Hoke County Schools

Staff Technology Handbook

2024-2025

Table of Contents

Using this Handbook

This handbook is a guide to proper usage of technology by all employees of Hoke County Schools. Signing the Device Usage Agreement in 1-to-1 Plus indicates that you have read this handbook and agree to all policies and procedures covered within.

Employee Users

No employee will be given access to the district's technology resources before the district has a signed Device Usage Agreement on file. Authorized employees may use the district's technology resources for reasonable, incidental personal purposes as long as the use does not violate any provision of district policies or procedures, hinder the use of the district's technology resources for the benefit of its students, or waste district resources. Any use that jeopardizes the safety, security or usefulness of the district's technology resources or interferes with the effective and professional performance of the employee's job is considered unreasonable. Unless authorized by the district, employees may not access, view, display, store, print or disseminate information using district technology resources that students or other users could not access, view, display, store, print or disseminate.

Getting Connected

Gaining access to your necessary accounts is dependent upon several factors.

Upon hiring, the school principal fills out a request form. Upon receipt of this form, the technology department will create:

- Your **Google Workspace for Education Account**

    - This account gives you access to district email, cloud storage, calendar access, Chromebook login access, and the ability to use Single Sign-On (SSO) services using your HCS Google Credentials.

- Your **Windows Login Account**
    - This account enables you to login to classroom workstations and laptops that run the Windows operating system.

- Your **HCS-WLAN-ADMIN-HOKE** Wi-Fi access credentials.
    - This information allows you to connect up to three (3) personal devices to the HCS wireless network.

The above information will be sent to your *personal email address,* which you supplied to your principal at the time of completing the form.

Once you have received your Google account information, you can sign out a teacher issued Chromebook by contacting dtif@hcs.k12.nc.us or calling 910-904-0026.

Once hired, your school Data Manager will add you to the student information system, **PowerSchool**.

24 hours after being added to PowerSchool, your **Canvas** and **Clever** access will become active.

Note: You will access Canvas, PowerSchool, Clever, and all other critical systems (except Google) through **RapidIdentity** at https://my.ncedcloud.org using your state provided UID number.If you do not know your UID number, contact your principal.

Login Checklist

System	Description	Who to contact...
Classroom Computer	Accessing any district managed Windows device.	stephen.locklear@hcs.k12.nc.us
Staff Chromebook	Accessing your assigned staff device with your Google Account.	dtif@hcs.k12.nc.us
Google	Provides access to district email, Google Drive, Calendar, Google productivity suite, and SSO services	dtif@hcs.k12.nc.us
NCEdCloud	Access to PowerSchool *(attendance)*, SchoolNet, PowerTeacher *(grades),* Canvas, Clever, NCEES, etc.	School Data Manager
Canvas	Learning Management System *(assignments, class rosters, etc...)*	School Data Manager
Clever	Automated rostering and access for various programs.	School Data Manager
Other systems...	Other systems that may be required depending on role.	School Principal, Department Director

Password Security

The District requires the use of strictly controlled passwords for network access and for access to secure sites and information. All passwords to district systems shall meet or exceed the below requirements:

- Passwords shall never be shared with another person.
- Passwords shall be secure according to National Institute of Standards and Technology (NIST) recommended standards.
- When possible, user created passwords should adhere to the same criteria as required for district network access as outlined below.
    - Passwords shall only be saved by district supported password lockers and single sign-on (SSO) systems as approved by the Technology Department.
    - Passwords shall not be programmed into a PC or recorded anywhere that someone may find and use them.
    - When creating a password for secure information or sites, it is important not to use passwords that are easily guessed due to their association with the user (i.e. children's names, pets' names, or birthdays).
- Users and employees who have reason to believe a password is lost or compromised must notify the appropriate party, as outlined in the table above, as soon as possible. The technology department will verify the identity of the person requesting the change before resetting the password.

Email

The district uses Google Workspace for email, document storage and collaboration.Although you can log-in through Google and your email looks very similar to a regular GMail account, your District email is owned and managed by the district and is not a personal GMail account.

Responsibility

Unless otherwise specified by your supervisor, you are expected to read and respond to email in a professional and timely manner. Email is a primary method of communication in and among district buildings and failing to check your email on a regular basis can leave you unaware of critical information.

The user is responsible for all email originating from the user's email account.

1. Forgery or attempted forgery of email messages is illegal and is prohibited.
2. Unauthorized attempts to read, delete, copy or modify e-mail of other users are prohibited.
3. Users are prohibited from sending unsolicited mass email, unless the communication is a necessary, employment-related function or an authorized publication.
4. All users must adhere to the same standards for communicating electronically that are expected in the classroom and that are consistent with district policies and procedures.
5. Users must obtain permission from the superintendent or designee before sending any districtwide email messages.

Basics

- Log in to GMail by visiting https://gmail.google.com and using your provided account information.
- HCS requires Two Factor Authentication (2FA) on all staff HCS Google accounts. Be sure to set it up or you will be locked out of your account after 30 days.
- Always check the sender of an email message. Do not open messages from an unrecognized sender.
- Never send passwords or reply to messages asking for your password. The district will never ask for your password through email.
- Do not include a student or staff name in the subject of your email. Anyone who can view your screen can easily see this information.
- District email is to be used only for district business.

Phishing

Phishing is a type of malicious email trying to trick you into giving the sender private or useful information. Phishing emails typically mirror other well known generic emails to deceive the user into believing the email is legitimate and relinquish information.

There are several ways to protect yourself from phishing emails:

- Always check the sender's address.
- If the email does not look quite right or is unfamiliar use Google email tools to label email as phishing or spam. This will let Google

know that any email from the sender's address is malicious and to directly deposit it to a spam/junk email folder.

- Phishing emails are only dangerous if you click any links in the email or if you respond to the email.
- Responding to the email may help the attacker to achieve what is called double phishing or phishing a company for a response in order to get an email from said company. The attacker then can make a new phishing email replicated from your email to attack your company again or another company.

Emailing Parents

Parents can be emailed through district email. You must never include multiple parent email addresses in the TO: or CC: lines which will reveal email addresses to other parents.

- Email an individual parent directly from your district email.
- Email multiple parents by only using the BCC (blind carbon copy) line. No recipients will see the addresses of any other recipient.

Legal

All emails are documented permanently in the Google Workspace Vault. No expectation of privacy is guaranteed while using district email. All messages to and from district accounts are subject to search without prior notice.

Social Media

The district encourages staff to use district-approved electronic media to communicate with parents and students; however, the line between public/private and personal/professional is blurred in the digital world. Unprofessional and/or inappropriate use of electronic media reflects poorly on the district as well as the individual and can be cause for disciplinary action.

Read and be familiar with the board policy regarding social media usage (Hoke County Board of Education Policy 7335).

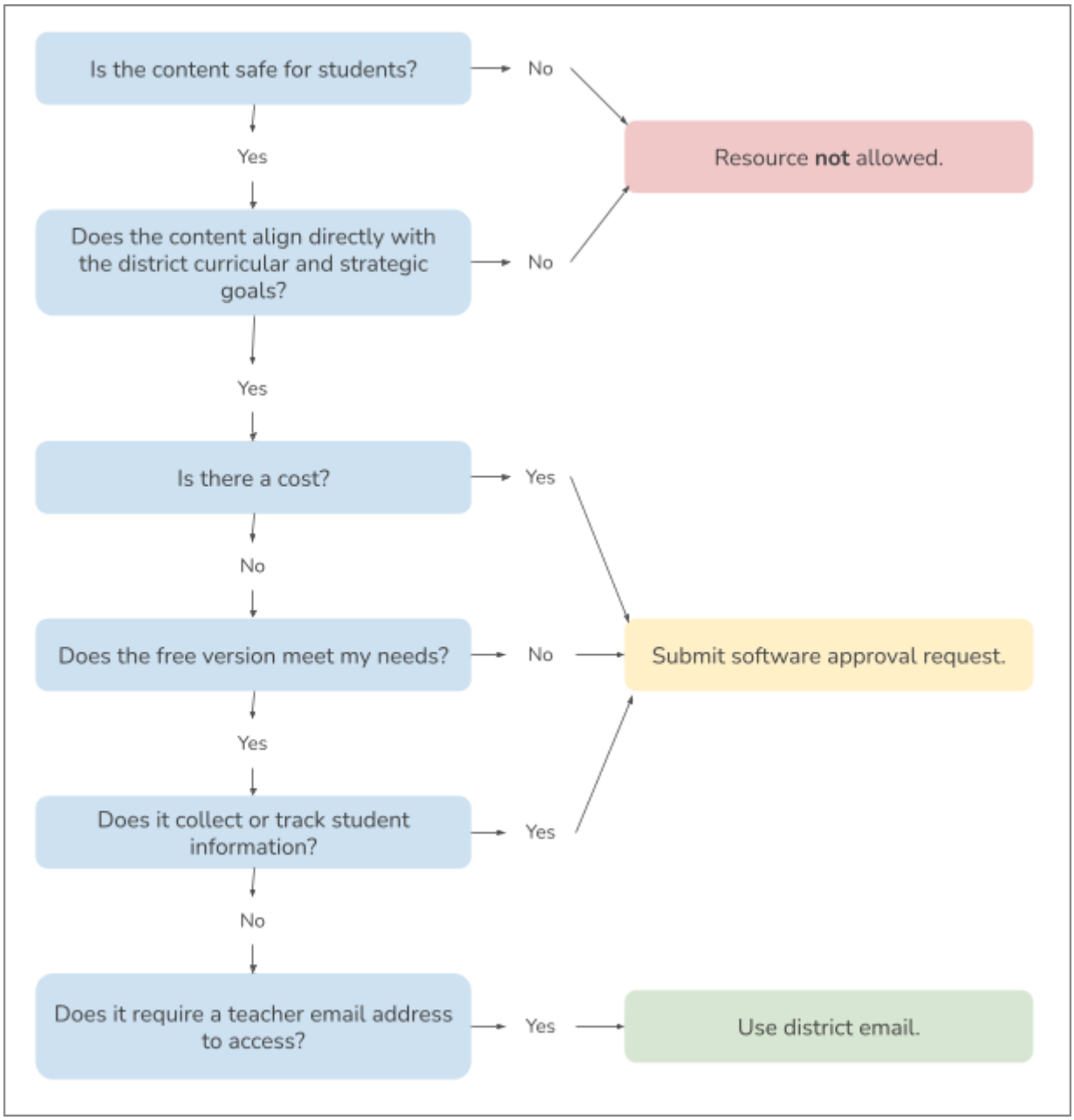
Digital Resources

The district provides many digital resources for use in the classroom. The Technology department website and the Digital Teaching and Learning website have lists of approved software resources for you to use.

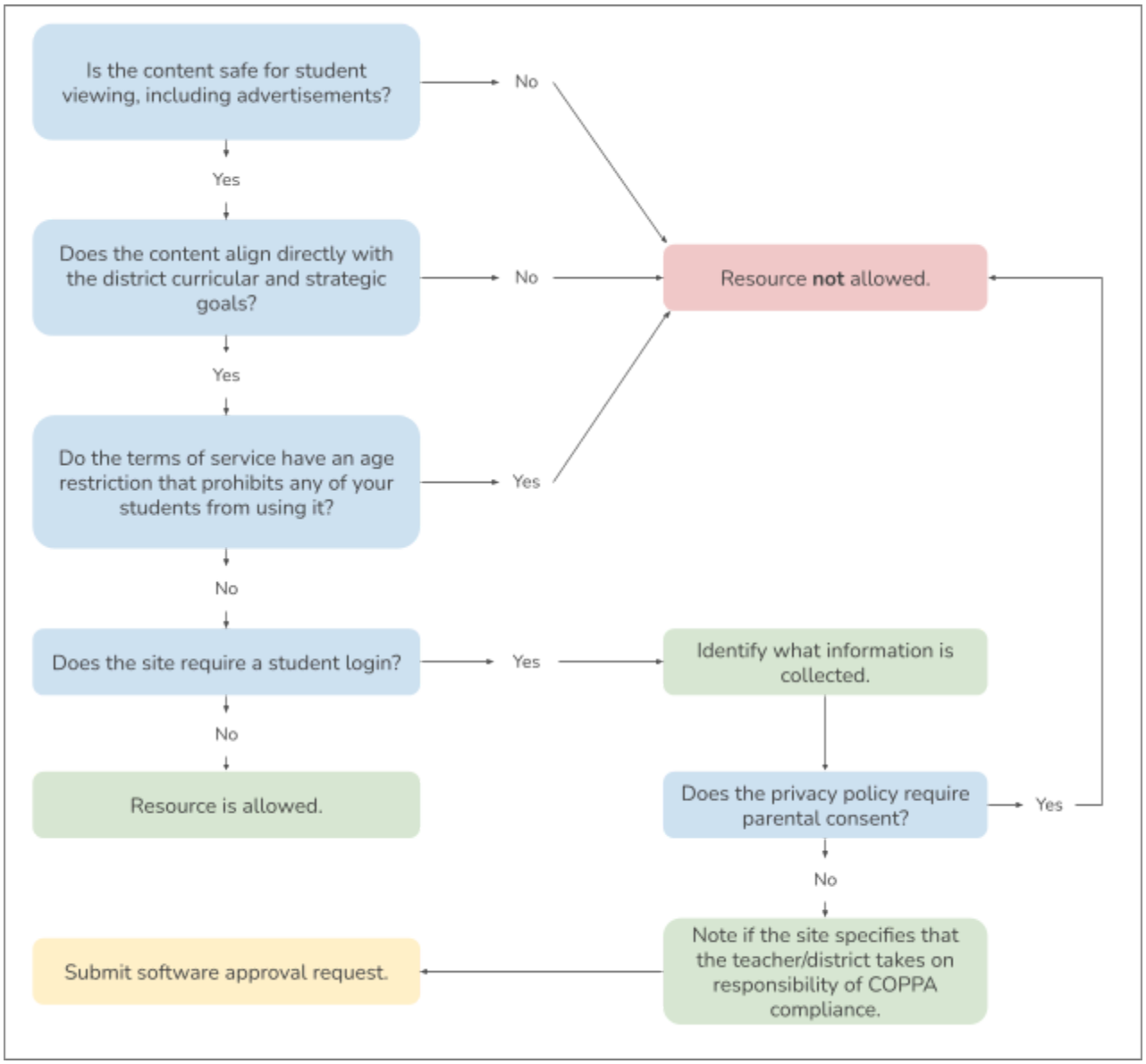
New resources are approved through a software approval form, completed by your school principal or department head. Before being approved, each resource is scrutinized under the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), the Children's Internet Protection Act (CIPA), and the North Carolina DPI 3rd Party Data Integration Standards.

Before requesting new software, use the flowcharts below to guide you through the process of evaluating the appropriateness of the software.

Software for Teacher Use (no students)



For Student Use



Learning Management Systems

A learning management system (LMS) is a software application for the administration, documentation, tracking, reporting, and delivery of electronic educational technology.

For grades Pre-K through 1, **SeeSaw** is the supported LMS. In grades 2 through 13, the official LMS is **Canvas**. Canvas can be accessed through your RapidIdentity dashboard.

Generative AI Guidance and Best Practices

Generative Artificial Intelligence (GenAI) is poised to transform the realms of business, technology, and education. As educators committed to preparing students for the realities of the modern world, Hoke County Schools recognizes the immense potential that GenAI tools hold to transform teaching and learning. However, with transformational technological advancements comes the need to address the appropriate use of GenAI in educational settings. It is crucial to address the changes that GenAI brings with clear guidance to ensure an ethical and effective educational experience for all.

In combination with the North Carolina Generative AI Implementation Recommendations and Considerations (available at go.ncdpi.gov/AI_Guidelines), these guidelines are designed to help district leaders navigate the complex landscape of Generative AI in educational settings. GenAI offers unparalleled resources for research, composition, and presentation, but it also raises questions about originality and authenticity. This guidance serves as a framework for understanding what constitutes appropriate and inappropriate use of GenAI in schools. It is crafted to empower faculty, staff, and students to use these tools responsibly and creatively, ensuring that the focus remains on learning, skill development, and innovation.

This document contains guidelines and examples of appropriate and inappropriate use of GenAI in the following domains:

- **Transparent Use** - The clear and open disclosure of the use of generative AI tools in the creation of work using formal attribution practices. This ensures that all parties are aware of the technological aid involved in the creation of student submissions.

- **Verification of Content Accuracy** - The process of rigorously reviewing and fact-checking any outputs generated by GenAI to ensure its accuracy and reliability. This step is crucial to mitigate the risks of AI “hallucinations” (false information generated by the AI) or embedded biases that may skew the information or data presented.
- **Originality** - The use of GenAI as a tool to augment and enhance the student’s own creative ideas and work, rather than replacing that cognitive work. It involves awareness and avoidance of plagiarism, ensuring that the final work is a unique and authentic representation of the student’s own effort and creativity.

As AI technology and its use in educational settings continue to evolve, this guidance will be continuously updated to reflect these advances. Hoke County Schools is committed to providing opportunities for students to explore and grow in this rapidly changing technological landscape. We are excited to see how our students and faculty will leverage GenAI to push the boundaries of what's possible in teaching and learning.

Guidance for the Use of Generative AI in Educational Settings

Transparent Use

Students should disclose the use of GenAI in their formal coursework with proper attribution. This includes actions such as:

- Paraphrasing or quoting GenAI-generated text
- The incorporation of GenAI-generated images or other media
- Indirect support such as brainstorming, research, and proofreading/editing

To further ensure transparency and accountability, students should be prepared to produce GenAI chat histories if requested.

Teachers should clearly state their expectations for GenAI use in all graded coursework on an assignment-by-assignment basis. Depending on the circumstances, this may include:

- No GenAI use
- Indirect GenAI support (e.g., generative search, proofreading, etc.)
- GenAI augmentation (e.g., help with drafting, image production, etc.)
- Unrestricted GenAI use

Students must adhere to all GenAI documentation and citation protocols as outlined by the teacher for each assignment, and be prepared to produce search histories, chat histories, and prompts upon request.

How to Attribute GenAI Usage

Specify the extent and nature of the AI's assistance, as well as the name of the tool and the date it was used in accordance with the appropriate style guide as assigned by the teacher. This will generally involve the use of:

- In-text citations
- Footnotes or endnotes
- Works-cited list or bibliography

Verification of Content Accuracy

Students and teachers must always check the accuracy of information obtained from GenAI chatbots and search tools. Ensure the information is current and relevant to the

topic at hand, using traditional search engines, research, and/or databases to find similar information from recognized authorities.

In addition, students and teachers must critically evaluate all GenAI-generated content for bias and hallucinations before submitting or assigning GenAI-assisted work.

- Bias occurs when the GenAI's outputs reflect prejudiced views or unequal representation, often stemming from the data on which the model was trained.
- Hallucinations are instances in which the GenAI presents fabricated, inaccurate, or misleading information as if it were true. When the GenAI encounters gaps in its knowledge, it will make up answers. For example, GenAI chatbots have knowledge cutoffs that can impact the accuracy of outputs (e.g., ChatGPT 4 currently has a knowledge cutoff of December 2023).

Originality

Teachers and students should use AI to enhance, not replace, their own creativity, beginning with their own ideas and concepts before turning to AI for support. Maintain awareness of plagiarism and academic integrity when using GenAI-generated content. Use writing tools such as Grammarly to check for accidental plagiarism, but do not rely on these tools to “fix” plagiarized content.

Teachers and students should always distinguish their own creative contributions from the GenAI-generated content, and credit the GenAI tool where necessary to uphold academic integrity.

Examples of Appropriate and Inappropriate Use

"Generative AI" refers to a broad range of advanced technological tools that can create or modify digital content. The scenarios below provide examples of appropriate and inappropriate use for:

- *Conversational AI*—Systems like ChatGPT and other chatbots that simulate human-like interactions, allowing users to engage in text or voice-based conversations with artificial intelligence.
- *Generative Search*—A type of GenAI tool that produces dynamic search results based on user queries.
- *Multimodal AI*—Systems like DALL-E that can process, understand, and produce various types of media, including images, video, and audio simultaneously.
- *AI Writing Support Tools*—Platforms like Grammarly and Quill that use natural language processing to analyze and enhance written content.

<table>
<tr><td colspan="2">Conversational AI: ChatGPT, Claude, Gemini, etc.</td></tr>
<tr><td colspan="2">Scenario: Students are tasked with creating a research project on a historical figure of their choice.</td></tr>
<tr><td>Appropriate Use:
With teacher permission, a student uses ChatGPT to organize their initial ideas about Henry VIII into an outline. When struggling with how to word a particular concept, they turn to ChatGPT for ideas, eventually combining some of its suggestions with their own words. The student uses an in-text citation to document the AI use in MLA format.</td><td>Inappropriate Use:
A student uses ChatGPT to generate their entire research project and turns it in without significant modifications or personal contributions. They do not disclose the use of AI in any way, presenting the work as entirely their own.</td></tr>
</table>

Generative Search: Perplexity, Andi Search, Metaphor, etc.

Scenario: Business students are developing a comprehensive market analysis for a hypothetical new product launch.

Appropriate Use:	**Inappropriate Use:**
A group of students use Perplexity to gather initial data on market trends, consumer preferences, and competitive landscapes. They use this data as a foundation to further conduct traditional research. The students verify the information obtained from Perplexity with credible sources. In their report, they clearly cite the generative search tool as one of the multiple sources used for preliminary data gathering.	A group of students use Perplexity to gather all their market data, consumer insights, and competitive analysis. They do not cross-check Perplexity's information with credible sources. In their market analysis report, the team presents the AI-generated data as if it were gathered through traditional research methods.

Multimodal AI: DALL-E, Midjourney, Synthesia, etc.

Scenario: Students are asked to create a presentation on the theme of a recent novel study.

Appropriate Use:	**Inappropriate Use:**
A student uses DALL-E to produce initial ideas for a mood board representing the main thematic elements of the novel. They input basic concepts and desired elements, and the AI generates several options. The student modifies this content to suit their intended purposes and reflect their creativity. The final presentation is a blend of AI-generated images and the student's creative modifications. They attribute DALL-E in their project, stating which elements were AI-assisted and emphasizing their own significant contributions to the final design.	A student inputs summaries of the novel's theme found online into DALL-E and use them to generate the entire collection of images used in the presentation, without any significant modification or personal contribution. In their project submission, the student presents these materials as entirely their own work. They fail to disclose the extent to which the DALL-E was used, giving the impression that the creative design was solely their effort.

AI Writing Assistance: Grammarly, Quill, HyperWrite, etc.	
Scenario: Students are participating in a project-based learning experience that involves writing emails to local business owners.	
Appropriate Use: After brainstorming and drafting the original email message, a student uses Grammarly to refine the language, check for tone consistency, and ensure the content is error-free. The student critically assesses the AI's suggestions, selectively incorporating edits that enhance their message. They ensure the final content reflects their unique creative strategy, not just Grammarly's language capabilities.	**Inappropriate Use:** After creating a rudimentary draft of their own email, a student relies on Grammarly to rewrite the entire message. When submitting their documentation for assessment, the student presents this as their own original communication.

District Devices

The district issues devices to staff based on job role and instructional need. No devices will be issued before the district has the appropriate signed user agreements on file. Use of district devices must comply with all other technology policies. Device inventory and issuance is tracked by the technology department.

Care of Devices

The district expects those who receive devices to take reasonable precautions to prevent damage. Employees may be required to reimburse the district for any damage or theft that was the result of the employee's negligence.

Always use the provided case for assigned devices.

Any accidental damage must be reported immediately. Damage not reported immediately will be considered improper care of equipment and may be deemed negligence.

District devices may not be personalized in any way that is not immediately removable or has the potential to leave behind glue or other material.

- No stickers, paint, white out, ink, tape, glue, glitter, rhinestones, etc.
- Personal cases, covers, or bags are ok and may be personalized if not provided by the district.

Reporting Damage, Viruses, and Other Trouble

Damage

Staff with a damaged Chromebook device should enter a work ticket by logging in to 1-to-1 Plus with their HCS Google account.

Stolen Devices

If a device is stolen and a police report is filed, the user will be fined $100.00 for replacement, as long as the police report is provided. If no police report is provided, the user will be fined the entire replacement cost of the device.

Viruses

If you suspect your device has been infected by a virus or other malicious software, immediately contact the technology help office at 910-904-0026.

Student Devices

Students in Hoke County Schools are assigned either iPads (Pre-K—1st Grade) or Chromebooks (2nd—12th Grade) and an appropriate charger. While it is the student's responsibility to maintain and track the devices assigned to them, staff members can aid in this process by maintaining good practices in the classroom.

As a rule, staff members should never instruct students to share, lend, or borrow another student's chargers. This practice often results in chargers changing hands or getting lost. The ultimate result of this practice is students who are fined for their missing chargers.

Students are instructed to charge their devices at home and not bring their chargers to school. In the event that you have students who arrive with dead batteries, consider the following as alternatives to mandating charger sharing:

- Consider allowing the student to participate using a paper version of the assignment or other non-digital alternatives.
- Encourage peer collaboration on shared devices, where appropriate, without sharing chargers.
- Allow students to take their device to the media center and plug it in to charge while the student returns to class.
- Engage the student in alternative activities that reinforce the lesson without the use of a device.

End of Year Process

Computer

At the end of the school year, a technology representative or your school Media Coordinator will do a physical inspection of your technology hardware. A sign out sheet will be signed by both parties before you can leave and will record any damage/issues with the machine.

Staff members who do not return assigned devices at the conclusion of the school year will have the replacement costs for the device drafted from their final paycheck.

Other Technology

All other technology used by or checked out to you will need to be inspected or turned in before leaving. This technology is includes but is not limited to:

- Document camera
- Webcams
- headsets

Use of Personal Devices

By allowing teachers to use personal technology devices, such as laptops, handhelds, and mobile phones in the classroom, we ultimately expand the availability of devices in the classroom for instructional purposes.

All use of personal devices must adhere to Board policy outlining the use of technology, social media, Internet, and communicative resources. Use of a personal device is for instructional purposes and must align with district curriculum. Use of personal devices by teachers will be at their own risk. Hoke County Schools will not be

responsible for theft, loss, or damages to any personal device used. In addition, technology staff members will not provide any technical or repair services to any personal devices. Troubleshooting and repair of personal devices are the responsibility of their respective owner.

Wireless Access

Hoke County Schools has installed wireless access in all schools. HCS provides access to wireless Internet connection for staff members through personalized access passwords. Each staff member's unique password can be used on a maximum of three (3) personal devices (i.e., phone, tablet, laptop, watch, etc).

Additionally, the HCS Guest wireless network is available in common areas of district facilities. The guest wireless code will be provided internally to all staff members through school administration.

Get Technical Help

Putting in a work ticket is your first option to notify technology for help .The workorder system can be found under Staff Resources on the HCS district website.

Cell Phone Use

District provided cell phones are subject to all policies concerning district devices. Employees do not have any expectation of privacy in district-provided cell phones or any information stored on them, and such phones may be confiscated and searched at any time.

If an employee chooses to decline the district-provided phone deemed required for the position, the employee must agree to provide their personal phone information to necessary staff and to carry data coverage on their phone if deemed necessary by their position.

In order to ensure security and privacy of student and staff data, upon termination of employment, the district may send a command to any connected personal devices that will reset the device to factory defaults. This command will erase all information stored on the device, including any personal information.

Securing Data at Rest & Transit

Google Drive

The district uses Google Drive for work-related file storage.

Google provides space for employees to utilize for storing files. Please note that files uploaded into a shared folder are accessible by all users who have access to that folder by default. It is the employee's responsibility to report any Google Drive or cloud storage security problems immediately.

Google Drive is also ideal for collaboration. Google makes it very easy to share and work on files simultaneously.

External Storage

The term "External Storage Devices" is used to define all portable storage devices (including usb drives, rewritable cds, and external hard drives) used by staff and students. While the district recognizes the advantages for staff and students to

maintain information on these devices, users are strongly encouraged to rely on their district provided Google Workspace for Education Drive account for all storage needs.

You are responsible for all content on external storage devices that have been connected to district technology resources. This includes ensuring the device is free of harmful software and that files containing student information are encrypted or password protected. Never transfer documents labeled classified, confidential, or restricted to any external storage device. You must delete any district created/provided content when leaving the district.

Transferring Files

Policies and guidelines related to file storage apply to files in transit as well. It is your responsibility to secure sensitive data for transmission with encryption or a password. Classified, confidential, or restricted information should not be transferred through email, Google Drive, external storage devices, or third party file transfer services. See the Email and Safety sections for guidelines on safe email usage.

The technology department can set up secure file transmission when needed. Examples include approved software or websites that regularly need to receive and send student data. See the Digital Resources section for instructions to review and request use of software or a website.

Exceptions

Exceptions to district rules will be made for district employees or agents conducting an investigation of a use that potentially violates the law, district policies or procedures. Exceptions will also be made for technology administrators who need access to district

technology resources to maintain the district's resources or examine and delete data stored on district computers as allowed by the district's retention policy.