources for staff in technology use.

C. Teachers and School Staff

- Integrate technology effectively into curriculum and instruction.
- Model appropriate and responsible technology use for students.
- Supervise students' use of technology in classrooms and labs.
- Educate students about digital citizenship, online safety, and the AUP.

- Report technology issues, inappropriate use, or security concerns to the Technology Department or administration.
- Participate in professional development to enhance technology skills.

D. Students

- Adhere to the district's AUP and all technology-related policies.
- Use technology resources respectfully, ethically, and responsibly for educational purposes.
- Protect their login credentials and personal information.
- Report any damage, malfunction, or inappropriate content/activity to a staff member.
- Engage in positive digital citizenship practices.
- Understand that technology use is a privilege, not a right.

E. Parents/Guardians

- Review and discuss the AUP and this handbook with their children.
- Support and reinforce responsible technology use at home.
- Communicate with school staff about technology concerns or questions.
- Monitor their child's online activities, especially when using personal devices.
- Understand that school technology resources are subject to monitoring.

V. Network and Internet Use

The GCSD's network and internet access are powerful tools for learning and communication, but their use comes with significant responsibilities.

A. Access and Security

- **User Accounts:** Each user is assigned a unique account and password. Accounts are for individual use and must not be shared.
- **Passwords:** Choose strong, unique passwords and keep them confidential. Change passwords regularly as advised by the Technology Department.
- **Unauthorized Access:** Any attempt to gain unauthorized access to district systems, networks, or data is strictly prohibited and will result in disciplinary action and potential legal consequences.
- **Network Integrity:** Do not introduce viruses, malware, or any unauthorized software that could compromise the network's security or performance.

B. Filtering and Monitoring (CIPA Compliance)

- In compliance with the Children's Internet Protection Act (CIPA), the district employs content filtering technology to block access to obscene, pornographic, or harmful content.

- Attempts to bypass or circumvent the filtering system are strictly prohibited.
- All internet traffic, network activity, and communications on district systems are subject to monitoring and logging by authorized personnel for security, troubleshooting, and compliance purposes. Users should have no expectation of privacy.

C. Bandwidth and Data Usage

- Use network resources efficiently. Avoid activities that consume excessive bandwidth or storage (e.g., large file downloads unrelated to education, streaming non-educational video/audio).
- Respect data storage limits on district servers. Save essential educational files to designated cloud storage or network drives.

VI. Hardware and Software

A. District-Issued Devices

- Devices (laptops, tablets, Chromebooks) issued to students and staff remain the property of the district.
- Users are responsible for the care and proper functioning of their assigned devices.
- Report any damage, malfunction, or loss immediately to the appropriate staff (e.g., teacher, librarian, tech support).
- Do not attempt to repair, open, or modify district-issued devices.
- Keep devices clean and protected from extreme temperatures, liquids, and physical impacts.
- Ensure devices are charged and ready for use daily.
- Students are responsible for any damage incurred to the device they are assigned. Please see the attached fee schedule.

B. Software Licensing and Installation

- Only authorized and licensed software may be installed on district-owned devices.
- Users are strictly prohibited from downloading, installing, or running unauthorized software, shareware, or pirated programs.
- Requests for new software should be submitted to the Technology Department for review and approval.

C. Maintenance and Repair

- All maintenance and repair of district technology equipment must be performed by authorized Technology Department staff.
- Never attempt to perform repairs yourself or enlist unauthorized individuals.

VII. Data Security and Privacy

Protecting the privacy of student and staff data is a top priority.

A. Student Data Privacy (FERPA Compliance)

- The district adheres to the Family Educational Rights and Privacy Act (FERPA), which protects the privacy of student education records.
- Access to student data is limited to authorized personnel with a legitimate educational interest.
- Staff must exercise caution when discussing student information and avoid sharing it publicly or through insecure channels.

B. Staff Data Privacy

- Staff personal data maintained by the district is protected according to relevant privacy laws and district policies.
- Users should be aware that communications and files on district systems are subject to monitoring and disclosure as necessary for legal, security, or operational reasons.

C. Password Management

- Create strong, unique passwords for all district accounts.
- Never share passwords with anyone.
- Do not write down or store passwords in easily accessible locations.
- Change passwords immediately if you suspect they have been compromised.

D. Cloud Storage Use

- Utilize district-approved cloud storage solutions (e.g., Google Drive, Microsoft OneDrive) to save school-related documents and projects.
- Be mindful of the type of information stored in the cloud, especially sensitive or confidential data.
- Do not use personal cloud storage services for district-related, sensitive, or confidential information unless explicitly approved.

E. Reporting Incidents

- Report any suspected data breach, security incident, or unauthorized access to the Technology Department immediately.
- This includes suspicious emails (phishing attempts), unusual network activity, or lost/stolen devices.

VIII. Digital Citizenship and Online Safety

Digital citizenship is the responsible and ethical use of technology. All members of the district community are expected to practice good digital citizenship.

A. Cyberbullying

- Cyberbullying (harassing, intimidating, or targeting others through digital means) is strictly prohibited and will be addressed with serious disciplinary action.
- Do not participate in or condone cyberbullying.
- Report any instances of cyberbullying you experience or witness to a trusted adult immediately.

B. Plagiarism and Copyright

- **Plagiarism:** Never present someone else's work, ideas, or words as your own. Always cite sources appropriately when using information from the internet or other digital resources.
- **Copyright:** Respect intellectual property rights. Do not illegally download, distribute, or use copyrighted material (e.g., music, movies, software) without permission.

C. Online Etiquette (Netiquette)

- Use respectful and appropriate language in all online communications (emails, collaborative documents, discussion forums).
- Be mindful of your digital footprint; anything posted online can be permanent and widely accessible.
- Think before you post or share.

D. Evaluating Online Information

- Develop critical thinking skills to evaluate the credibility, accuracy, and bias of information found online.
- Consider the source, date, and purpose of online content.

E. Reporting Concerns

- If you encounter inappropriate content, suspicious individuals, or feel unsafe online, report it immediately to a teacher, administrator, or parent/guardian.

IX. Support and Troubleshooting

The Technology Department is here to help!

A. How to Get Help

- **Students:** Report technology issues to your teacher or library/media specialist first. They may be able to resolve common issues or will escalate to the Technology Department.
- **Staff:** Submit a help desk ticket through IncidentIQ.
- **Parents/Guardians:** Contact your child's school administration for technology-related inquiries.

B. Common Troubleshooting Tips (for minor issues)

- **Restart:** Often, simply restarting a device or application can resolve minor glitches.
- **Check Connections:** Ensure all cables are securely plugged in (power, network, peripherals).
- **Internet Access:** Verify if other devices can connect to the internet. If not, it might be a network issue.

X. Disciplinary Actions

Violations of this Technology Handbook or the district's Acceptable Use Policy (AUP) will result in disciplinary action consistent with the district's Student Code of Conduct for students, or relevant personnel policies for staff. Actions may include, but are not limited to:

- Verbal or written warning.
- Temporary or permanent loss of technology privileges.
- Detention, in-school suspension, or out-of-school suspension for students.
- Referral to law enforcement for illegal activities.
- For staff, disciplinary actions up to and including termination of employment.

The severity of the disciplinary action will depend on the nature and severity of the violation, as well as any prior offenses.

Contact Information:
Technology Coordinator: Erin Weaver
Email: erin.weaver@gcsd.us
Phone: 601.947.6993;2076

GCSD Technology Device Fee List

Device:	HP 11 G6 EE	HP 11 G8 EE	HP 11 G9 EE	Lenovo 14 E Gen 1, 2, 3	Lenovo 100 E
Screen Replacement	$25	$25	$25	$50	$25
Keyboard Replacement	$35	$40	$40	$50	$40
Charger Replacement	$25	$25	$25	$30	$25
Case/Protecti ve Cover Replacement	$30	$30	$30	$50	$30
Hinge/Frame Replacement	$5	$6	$10	$10	$10
Motherboard Replacement	$40	$50	$130	$200	$45
Plastics (general casing of device()	Top: $ 10 Bottom: $ 10	Top: $ 20 Bottom: $ 20	Top: $ 20 Bottom: $ 20	Top: $ 40 Bottom: $ 20	Top: $20 Bottom: $20
Whole Device Replacement:	$99	$199	$202	Gen 1: $238 Gen 2: $239 Gen 3: $384	$105