

George County School District **APPROVED**

Technology Handbook

2026–2027

JUL 07 2026

G C SCHOOL BOARD

I. Introduction

Welcome to the George County School District (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 a technologically advanced world.
- Facilitate efficient communication and administrative processes.

This handbook outlines policies, procedures, and best practices to ensure that 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 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 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, must not interfere with educational or administrative objectives, and must 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.
- **AI & Emerging Technology:** Use AI tools only when district-approved; never enter student PII into external AI platforms.

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, evaluate, and recommend new and emerging technologies—including AI tools—to support educational goals.
- Provide training and resources for staff in technology use and digital safety.

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.
- Guide students on appropriate and authorized use of AI tools.
- 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.
- Use AI tools only when explicitly authorized by a teacher.
- 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, including appropriate AI and social media habits.
- 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. Enable multi-factor authentication (MFA) where available. 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 their assigned device. Please refer to the Device Fee Schedule on the final page of this handbook.

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 or applications (including AI tools) 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.
- Student personally identifiable information (PII) must never be entered into external AI platforms or unapproved third-party services.

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, including colleagues or students.
- 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, phishing attempt, ransomware, or unauthorized access to the Technology Department immediately.
- This includes suspicious emails, unusual network activity, or lost/stolen devices.
- Do not attempt to investigate or resolve a suspected security incident independently.

VIII. Artificial Intelligence (AI) Tools

AI-powered tools—including generative writing assistants, image generators, chatbots, and AI-based tutoring platforms—are increasingly available and require clear guidance for responsible use within the district.

A. Approved Use

- AI tools may only be used on district devices or networks when reviewed and approved by the Superintendent.

- Teachers may authorize specific AI tools for defined instructional activities. Students must receive explicit permission before using any AI tool for schoolwork.
- Staff may use district-approved AI tools to support lesson planning, administrative tasks, and professional development.

B. Data Privacy & AI

- No student personally identifiable information (PII)—including names, student IDs, addresses, grades, or photos—may be entered into any external or unapproved AI platform.
- Confidential district data must not be used as input for any AI tool not vetted and approved by the Technology Department.
- All AI-generated content used in official communications, reports, or student-facing materials must be reviewed and verified for accuracy before use.

C. Academic Integrity

- Using AI to complete student assignments without teacher authorization constitutes academic dishonesty and is subject to disciplinary action.
- Staff are responsible for establishing clear expectations for AI use within their classrooms and communicating those expectations to students and parents.
- AI-generated content is not always accurate or unbiased. All users are responsible for critically evaluating AI outputs.

D. Requesting New AI Tools

- Requests to use new AI platforms or tools (for instructional or administrative use) must be submitted to the Superintendent for review prior to use.
- The Technology Department will evaluate tools for data privacy compliance, educational value, and alignment with district policy.

IX. 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. Social Media

- Social media use on district devices or networks is restricted to district-approved, curriculum-related activities only.
- Staff must not communicate with students via personal social media accounts.

- Student images, names, or personal information must not be posted to social media without written parental/guardian consent.
- Content posted on personal accounts that targets, threatens, or harasses members of the school community may result in disciplinary action.

C. 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. This includes AI-generated content.
- **Copyright:** Respect intellectual property rights. Do not illegally download, distribute, or use copyrighted material (e.g., music, movies, software) without permission.

D. 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.

E. Evaluating Online Information

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

F. Reporting Concerns

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

X. 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 the appropriate channels at your campus.
- **Parents/Guardians:** Contact your child's school administration for technology-related inquiries.

B. Common Troubleshooting Tips (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 whether other devices can connect to the internet. If not, it may be a network issue—contact the Technology Department.

XI. 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.

XII. Contact Information

Technology Coordinator	Erin Weaver	Technology Staff:
Email	erin.weaver@gcsd.us	Amber Littlefield – amber.littlefield@gcsd.us – ext 2074
Phone	601.947.6993 ext. 2076	DD Long – dd.long@gcsd.us – ext 2076
		Skylar Henderson – skylar.henderson1@gcsd.us – ext 2075
		Conner Green – greenc@gcsd.us – ext 2079
		Jackson Davis – davisja@gcsd.us – ext 2077

GCSD Technology Device Fee Schedule

School Year 2026–2027

Students are responsible for all damage to assigned devices. Fees below reflect repair/replacement costs.

Damage Type	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 / Protective Cover	\$30	\$30	\$30	\$50	\$30
Hinge / Frame Replacement	\$5	\$6	\$10	\$10	\$10
Motherboard Replacement	\$40	\$50	\$130	\$200	\$45
Plastics (top casing)	\$10	\$20	\$20	\$40	\$20
Plastics (bottom casing)	\$10	\$20	\$20	\$20	\$20
Whole Device Replacement	\$99	\$199	\$202	Gen 1: \$238 Gen 2: \$239 Gen 3: \$384	\$105

Note: Fees are subject to change. Multiple damage items are charged cumulatively. Accidental damage is assessed on a case-by-case basis. Intentional damage may result in full replacement cost plus disciplinary action.

Questions about fees? Contact the Technology Department • erin.weaver@gcsd.us • 601.947.6993 ext. 2076

GEORGE COUNTY SCHOOL DISTRICT

Student Acceptable Use Policy (AUP)

School Year 2026–2027 | Grades K–12

This is a legally binding document. Parents/guardians and students must read carefully before signing.

1. Purpose & Scope

George County School District (GCSD) provides students with access to district-owned technology resources — including computers, networks, internet access, and educational software — to support learning and curriculum objectives. These resources are a privilege extended to students in grades K–12 who agree to use them responsibly.

This Acceptable Use Policy governs all student use of district technology, whether on campus or accessed remotely. Use of district technology resources constitutes acceptance of this policy in full.

The GCSD is in compliance with the Children’s Internet Protection Act (CIPA) and all applicable state and federal regulations governing student technology use. Content filtering and monitoring are active on all district networks and devices.

2. Internet Safety & CIPA Compliance

As required by CIPA, the district maintains electronic content filters on all devices and network connections to prevent access to inappropriate material. The district also provides instruction for all students (K–12) on:

- Appropriate online behavior and digital citizenship
- Safe interaction on social networking websites and in online communities
- Recognizing and responding to cyberbullying
- Protecting personal information online

All student internet activity is monitored. There is no expectation of privacy when using district technology resources, including browsing history, email, files stored on school systems, or any other network activity.

3. Acceptable Use of District Technology

3.1 Permitted Activities

Students may use district technology resources for:

- Assigned schoolwork, research, and curriculum-related activities
- Communication with teachers and school staff for educational purposes
- District-approved educational platforms and applications
- College and scholarship applications with teacher or staff guidance

3.2 Prohibited Activities

The following are strictly prohibited on district technology or networks:

- Accessing, transmitting, or downloading pornographic, obscene, threatening, harassing, or otherwise inappropriate content
- Cyberbullying, harassment, or threatening communications directed at any person
- Sharing personal information (name, address, phone number, photos) of yourself or others without authorization
- Using social networking, chat, or gaming sites unless part of an approved classroom activity
- Downloading or installing unauthorized software, games, or applications
- Uploading or transmitting viruses, malware, or any disruptive software
- Attempting to bypass content filters, hack systems, or access unauthorized accounts or areas
- Using another person's login credentials or sharing your own password
- Copying, uploading, or distributing copyrighted material without authorization (including plagiarism)
- Downloading or streaming large media files (music, video) unrelated to schoolwork
- Any commercial, political, or personal business activity
- Any activity harmful to or reflecting negatively on the GCSD community

4. Artificial Intelligence (AI) Tools

AI-powered tools (such as writing assistants, image generators, chatbots, and AI tutoring platforms) are increasingly common. Students must follow these guidelines when using any AI tool at school or for school assignments:

- AI tools may only be used when explicitly permitted by a teacher for a specific assignment or activity.
- Students must never enter personal information — including their name, address, school, photos, or information about classmates — into any external AI platform.
- Work submitted as your own must genuinely reflect your own effort. Using AI to complete assignments without teacher authorization may be considered academic dishonesty.
- AI-generated content is not always accurate. Students are responsible for verifying information before using it in schoolwork.
- Any district-approved AI tools will be communicated by teachers. When in doubt, ask before using.

5. Social Media Guidelines

Social media use on district devices or networks is restricted to district-approved, curriculum-related activities only. Students must additionally:

- Never post or share the personal information, images, or location of classmates, teachers, or other school community members without their explicit consent.
- Never use district accounts or devices to create or maintain personal social media profiles.
- Understand that content posted online — even from personal accounts — that targets, threatens, or harasses students or staff may result in school disciplinary action.
- Report any cyberbullying, inappropriate contact, or threatening messages to a teacher, counselor, or administrator immediately.

6. Personal Device Use (BYOD)

Personal electronic devices (smartphones, tablets, personal laptops, smartwatches, etc.) are subject to district and campus policy on student device use. When permitted on campus or connected to the district network, students must:

- Follow all acceptable use rules in this policy on personal devices, just as they would on district equipment.
- Not connect personal devices to the district network without explicit permission.
- Not use personal devices to bypass content filters or access blocked content while on campus.
- Understand that the district is not responsible for loss, theft, or damage of personal devices on school property.

Campus-level device rules (e.g., phone-free classroom policies) are separate from this AUP and will be communicated by each campus.

7. Cybersecurity & Student Privacy

7.1 Account Security

- Students must keep their login credentials (username and password) private and not share them with other students.
- Students must not access, use, or attempt to access another person's account or files.
- Any suspected account compromise or unauthorized access should be reported to a teacher or the Technology Department immediately.

7.2 Student Data & Privacy

- Student education records are protected under FERPA. District staff will not share student information without appropriate authorization.
- Students should not share personal or sensitive information via district email, chat systems, or any school platform.
- The district archives all email communications on district servers as required by state law.

7.3 Reporting Incidents

- If a student accidentally accesses inappropriate content, they must report it to a teacher or administrator immediately.
- Students who witness or experience cyberbullying, online threats, or suspicious online contact should report it to a trusted adult at school right away.

8. Care of District Equipment

Students are responsible for the proper care and use of any district technology equipment assigned to or used by them.

- Deliberate damage to district computers, peripherals, or network equipment is prohibited. Parents or guardians of students who intentionally damage district equipment (grades K–12) are financially responsible for all repair or replacement costs.
- Students must not move, reconfigure, or tamper with district equipment or its settings.

- USB/flash drives are permitted for data storage only. No executable files may be transferred to district equipment.
- Lost or damaged district equipment must be reported to a teacher or administrator promptly.

9. Consequences for Policy Violations

Violations of this Acceptable Use Policy may result in:

- Suspension or revocation of technology access privileges
- Removal from a computer-based class for the remainder of the semester or year
- School detention, suspension, or expulsion depending on the severity of the violation
- Financial restitution for damage caused
- Referral to local, state, or federal law enforcement for illegal activity

Disciplinary decisions will reflect the nature and severity of the violation. Students and families may appeal disciplinary actions through the standard channels provided in the GCSD disciplinary policy.

Signing this document is legally binding and indicates that the student and parent/guardian have read, understood, and agreed to comply with all terms.

Technology Dept.	Erin Weaver, Technology Coordinator
Contact	Erin.weaver@gcsd.us – 601.947.6993 ext 2076

STUDENT INTERNET USE CONTRACT

Grades K–12 | School Year 2026–2027

This is a legally binding document.

First Name _____

Last Name _____

Grade Level _____

Date _____

Student Contract Agreement

Carefully read the attached George County School District Acceptable Use Policy (AUP). If you have any questions about what is expected of you when using district internet access, school network, or computer equipment, ask a teacher, librarian, or someone in the office to help you understand.

When you understand the rules, sign the contract below to access the school network and available technology.

Student Agreement

I have read the George County School District Acceptable Use Policy (AUP). I understand the rules I must follow when using the internet and technology at school, including rules about:

- Appropriate use of district computers, networks, and internet access
- Artificial intelligence (AI) tools and when they may or may not be used
- Social media and online communication
- Protecting my personal information and the privacy of others
- Cybersecurity, account security, and reporting problems
- Care of district equipment

I understand that if I break the rules, I will be subject to disciplinary action based on the type and seriousness of the violation, as determined by George County School District administration. I also understand that if I break a law, the courts and law enforcement officials will determine the consequences I receive.

Student's Name (Print) _____

Student's Signature _____

Date _____

K–3 students may print their name in place of a signature.

PARENT / GUARDIAN PERMISSION FORM

Internet & Technology Acceptable Use | Grades K–12 | 2026–2027

This is a legally binding document.

Student's Full Name (Print)

Grade Level

Date

Parent / Guardian Agreement

As the parent or guardian of the student named above, I confirm that I have read the George County School District Acceptable Use Policy (AUP) for 2026–2027 and understand the rules and expectations governing my child's use of district technology, internet access, and school networks.

I have discussed appropriate technology use — including internet safety, AI tools, social media, and cybersecurity — with my child.

Parent / Guardian Understanding

I understand that:

- District internet and technology access is provided for educational purposes only.
- The district uses content filtering and monitoring on all devices and networks in compliance with CIPA but cannot guarantee restriction of all inappropriate content.
- I will not hold the district responsible for any material my child may access on the network, and I accept supervisory responsibility for my child's technology use outside of school.
- If my child violates district technology policies, he or she will be subject to disciplinary action based on the type and severity of the violation.
- If my child violates a law, the courts and law enforcement officials will determine the consequences.
- I accept financial responsibility for any damages to district equipment caused by my child.
- All district email and network communications are archived as required by state law and may be produced in response to legal requests.
- There is no expectation of privacy when using district technology resources.

Permission Selection

Please initial ONE of the following:

YES — My child has my permission to use the George County School District's network and internet access for educational purposes, subject to all terms of the AUP.

George County School District

Student Acceptable Use Policy | 2026–2027

NO — My child does NOT have my permission to use the George County School District's network or internet access. I understand this may make enrollment in certain classes impossible.

Parent or Guardian Name (Print)

Parent or Guardian Signature

Relationship to Student

Date

I hereby certify that the information I have provided on this form is correct and that I have read and understood the George County School District Acceptable Use Policy.

Return this completed form to your child's school office before technology access is granted.

GEORGE COUNTY SCHOOL DISTRICT

Staff Acceptable Use Policy (AUP)

School Year 2026–2027

This is a legally binding document. Please read carefully before signing.

First Name _____	Last Name _____
School / Campus _____	Date _____

1. Purpose & Scope

George County School District provides staff members with access to district-owned technology resources, including computers, networks, internet access, email systems, and software applications. These resources are provided to support educational goals, administrative functions, and professional responsibilities.

This Acceptable Use Policy (AUP) governs the use of all district technology resources by all district employees, contractors, and authorized personnel, whether accessed on-campus or remotely. Use of these resources constitutes acceptance of this policy.

2. General Use of District Technology

2.1 Acceptable Use

District technology resources may be used for:

- Instructional preparation, delivery, and student support
- Administrative and professional duties assigned by the district
- Communication with students, parents, colleagues, and district leadership
- Professional development and research directly related to district responsibilities

2.2 Prohibited Use

Staff members may not use district technology resources for:

- Personal commercial activity, advertising, or financial gain
- Accessing, downloading, or distributing obscene, pornographic, or otherwise inappropriate content
- Harassment, bullying, or threatening communications of any kind
- Unauthorized copying, distribution, or installation of software or media
- Attempting to bypass security controls, firewalls, or content filters
- Any activity that violates local, state, or federal law

3. Artificial Intelligence (AI) Tools

The use of AI-powered tools (including but not limited to generative AI writing assistants, image generators, chatbots, and AI-based tutoring platforms) is subject to the following guidelines:

- AI tools may only be used for legitimate instructional or administrative purposes aligned with district goals.
- Staff must not enter personally identifiable information (PII) about students, staff, or families into any external AI platform not approved by the district.
- AI-generated content used in official district communications, reports, or instructional materials must be reviewed and verified for accuracy by the staff member before use.
- Staff are responsible for the accuracy, appropriateness, and compliance of any AI-assisted work they submit or publish.
- The use of AI tools to falsify records, misrepresent work, or circumvent district processes is prohibited.

Questions about approved AI tools should be directed to the Technology Department.

4. Social Media Guidelines

Staff members using social media in a professional or school-related capacity must adhere to the following:

- Do not share student images, names, grades, or any other student information on personal or public social media accounts without written parental/guardian consent.
- District-affiliated social media accounts must be approved and administered in accordance with district communications policy.
- Staff should maintain a clear distinction between personal and professional online presence.
- Do not post content that could be construed as representing the district without authorization.
- Engaging in or facilitating online communication with students via personal social media accounts is prohibited.
- All social media use on district devices or networks is subject to monitoring and logging.

5. Personal Device Use (BYOD)

Staff members who connect personal devices (smartphones, tablets, laptops, etc.) to district networks or use them for district purposes must comply with the following:

- Personal devices connected to the district network are subject to the same acceptable use standards as district-owned equipment.
- Staff assume full responsibility for the security and maintenance of personal devices used for district purposes.
- District data, including student records, must not be stored on personal devices unless encrypted and approved by the Technology Department.
- The district is not responsible for damage, loss, or theft of personal devices on school property.
- Staff must not circumvent district content filtering by using personal devices to access restricted content while on campus.

6. Cybersecurity & Data Privacy

6.1 Password & Account Security

- Staff must use strong, unique passwords for all district accounts and must not share login credentials with anyone.
- Multi-factor authentication (MFA) must be enabled on all district accounts where available.
- Staff must report suspected account compromises to the Technology Department immediately.

6.2 Data Handling

- Student education records are protected under FERPA. Access and disclosure must comply with district policy and applicable law.
- Confidential district data must not be transmitted via personal email accounts or unapproved cloud services.
- Staff must not copy, remove, or transfer district data to unauthorized external storage devices or services.

6.3 Incident Reporting

- Any suspected cybersecurity incident, data breach, phishing attempt, ransomware, or malware must be reported immediately to the Technology Department.
- Do not attempt to investigate or remediate a suspected security incident independently.

7. Remote & Off-Campus Use

Staff accessing district systems remotely (e.g., from home or off-campus locations) are subject to this policy in full and must additionally:

- Use only district-approved secure connections (e.g., district-provided VPN) when accessing sensitive district systems remotely.
- Ensure that district devices and data are not accessible to unauthorized household members or third parties.
- Follow all applicable district security requirements on personal networks.
- Remote access privileges may be revoked at any time at the district's discretion.

8. Internet & Email Use

District internet and email systems are provided for professional use. Staff should have no expectation of privacy when using district technology. The district reserves the right to monitor, inspect, and log all activity on district networks, devices, and accounts.

- Email communications using district accounts should always be professional and appropriate.
- Mass emails to parents or students must follow district communication protocols.
- Phishing emails or suspicious attachments must not be opened and should be reported to the Technology Department.

9. District Equipment & Property

Equipment assigned to or used by staff in classrooms and offices belongs to the George County School District. Its use is governed entirely by district policies and regulations.

- Copying, deleting, or removing district files or software from school premises without authorization is prohibited.
- Staff are responsible for the proper use and care of district equipment assigned to them.
- Lost, stolen, or damaged equipment must be reported to the Technology Department and building administrator promptly.
- Staff must return all district equipment upon separation from employment.

10. Policy Violations & Disciplinary Action

Violations of this Acceptable Use Policy may result in disciplinary action up to and including suspension or termination of employment, in accordance with district policy and applicable employment regulations. The nature and severity of the disciplinary action will be based on the type and seriousness of the violation.

Staff members who violate local, state, or federal law while using district technology resources may be subject to civil or criminal penalties. Law enforcement may be notified.

11. Questions & Contact

If you have questions about this policy or are unsure whether a specific use of district technology is appropriate, contact:

Technology Department	Erin Weaver, Technology Coordinator
Contact	Erin.weaver@gcsd.us - 601.947.6993 ext 2076

Staff Contract Agreement & Signature

I have read and understand the George County School District Acceptable Use Policy (AUP) for the 2026–2027 school year. I agree to comply with all terms and conditions set forth in this policy. I understand that:

- District technology resources are provided for professional and educational purposes and are not personal property.
- I have no expectation of privacy when using district devices, networks, or accounts.
- Violations of this policy may result in disciplinary action, up to and including termination of employment.
- Violations of law may result in civil or criminal penalties independent of district action.

George County School District
Staff Acceptable Use Policy | 2026–2027

Staff Member's Name (Print)

Job Title / Position

School / Campus

Date

Staff Member's Signature

Supervisor / Administrator Signature

By signing above, I acknowledge receipt of this policy and agree to be bound by its terms.

George County School District • Lucedale, Mississippi • 2026–2027