

**Future Focused.
Student Centered.**



HOKE COUNTY SCHOOLS

STAFF TECHNOLOGY
HANDBOOK

2026/27

Future Focused. Student Centered.



Revision Date	Revisions
August 2026	Tone and voice changes. Updated MFA information added. Device take-home opt-in information added. Number of devices allowed on the network updated.

Table of Contents

Using this Handbook.....	5
Employee Users.....	5
Getting Connected.....	5
Login Checklist.....	7
Password Security.....	8
Email.....	9
Responsibility.....	9
Basics.....	10
Phishing.....	10
Emailing Parents.....	12
Legal.....	12
Social Media.....	13
Digital Resources.....	13
Learning Management Systems.....	15
Generative AI in Hoke County Schools.....	16
Purpose.....	16
Expectations for Staff.....	16
District Devices.....	19
Care of Devices.....	20
Reporting Damage, Theft, Viruses, and Other Problems.....	20
Student Devices.....	21
End-of-Year Process.....	22
Use of Personal Devices.....	23
Wireless Access.....	23
Get Technical Help.....	24
Cell Phone Use.....	24
Securing Data at Rest & Transit.....	24
Google Drive.....	24
Personal Cloud Storage.....	25
External Storage.....	25
Transferring Files.....	26
Exceptions.....	26

Using this Handbook

This handbook provides guidance for the appropriate use of technology resources by all Hoke County Schools employees. By signing the Device Usage Agreement, employees acknowledge that they have read this handbook and agree to follow the policies and procedures outlined within.

Employee Users

No employee will be granted access to district technology resources until a signed Device Usage Agreement is on file.

Authorized employees may use district technology resources for reasonable, incidental personal purposes, provided that such use does not violate district policies or procedures, interfere with the use of district resources for students, or result in unnecessary use of district resources.

Any use that compromises the safety, security, or functionality of district technology resources, or that interferes with the effective and professional performance of an employee's duties, is considered inappropriate.

Unless specifically authorized by the district, employees may not use district technology resources to access, view, display, store, print, or distribute information that students or other users would not otherwise be permitted to access, view, display, store, print, or distribute.

Getting Connected

Access to district accounts and technology resources depends on several steps in the employee onboarding process.

Upon hiring, the school principal or department director submits an account request form. Once the form is received, the Technology Department will create:

- Your **Google Workspace for Education account**
 - This account provides access to district email, cloud storage, Google Calendar, Chromebook login, and Single Sign-On (SSO) services that use your HCS Google credentials.
- Your **Windows login account**
 - This account allows you to log in to district-managed classroom workstations and laptops running the Windows operating system.
- Your **HCS-WLAN-ADMIN-HOKE Wi-Fi credentials**
 - These credentials allow you to connect up to five (5) personal devices to the HCS wireless network.

Your account information will be sent to the *personal email address* provided to your principal or director during the account request process.

Once you receive your Google account information, you may check out a district-issued staff Chromebook by contacting your School Library Media Coordinator.

District personnel will also add you to the student information system, **Infinite Campus**. Approximately 24 hours after being added to Infinite Campus, your **Canvas** and **Clever** access will become active.

Note: Canvas, Infinite Campus, Clever, and other critical state and district systems are accessed through **RapidIdentity** at <https://my.ncedcloud.org> using your state-provided UID number. If you do not know your UID number, contact your principal.

As of July 1, 2026, all staff are required to set up and use **Multi-Factor Authentication (MFA)** to access RapidIdentity. You may use the authenticator

app of your choice; Hoke County Schools recommends Google Authenticator. For assistance with setting up MFA, contact your school data manager.

Login Checklist

System	Description	Who to contact...
Classroom Computer	Accessing any district managed Windows device.	HCS Technology (work-ticket)
Staff Chromebook	Accessing your assigned staff device with your Google Account.	School Media Coordinator
Google	Provides access to district email, Google Drive, Calendar, Google productivity suite, and SSO services	HCS Technology (work-ticket)
NCEdCloud	Access to Infinite Campus (<i>attendance and grades</i>), SchoolNet, Canvas, Clever, NCEES, etc.	School Data Manager
Canvas	Learning Management System (<i>assignments, class rosters, etc...</i>)	School Data Manager

System	Description	Who to contact...
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 secure passwords for network access and for access to protected systems and information. All passwords used with district systems must meet or exceed the following requirements:

- Passwords must never be shared with another person.
- Passwords should follow current National Institute of Standards and Technology (NIST) recommendations for password security.
- When creating passwords for other work-related systems, employees should follow the same security practices required for district network access whenever possible.
 - Passwords may only be stored using district-supported password managers or approved Single Sign-On (SSO) systems.
 - Passwords should not be saved on a computer or recorded in any location where they could be easily found or used by another person.
 - Passwords should not contain information that is easily associated with the user, such as children's names, pets' names, birthdays, or other commonly known personal information.

- Employees who believe a password has been lost, exposed, or compromised must notify the appropriate support contact as soon as possible. Before resetting a password, the Technology Department will verify the identity of the person requesting the change.

Email

The district uses **Google Workspace for Education** for email, document storage, and collaboration. Although district email is accessed through Google and may look similar to a personal Gmail account, your HCS email account is owned and managed by the district and should not be treated as a personal account.

Responsibility

Unless otherwise directed by your supervisor, employees are expected to read and respond to email in a professional and timely manner. Email is a primary method of communication throughout the district, and employees are responsible for checking their district email regularly to remain informed of important information.

Employees are responsible for all messages sent from their district email accounts.

1. Forgery or attempted forgery of email messages is prohibited.
2. Unauthorized attempts to read, delete, copy, or modify another user's email are prohibited.
3. Employees may not send unsolicited mass email unless the communication serves a necessary employment-related purpose or is otherwise authorized by the district.

4. Electronic communication must meet the same standards of professionalism expected in other work-related settings and must comply with district policies and procedures.
5. Employees must obtain permission from the superintendent or designee before sending districtwide email messages.

Basics

- Log in to **Gmail** at <https://gmail.google.com> using your district-provided account credentials.
- HCS requires **Two-Factor Authentication (2FA)** on all staff Google accounts. Employees must complete 2FA setup within 30 days of account creation to avoid losing access.
- Always verify the sender of an email message before opening links, attachments, or responding. Use caution with messages from unfamiliar or unexpected senders.
- Never send your password by email or respond to a message asking you to provide it. Hoke County Schools will never ask for your password through email.
- Do not include student or staff names in the subject line of an email. Subject lines may be visible on screens, notifications, or other devices.
- District email should be used for district-related business.

Phishing

Phishing is a type of malicious communication designed to trick users into revealing sensitive information, providing account access, or taking an action that benefits an attacker. Phishing messages often imitate legitimate

organizations, services, or individuals to make the communication appear trustworthy.

There are several ways to protect yourself from phishing attempts:

- Always verify the sender's email address, particularly when a message is unexpected or asks you to take immediate action.
- Be cautious of unexpected links, attachments, QR codes, requests for credentials, or messages that create an unusual sense of urgency.
- Never open an unexpected attachment or scan a QR code from a message unless you are confident the sender and request are legitimate.
- If an email appears suspicious, use Gmail's reporting tools to mark the message as phishing or spam. This helps Google identify similar malicious messages and improve filtering.
- Never provide passwords, authentication codes, or other sensitive information in response to an unsolicited email.
- Avoid replying to suspicious messages. A response may confirm that your email address is active and can provide an attacker with additional information that may be used in future phishing attempts.

If You Believe Your Account Has Been Compromised

If you clicked a suspicious link, opened a questionable attachment, scanned a suspicious QR code, entered credentials on an unfamiliar website, approved an unexpected authentication request, or otherwise believe your account may have been compromised, **notify the HCS Technology Department immediately.**

Do not wait to see whether unusual activity occurs. Prompt reporting allows the Technology Department to limit potential damage and begin remediation.

When an account is believed to be compromised:

- The account may be temporarily suspended to prevent further unauthorized access while Technology Department staff investigate and remediate the issue.
- Technology staff will work with the employee to restore secure access once remediation is complete.
- The employee will be required to complete assigned cybersecurity awareness training through **KnowBe4** before or as part of the account restoration process.

Emailing Parents

Parents and guardians may be contacted using district email. When emailing multiple recipients, employees must protect the privacy of individual email addresses.

- Email an individual parent or guardian directly from your district email account.
- When sending the same message to multiple parents or guardians, place all recipient addresses in the **BCC (blind carbon copy)** field. Do not place multiple parent or guardian email addresses in the **TO** or **CC** fields, as doing so will reveal those addresses to other recipients.

Legal

District email is archived in **Google Vault** in accordance with district retention practices. Employees should have no expectation of privacy when using district email. Messages sent to or from district accounts may be reviewed or searched by authorized district personnel without prior notice, as permitted by district policy and applicable law.

Social Media

Reference Policy Code: [7335 Employee Use of Social Media](#)

The district encourages employees to use district-approved electronic media to communicate with parents, guardians, and students. Because the boundaries between personal and professional communication can be less distinct in digital environments, employees are expected to maintain professional standards when using social media and other electronic communication platforms.

Inappropriate or unprofessional use of electronic media may reflect negatively on both the employee and the district and may result in disciplinary action.

Employees are expected to read and comply with **Hoke County Board of Education Policy 7335, Employee Use of Social Media**.

Digital Resources

The district provides a variety of digital resources for instructional use. The **Technology Department** and **Digital Teaching and Learning** websites maintain lists of approved software and digital resources available to staff.

New resources must be reviewed through the district's software approval process. Requests are submitted by a school principal or department director using the appropriate software approval form. Before a resource is approved, it is evaluated in the following areas:

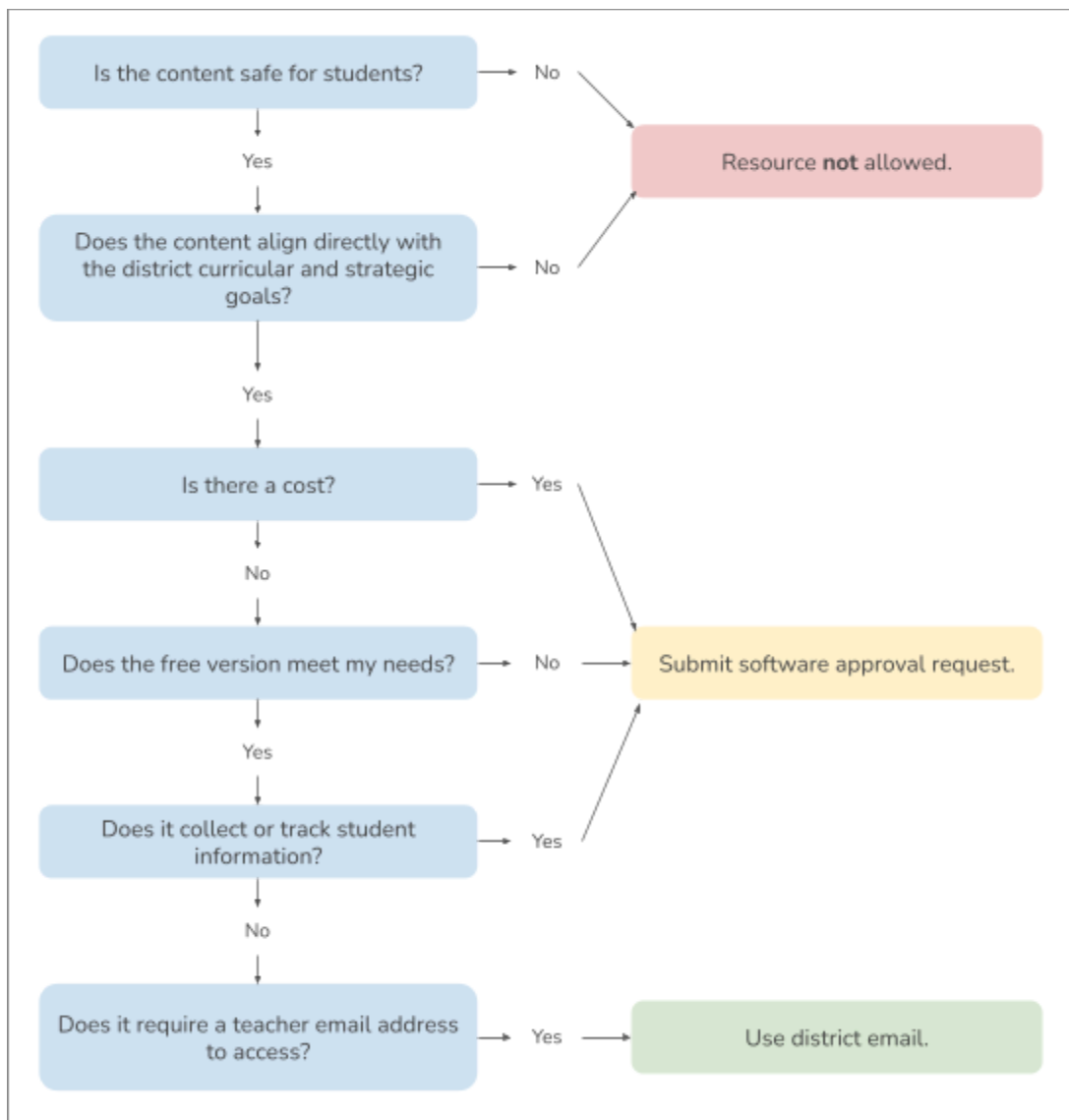
1. **Student data privacy and legal compliance**, including requirements related to the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), the Children's Internet

Protection Act (CIPA), and the North Carolina DPI Third-Party Data Integration Standards.

2. **Alignment with district curricular and instructional goals.**
3. **Compatibility with district technology infrastructure and systems.**

Before requesting approval for new software or a digital resource, use the flowcharts below to help determine whether the resource is appropriate for district use.

Software for Teacher Use (no student access)



Note: Any software designed for student use requires the submission of an approval request.

Learning Management Systems

A **Learning Management System (LMS)** is a digital platform used to organize, deliver, track, and support teaching and learning.

Hoke County Schools uses the following learning management systems by grade level:

- **Grades K–8:** Campus Learning, the LMS built into Infinite Campus
- **Grades 9–12:** Canvas

Generative AI in Hoke County Schools

Purpose

Generative Artificial Intelligence (GenAI) is reshaping education by offering new ways to enhance instruction, support creativity, and prepare students for a future in which AI will play an increasingly significant role. Hoke County Schools (HCS) is committed to supporting the ethical, responsible, and effective use of GenAI in teaching and learning.

This section provides an abbreviated overview of the full **Hoke County Schools Generative AI Guidelines**. For complete guidance, staff should refer to the full document available through the Department of Digital Teaching and Learning.

The expectations below are intended to support responsible GenAI use, maintain academic integrity, protect student data, and foster future-ready skills.

Expectations for Staff

Model Responsible Use

- Use GenAI as a teaching and planning support, not as a substitute for professional judgment.
- Disclose the use of GenAI when it is used to create or substantially support instructional materials.
- Maintain a human-centered approach to lesson planning, grading, feedback, and other professional responsibilities.

Integrate AI Thoughtfully

Staff may use GenAI to:

- Brainstorm lesson ideas.
- Support differentiation.
- Generate suggestions for feedback.
- Create or adapt non-assessment-related instructional materials.

Staff should not use GenAI to:

- Generate final grades or evaluative comments without professional review.
- Produce final student or family communications without personal review and oversight.
- Replace professional judgment or responsibility for instructional content.

Teach Students About Ethical Use

Explicitly teach students to use GenAI responsibly, including:

- **Transparency:** Disclose GenAI use and provide appropriate attribution when required.
- **Verification:** Critically evaluate GenAI-generated content for accuracy, reliability, and bias.
- **Originality:** Use AI to support and extend original thinking rather than replace it.

Use the **Student Integration Scale** to communicate the level of AI use permitted for assignments:

- **Level 0: AI-Free** — AI use is not permitted.
- **Level 1: AI-Assisted** — AI may be used during limited support stages, such as brainstorming.
- **Level 2: AI-Enhanced** — AI-generated content may be incorporated into the final product when it is reviewed, revised, and appropriately integrated by the student.
- **Level ∞: AI-Empowered** — AI may be used as a significant part of a complex or creative process with strong student ownership and human oversight.

Clearly communicate the permitted level of AI use for each assignment.

Expectations should be established in course materials, syllabi, or individual assignment directions as appropriate.

Monitor and Support Ethical Practice

- Regularly review student work for originality and appropriate use of GenAI.
- When appropriate, address suspected AI misuse as an opportunity to clarify expectations and reinforce responsible use. Academic integrity concerns should be handled in accordance with applicable school and district policies.

- Require students to retain or submit AI chat histories, prompt logs, or other documentation when appropriate to the assignment.

Data Privacy Responsibilities

Staff must not enter **Personally Identifiable Information (PII)**, confidential information, or protected district data into public or unapproved GenAI tools.

Examples include:

- Student names or identification numbers.
- Contact information.
- Demographic information.
- Grades, academic records, or other educational records.
- Confidential employee or district information.

GenAI tools may only be used with protected information when the specific platform, account, and use have been approved by Hoke County Schools for that purpose.

Improper disclosure of protected information may violate FERPA, COPPA, district policy, or other applicable privacy requirements.

Professional Development and Resources

Hoke County Schools will continue to provide:

- Training for beginning and advanced GenAI users.
- Professional development related to ethical AI use, classroom integration, academic integrity, and digital citizenship.
- Updated guidance and resources as AI technologies and district expectations evolve.

Staff are encouraged to participate in available professional development and seek support from the Department of Digital Teaching and Learning as needed.

District Devices

The district issues devices to staff based on job responsibilities and instructional need. Devices will not be issued until the appropriate signed user agreements are on file. Use of district-issued devices must comply with all applicable district technology policies and procedures. Device inventory and assignment are maintained by the Technology Department.

Care of Devices

Employees who are issued district devices are expected to take reasonable precautions to prevent damage, loss, or theft. Employees may be required to reimburse the district for damage or loss resulting from negligence.

Always use the district-provided case with assigned devices.

Accidental damage must be reported promptly. Damage that is not reported may be considered improper care of district equipment and may be treated as negligence.

District devices may not be personalized in any way that is not immediately removable or that could leave adhesive, residue, markings, or other permanent changes.

- Do not apply stickers, paint, correction fluid, ink, tape, glue, glitter, rhinestones, or similar materials directly to district devices or district-provided cases.
- Personally owned cases, covers, or bags may be used and personalized, provided they do not damage or alter district equipment.

Reporting Damage, Theft, Viruses, and Other Problems

Damage

Staff members with a damaged Chromebook should submit a work ticket and log in to **1-to-1 Plus** using their HCS Google account.

Stolen Devices

If a district device is stolen, employees should report the theft immediately and provide a copy of the police report when available.

If a police report is provided, the employee will be assessed a \$100 replacement charge. If no police report is provided, the employee may be responsible for the full replacement cost of the device.

Viruses and Malicious Software

If you suspect that a district device has been infected with a virus, malware, or other malicious software, contact the Technology Department immediately at **910-904-0026**.

Student Devices

Hoke County Schools provides students with either iPads (**Pre-K-1**) or Chromebooks (**grades 2-12**), along with an appropriate charger for use at school.

Students in **grades K-8** may opt in to the district's device take-home program. Students in **grades 9-12** are permitted to take devices home unless otherwise directed by the school. Families who wish to opt in to the take-home program should contact their school's Media Coordinator.

Staff should not instruct students to share, lend, or borrow chargers. Charger sharing frequently results in chargers being misplaced or exchanged between students, which may result in charges for missing equipment.

Students who participate in the take-home program are expected to charge their devices at home and leave chargers there. If a student arrives at school with a discharged device, staff should consider alternatives to requiring students to share chargers, including:

- Providing a paper or other non-digital version of the assignment when appropriate.
- Allowing students to collaborate on a shared device when instructionally appropriate.
- Allowing the student to take the device to the media center for charging while returning to class.
- Providing an alternative activity that reinforces the learning objective without requiring a device.

End-of-Year Process

Assigned Computer

At the end of the school year, a Technology Department representative or School Media Coordinator will conduct a physical inspection of assigned technology equipment. The employee and staff representative will complete a sign-out or inspection record documenting the condition of the equipment and any identified damage or concerns.

Staff members who fail to return assigned devices at the conclusion of the school year may be charged the replacement cost of the equipment in accordance with applicable district procedures.

Other Technology

All other district technology assigned to or checked out by an employee must be inspected or returned before the employee completes the end-of-year checkout process. This equipment includes, but is not limited to:

- Document cameras
- Webcams
- Headsets

Use of Personal Devices

Employees may use personally owned technology devices, such as laptops, tablets, and mobile phones, when appropriate for instructional or work-related purposes.

Use of personal devices must comply with all applicable Board policies governing technology, social media, internet access, and electronic communication. Personal devices used for district-related purposes must support appropriate instructional or professional activities and align with district expectations.

Employees use personal devices at their own risk. Hoke County Schools is not responsible for the theft, loss, or damage of personally owned devices.

The Technology Department does not provide technical support, troubleshooting, or repair services for personal devices. Employees are responsible for maintaining and repairing their own equipment.

Wireless Access

Hoke County Schools provides wireless internet access throughout district schools and facilities. Staff members are provided personalized credentials for connecting approved personal devices to the district wireless network.

Each staff member's wireless credentials may be used to connect up to five (5) personal devices, such as a phone, tablet, laptop, or smartwatch.

The **HCS Guest** wireless network is also available in designated common areas of district facilities. Guest access information is provided internally to staff through school administration.

Get Technical Help

Submitting a **work ticket** should be your first step when requesting assistance from the Technology Department. The district work-order system is available under **Staff Resources** on the [HCS district website](#).

Cell Phone Use

District-provided cell phones are subject to all policies and procedures governing district-issued devices. Employees should have no expectation of privacy when using a district-provided phone or storing information on it. District-provided phones may be reviewed, accessed, or collected by authorized district personnel as permitted by district policy and applicable law.

If an employee declines a district-provided phone that is considered necessary for the position, the employee may be required to provide a personal phone number to appropriate district staff and maintain sufficient cellular service to meet the communication requirements of the position.

Securing Data at Rest & Transit

Google Drive

Hoke County Schools uses **Google Drive** as the primary platform for storing and collaborating on work-related files.

Employees are responsible for managing access to files and folders appropriately. Files placed in a shared folder are generally accessible to other users who have access to that folder, so sharing permissions should be reviewed carefully when storing sensitive information.

Any suspected Google Drive or cloud-storage security issue should be reported to the Technology Department immediately.

Google Drive also supports real-time collaboration, allowing multiple users to securely access and work on shared documents.

Personal Cloud Storage

District records, student information, staff information, and other protected or confidential data should not be stored in personally owned cloud-storage accounts or services.

Employees should not use personal Google Drive, Dropbox, OneDrive, iCloud, or similar services to store district-related files containing protected information. Work-related files should be stored using district-approved systems and accounts.

External Storage

External storage devices include portable media such as USB drives, rewritable CDs, and external hard drives.

Although these devices may be useful in limited situations, employees are strongly encouraged to use their district-provided **Google Workspace for Education Drive account** for work-related file storage whenever possible.

Employees are responsible for any content stored on external devices connected to district technology resources. This includes ensuring that:

- The device is free of viruses, malware, or other harmful software.
- Files containing student or staff information are appropriately protected.
- Confidential, classified, or restricted information is not stored on external storage devices.
- District-created or district-provided content is removed from personal storage devices when the employee leaves the district.

Transferring Files

The same security expectations that apply to stored files also apply when files are being transferred.

Employees are responsible for protecting sensitive information during transmission and should only use district-approved methods for sending or receiving protected data.

Confidential, classified, or restricted information should not be transferred through unapproved email, cloud-storage services, external storage devices, or third-party file-transfer services.

When secure file transmission is required, the Technology Department can assist with approved methods and systems. This may include district-approved software or websites that routinely exchange student or staff information.

See the **Digital Resources** section for information about requesting approval for software or online services.

Exceptions

Exceptions to district technology rules may be made for authorized district employees or agents conducting an investigation into activity that may violate applicable law, district policy, or established procedures.

Exceptions may also be made for authorized Technology Department personnel who require access to district technology resources in order to maintain systems, investigate technical or security issues, or review and remove data in accordance with district retention policies and applicable law.