Union County Public Schools Chromebook Handbook

UNION COUNTY PUBLIC SCHOOLS

BUILDING TOMORROW, ONE CHILD AT A TIME

TENNESSEE

Technology Device Procedures And Expectations

For Students and Parents

2022-2023

Table of Contents

District Policies and Procedures

The Board of Education policies that are relevant to the use of technology devices include but are not limited to 4.406, Internet Safety and Use of Digital Technology, found on pages 15-17.

Expectations

RECEIVING A TECHNOLOGY DEVICE

A system-wide process for training and deployment will occur for each school's student deployment.

- The session will consist of completion of paperwork and training sessions for students and parents/guardians.
- Parent/guardian and the student must sign and return the Union County Schools Technology Device Agreement before the device can be issued to the student.
- All students must have Chromebook for testing. BYOD is not an option due to test security.
- Students will use technology devices in a manner consistent with All Board of Education policies and district procedures and school rules.

Students will not receive their technology devices until their parents/guardians have attended a training session and signed the appropriate paperwork.

RETURNING A TECHNOLOGY DEVICE

- The individual's school technology device and accessories (technology device and charger, as well as any additional protective covering provided by the school) must be returned to the school at the end of each school year.
- Students who graduate early, withdraw, are suspended or expelled, or terminate enrollment for any other reason must return their school technology device on the date of termination. School records will not be released until the device and adapter are returned or paid for.
- Students who transfer from one school within the district to another school in the district must turn in their devices before transferring. The devices will be checked for damage before student records will be released.
- If a student fails to return the technology device at the end of the school year or upon the termination of enrollment, that student/parent/guardian will be subject to the replacement cost of the device. The technology devices are the property of Union County Schools.
- The student will be responsible for any damage to the technology device, charger, or protective covering. The student will be charged for any needed repairs, not to exceed the replacement cost of the technology device.
- At the end of the school year any remaining charges or missing devices or adaptors, damage to devices will result in the student becoming a day user the following year in which the student will not be allowed to take the device home and must check out a loaner device from his/her classes.

Reference School Board Policy 6.311 **(Pg. 18)**

Throughout the remainder of this document, the term Technology Device includes the device and charger.

Technology Device Use

- The care of the district technology device is the student’s responsibility. Students should not lend their technology devices to another person. If a student lends their device to another, the student who lent the device is responsible for any damages that take place as a result. Each technology device is assigned to an individual student and the responsibility for the care of the technology device rests solely with that student.
- Students should never leave the technology device unattended. When not in a student's possession, it should be in a secure, locked environment. For example, students are strongly encouraged to have locks on their school lockers.
- Students need to charge their technology devices each night at home so that it is fully charged when they arrive at school each day.
- If a student is a day user, the student must pick up his/her device before school or during breaks between classes.
- Failure to bring the district issued technology device (no personal home device) or other class materials does not release a studentucps.org from his/her responsibility for classwork. If a student repeatedly fails to bring materials to class, including the technology device, progressive discipline procedures will be followed.
- The technology device is the property of the Union County Schools and may be collected and inspected at any time. Students have no right to privacy for any material on a district technology device.
- Each technology device has a unique serial number and asset tag. Students should not modify or remove the tag. Students should not write on, draw on, or add stickers or labels directly to the technology device. No other form of tampering will be permitted.
- If a student’s technology device is not working or is damaged, the student must report the problem immediately to the technology coach or teacher at their school.
- If a label has been damaged or has fallen off, the student must return the device to the help desk. If no one is at the help desk the student must return the device to the technology coach or teacher so that a new label can be made and placed on the device.
- If a student's technology device is lost or stolen at school, the student must report the loss immediately to the school administration. If a student’s technology device is lost or stolen outside of school, parents/guardians must report the loss immediately to the local police and obtain a police report. If student’s technology device is lost or stolen at an unknown location, please treat it as if it had been lost or stolen outside of school.
- Students are responsible for using the technology device according to school and district policies and procedures.

Technology Device Guidelines

CARE & MAINTENANCE

• Devices should **NEVER** be picked up by the lid. Students should close the technology device before it is picked up.
• Students will use the school-issued protective covering/bag.
• When carrying the device to and from school campus, it is expected that the device will be placed in a backpack, bag, or other carrying cases.
• It is recommended that if students use a backpack, then the technology device should always be placed in the backpack with the port-side facing up. Technology devices should be kept at room temperature and should **NOT** be exposed to extremes of hot or cold. Students should **NOT LEAVE** their technology device **IN AN AUTOMOBILE**. Students should not leave their technology devices outside.
• Liquids and food should not be used/consumed in the vicinity of the technology device.
• Cleaners, sprays, alcohol, ammonia, or abrasives should not be on the technology device.
• Devices should be cleaned with a soft, lint-free cloth.
• The device should remain in the protective cover when not in use. The device should not be in a place where someone could accidentally sit or step on it.
• Devices can be tripping hazards when they are charging. Please be very careful to charge your device in such a manner that others will not trip over the wire.

TECHNOLOGY DEVICE PARENT/GUARDIAN GUIDE

• Monitor your child’s home and school use of the Internet, set filtering on school devices at home, and set the language sentiment analysis tool to warn you of cyberbullying and self-harm.
• Provide a place in an open area of your home, such as the kitchen or family room, where the technology device will be used.
• Use the Internet with your child to help develop safe Internet habits.
• Frequently ask to see your child’s technology device and ask how it is being used.
• Review with your child the programs installed on the technology device and ask them what each program does.
• Do not hesitate to contact your school if you have any questions or concerns about the technology device.

MAXIMIZE BATTERY LIFE

Students should use the technology device in a way that maximizes their battery life.

• Energy: The Energy Saver control panel offers several settings that determine power levels for the technology device. The technology device knows when it is plugged in and runs accordingly. When on battery power, it will dim the screen and use other components sparingly. If you change this setting to maximize performance, your battery will drain more quickly.

• Brightness: Students should dim the screen to the lowest comfortable level to achieve maximum battery life. For instance, when watching a video in a dark room, you may not need full brightness.
• Bluetooth Wireless: Likewise, you can turn off Bluetooth to maximize your battery life, as it also consumes power when not in use.
• Applications: quit applications when not in use.

Repair and Replacement Guidelines

The following is designed to be a guide and reference for dealing with issues related to student technology device damage with the understanding that the goal is for every student to have an operational device. Typically, issues will arise over one of the following: Theft, Non-preventable Damage, Preventable Damage/Negligence, and Willful Damage/Recklessness. During the time of a review, the student will become a "day user” in which they will check out a machine from their homeroom teacher each morning and return it to their homeroom teacher before they leave school each day.

THEFT/NON-PREVENTABLE DAMAGE

• The theft must be reported as soon as possible.
• An administrator will meet with the student and parent/guardian in order to investigate the theft.
• A police report is required to document a theft.
• After a police report is submitted, the student will be a day user during the time of the investigation. Upon finalizing the report, a student may be issued a new computer.
• For non-preventable Damage (these are rare, but examples might include but are not limited to: auto accident, house fire, etc.), an administrator will meet with the student to investigate the incident and discuss with parent/guardian as necessary.
• Upon determination of a verifiable accident, the student will be issued another computer.

PREVENTABLE DAMAGE/NEGLIGENCE

• Damage must be reported as soon as possible, within a window of one week from the time of the damage unless the damage occurs during a break; in this case, the damage must be reported within one week of the student’s return to school.
• The parent/guardian and student have accepted responsibility for the technology device and therefore are liable for the damage penalty explained in the damage matrix.
• If the computer is still functional it is then considered level 1 damage, the damage penalty can be paid through May 10th and the student will still be able to use the device while waiting for repair. If another incident of level 1 damage occurs, there will not be an additional penalty.
• If the computer is no longer functional or internal components are exposed, it is level 2 damage. In this case, the computer needs to be turned in immediately and the penalty will be due at that time.

• If the adaptor is damaged and must be replaced, the parent/guardian and student are liable for the cost of replacement. Adaptors are NOT included in insurance price. School adaptors cannot be replaced by aftermarket adaptors. Students must return their original adaptor or purchase a new one from the school.
• An administrator will meet with the student to investigate the incident and discuss with parent/guardian as necessary.
• Student will become a "day user" until the damage penalty is received unless it is level 1 damage as indicated above. Principals may make an exception to this rule if the family has started payment and has an agreed-upon payment plan for the remainder of the penalty.

WILLFUL DAMAGE/RECKLESSNESS

• The parent/guardian/guardian and student have accepted responsibility for the machine and therefore are liable for the cost of the repair or replacement of the device.
• An administrator will meet with the student to investigate and discuss with parent/guardian as necessary.
• Student will become a "day user" until the cost of the repair or replacement is received. If the payment is not received within 30 days, the student will be removed from day user status, and will only be able to use classroom loaner machines. Principals may make an exception to this rule if the family has started payment and has an agreed-upon payment plan for the remainder of the charge.
• The replacement cost of the machine cannot be satisfied by families themselves purchasing their own replacement device.
• The replacement cost of the charger or bag cannot be satisfied by families themselves purchasing their own replacement chargers or bags.
• The cost of repairs will be assessed for each reported incident.
• Please note that willful damage also includes asset tags and power supply identifiers. It is not acceptable for a student to intentionally remove asset tags and identifiers.
Multiple offenses should be handled appropriately and in consultation with the district office if necessary.

If a student owes a penalty at the beginning of the school year based on the previous school year, the penalty will have to be paid before a device is issued. Principals may make an exception to this rule if the family has started payment and has an agreed-upon payment plan for the remainder of the charge.

Discipline starts over at the beginning of each school year.

DAMAGE MATRIX

Students may purchase insurance at the beginning of each year at the cost of $5. Insurance does NOT cover the charger or **keys** that have been torn off intentionally. Insurance can be purchased at any time but the device must be inspected before insurance will be issued to ensure damage has not already occurred. Insurance will cover two incidents without cost to parents or guardians. Each unintentional incident after will cost $50 with insurance and the cost of repair without insurance unless damage is deemed intentional by the administration.
The following table summarizes the consequences of the various damage scenarios for the Chromebook and/or loaner Chromebooks:

Damage	**Financial Consequences With Paid Insurance**	**Financial Consequences without Paid Insurance**	**Additional Consequences**
Unintentional/First Offense/Level 1 Damage (even if there is more than one incident in the school year)	$0 penalty	Cost of repair	
Unintentional/Second Offense (excluding Level 1 damage)	$0 penalty	Cost of repair	1 month probationary period as a day user
Unintentional/Third Offense	$50 additional penalty	Cost of the repair	Day user for the remainder of the school year
Unintentional/Fourth Offense	$50 additional penalty	Cost of the repair	The student will only be able to use classroom devices
Intentional Damage	Cost of repair or replacement	Cost of repair or replacement	Day user for the remainder of the school year & disciplinary action will be taken.

***If you choose not to purchase insurance upon receiving your Chromebook, you must have the Chromebook inspected for damage before purchasing it later.**

Acceptable Use Policy

GUIDELINES FOR USE OF TECHNOLOGICAL RESOURCES

Union County School System provides Internet access to students, teachers, and other staff. It allows users to find, utilize, and share information in a variety of unique ways to support our curriculum. The Internet has a vast amount of resources available, including some materials that are not suitable for viewing in a school environment. Union County School System takes every precaution to restrict access to inappropriate information in compliance with the Children's Internet Protection Act (CIPA). However, an industrious user may discover it. It is prohibited to locate materials that are illegal, defamatory, or offensive. We firmly believe that the valuable information and interaction available on the Internet far outweigh the possibility that users may obtain unsuitable material. Disciplinary action will be taken by the Union County Director of Schools and/or the Union County Board of Education against users found sending or acquiring illegal or inappropriate materials over the Internet.

The following actions are not permitted (inclusive of, but not limited to :)

• Users will not use the district's electronic technologies to access, review, upload, download, complete, store, print, post, receive, transmit or distribute:

1. Pornographic, obscene or sexually explicit material or other visual depictions;
2. Obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful or sexually explicit language;
3. Materials that use language or images that are inappropriate in the education setting or disruptive to the educational process;
4. Materials that use language or images that advocate violence or discrimination toward other people or that may constitute harassment, discrimination or threatens the safety of

others;

• Users will not use the district's electronic technologies to knowingly or recklessly post, transmit or distribute false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.
• Users will not use the district's electronic technologies to engage in any illegal act or violate any local, state or federal laws, including downloading copyrighted material.
• Users will not use the district's electronic technologies to vandalize damage or disable the property of another person or organization.
•Users will not make deliberate attempts to degrade or disrupt equipment, software or system performance by spreading computer viruses, engaging in "spamming" or by any other means.
•Users will not tamper with, modify or change the district system software, hardware or wiring or take any action to violate the district's security system.
•Users will not use the district's electronic technologies in such a way as to disrupt the use of the system by other users.

STUDENT INTERNET SAFETY

Students will be instructed as to safe and responsible use of the Internet using readily available and age appropriate tools and information, as the curriculum permits. Students must abide by all laws, this Acceptable Use Policy and all District security policies when using the District network. For additional information regarding students and internet safety please refer to the student discipline handbook.

Cyber Bullying

Cyberbullying Per release of the FCC (Federal Communications Commission) and CIPA (Children's Internet Protection Act) to prohibit inappropriate online behavior which includes interaction with other individuals, students and staff shall not use cell phones, instant messaging, email, chat rooms, social networking sites, or other types of digital technology to bully, threaten, discriminate, or intimidate others.
If a student or staff member receives a text, email, blog comment, social network posts, or message via other Web tools that makes them feel uncomfortable or is not respectful, they must report the incident to the school administrator or building designee, and must not respond to the comment. This policy includes "cyber baiting", a term used for students deliberately provoking a teacher until they lose their composure in order to capture video that is then posted in a public forum online. Any staff member who suspects they have been targeted should immediately inform their supervisor.

Parent/Guardian Consent

We recognize that parents/guardians of minors are responsible for setting and conveying the standards their children should follow when using media and information sources. Accordingly, before a student may independently access the Internet, the student's parent/guardian must be made aware of the possibility that the student could obtain access to inappropriate material while engaged in the independent use of the Internet. The parent/guardian and the student must consent to the student's independent access to the Internet and to the monitoring of the student's communication by school personnel. As an added backup, parents can request a log of their child’s Chromebook activities from our web filter, GoGuardian.

PRIVACY

No right of privacy exists in the use of technological resources. Users should not assume that files or communications accessed, downloaded, created or transmitted using school district technological resources or stored on services or hard drives of individual computers will be private. School district administrators or individuals designated by the Director of Schools may review files, observe screen activity, monitor all communication and intercept email messages to maintain system integrity and to ensure compliance with board policy and applicable laws and regulations. School district personnel will endeavor to monitor the on-line activities of individuals who access the Internet via a school-owned computer. Under certain circumstances, the school may be required to disclose such electronic information to law enforcement or other third parties, for example, as a response to a document production request in a lawsuit.

SECURITY/CARE OF PROPERTY

Security on any computer system is a high priority, especially when the system involves many users. Users are responsible for reporting information security violations to appropriate personnel. Users should not demonstrate the suspected security violation to other users. Unauthorized attempts to log onto any school system computer on the network as a system administrator may result in cancellation of user privileges and/or additional disciplinary action. Any user identified as a security risk or having a history of problems with other systems may be denied access. Users of school district technology resources are expected to respect school district property and be responsible for using the equipment. Users are to follow all instructions regarding maintenance or care of the equipment. Users may be held responsible for any loss or damage caused by intentional or negligent acts in caring for computers while under their control. The school district is responsible for any routine maintenance or standard repairs to school system computers.

Insurance

• Students may purchase insurance at the beginning of each year at the cost of $25. Insurance does NOT cover the charger keys that have been torn off intentionally. Insurance can be purchased at any time but the device must be inspected before insurance will be issued to ensure damage has not already occurred. Insurance will cover two incidents without cost to parents or guardians. Each unintentional incident after will cost $50 with insurance and the cost of repair without insurance unless damage is deemed intentional by administration. (See damage matrix above).

G Suite for Education Notice to Parents and Guardians

This notice describes the personal information we provide to Google for these accounts and how Google collects, uses, and discloses personal information from students in connection with these accounts.

Using their G Suite for Education accounts, students may access and use the following "Core Services" offered by Google (described at https://gsuite.google.com/terms/user_features.html):

Gmail
Google+
Calendar
Chrome Sync
Classroom
Cloud Search
Contacts
Docs, Sheets, Slides, Forms
Drive
Groups
Hangouts, Hangouts Chat, Hangouts Meet, Google Talk
Jamboard
Keep
Sites
Vault

In addition, we also allow students to access certain other Google services with their G Suite for Education accounts. Specifically, your child may have access to the following “Additional Services”:

> YouTube, Blogger, Google Bookmarks, Google Books, Google Earth, Google Maps, Google Play.

Google provides information about the information it collects, as well as how it uses and discloses the information it collects from G Suite for Education accounts in its G Suite for Education Privacy Notice. You can read that notice online at https://gsuite.google.com/terms/education_privacy.html You should review this information in its entirety, but below are answers to some common questions:

What personal information does Google collect?

When creating a student account, Union County Public Schools may provide Google with certain personal information about the student, including, for example, a name, email address, and password. Google may also collect personal information directly from students, such as telephone number for account recovery or a profile photo added to the G Suite for Education account.
When a student uses Google services, Google also collects information based on the use of those services. This includes:

> device information, such as the hardware model, operating system version, unique device identifiers, and mobile network information including phone number;
> log information, including details of how a user used Google services, device event information, and the user's Internet protocol (IP) address;
> location information, as determined by various technologies including IP address, GPS, and other sensors;
> unique application numbers, such as application version number; and
> cookies or similar technologies which are used to collect and store information about a browser or device, such as preferred language and other settings.

How does Google use this information?

In G Suite for Education Core Services, Google uses student personal information to provide, maintain, and protect the services. Google does not serve ads in the Core Services or use personal information collected in the Core Services for advertising purposes.
In Google Additional Services, Google uses the information collected from all Additional Services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and its users. Google may also use this information to offer tailored content, such as more relevant search results. Google may combine personal information from one service with information, including personal information, from other Google services.

Does Google use student personal information for users in K-12 schools to target advertising?

No. For G Suite for Education users in primary and secondary (K-12) schools, Google does not use any user personal information (or any information associated with a G Suite for Education Account) to target ads, whether in Core Services or in other Additional Services accessed while using a G Suite for Education account.

Can my child share information with others using the G Suite for Education account?

We may allow students to access Google services such as Google Docs and Sites, which include features where users can share information with others or publicly. When users share information publicly, it may be indexable by search engines, including Google.

Will Google disclose my child's personal information?

Google will not share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances applies:

- With parental or guardian consent. Google will share personal information with companies, organizations or individuals outside of Google when it has parents' consent (for users below the age of consent), which may be obtained through G Suite for Education schools.
- With Union County Public Schools, G Suite for Education accounts, because they are school-managed accounts, give administrators access to information stored in them.
- For external processing. Google may provide personal information to affiliates or other trusted businesses or persons to process it for Google, based on Google's instructions and in compliance with the G Suite for Education privacy notice and any other appropriate confidentiality and security measures.
- For legal reasons. Google will share personal information with companies, organizations or individuals outside of Google if it has a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to: meet any applicable law, regulation, legal process or enforceable governmental request, enforce applicable Terms of Service, including investigation of potential violations. Detect, prevent, or otherwise address fraud, security or technical issues. Protect against harm to the rights, property or safety of Google, Google users or the public as required or permitted by law.
- Google also shares non-personal information -- such as trends about the use of its services -- publicly and with its partners.

What choices do I have as a parent or guardian?

First, you can consent to the collection and use of your child's information by Google. If you don't provide your consent, we will not create a G Suite for Education account for your child, and Google will not collect or use your child's information as described in this notice.
If you consent to your child's use of G Suite for Education, you can access or request deletion of your child's G Suite for Education account by contacting Lisa Chesney at Union County High School. If you wish to stop any further collection or use of your child's information, you can request that we use the service controls available to limit your child's access to features or services, or delete your child's account entirely. You and your child can also visit https://myaccount.google.com while signed in to

the G Suite for Education account to view and manage the personal information and settings of the account.

What if I have more questions or would like to read further?

If you want to learn more about how Google collects, uses, and discloses personal information to provide services to us, please review the G Suite for Education Privacy Center (at https://www.google.com/edu/trust/), the G Suite for Education Privacy Notice (at https://gsuite.google.com/terms/education_privacy.html), and the Google Privacy Policy (at https://www.google.com/intl/en/policies/privacy/).
The Core G Suite for Education services are provided to us under Google's Apps for Education agreement (at https://www.google.com/apps/intl/en/terms/education_terms.html)

Union County Board of Education

Monitoring: **Review: Annually, in November**	Descriptor Term: **Use of the Internet**	Descriptor Code: **4.406**	Issued Date: **01/10/13**
		Rescinds: **4.406**	Issued: **10/18/11**

The Board supports the right of staff and students to have reasonable access to various information formats and believes that it is incumbent upon staff and students to use this privilege in an appropriate and responsible manner.

Employees

Before any employee is allowed use of the district's Internet or intranet access, the employee shall sign a written agreement, developed by the director/designee that sets out the terms and conditions of such use. Any employee who accesses the district's computer system for any purpose agrees to be bound by the terms of that agreement, even if no signed written agreement is on file.

The director of schools shall develop and implement procedures for appropriate Internet use which shall address the following:

1. Development of the Network and Internet Use Agreement.
2. General rules and ethics of Internet access.
3. Guidelines regarding appropriate instruction and oversight of student Internet use.
4. Prohibited and illegal activities, including but not limited to the following:[1]
    - Sending or displaying offensive messages or pictures
    - Using obscene language
    - Harassing, insulting, defaming or attacking others
    - Damaging computers, computer systems or computer networks
    - Hacking or attempting unauthorized access to any computer
    - Violation of copyright laws
    - Trespassing in another's folders, work or files
    - Intentional misuse of resources
    - Using another's password or other identifier (impersonation)
    - Use of the network for commercial purposes
    - Buying or selling on the Internet

Students

The director of schools shall develop and implement procedures for appropriate Internet use by students. Procedures shall address the following:

1. General rules and ethics of Internet use.
2. Prohibited or illegal activities, including, but not limited to:[1]
    - Sending or displaying offensive messages or pictures
    - Using obscene language

- Harassing, insulting, defaming or attacking others
- Damaging computers, computer systems or computer networks
- Hacking or attempting unauthorized access
- Violation of copyright laws
- Trespassing in another's folders, work or files
- Intentional misuse of resources
- Using another's password or other identifier (impersonation)
- Use of the network for commercial purposes
- Buying or selling on the Internet

INTERNET SAFETY MEASURES [3]

Internet safety measures shall be implemented that effectively address the following:

- Controlling access by students to inappropriate matter on the Internet and World Wide Web
- Safety and security of students when they are using electronic mail, chat rooms, and other forms of direct electronic communications
- Preventing unauthorized access, including "hacking" and other unlawful activities by students on-line
- Unauthorized disclosure, use and dissemination of personal information regarding students
- Restricting students' access to materials harmful to them

The director of schools/designee shall establish a process to ensure the district's education technology is not used for purposes prohibited by law or for accessing sexually explicit materials. The process shall include, but not be limited to:

- Utilizing technology that blocks or filters Internet access (for both students and adults) to material that is obscene, child pornography or harmful to students
- Maintaining and securing a usage log
- Monitoring on-line activities of students[2]

The Board shall provide reasonable public notice of, and at least one (1) public hearing or meeting to address and communicate, its Internet safety measures.

A written parental consent shall be required prior to the student being granted access to electronic media involving district technological resources. The required permission/agreement form, which shall specify acceptable uses, rules of on-line behavior, access privileges and penalties for policy/ procedural violations, must be signed by the parent/legal guardian of minor students (those under 18 years of age) and also by the student. This document shall be executed each year and shall be valid only in the school year in which it was signed unless parent(s) provide written notice that consent is withdrawn. In order to rescind the agreement, the student's parent/guardian (or the student who is at least 18 years old) must provide the director of schools with a written request.

E-MAIL

Users with network access shall not utilize district resources to establish electronic mail accounts through third-party providers or any other nonstandard electronic mail system. All data including e-mail communications stored or transmitted on school system computers shall be monitored. Employees/students have no expectation of privacy with regard to such data. E-mail correspondence may be a public record under the public records law and may be subject to public inspection.[3]

INTERNET SAFETY INSTRUCTION [4]

Students will be given appropriate instruction in internet safety as a part of any instruction utilizing computer resources. The director shall provide adequate in-service instruction on internet safety. Parents and students will be provided with material to raise awareness of the dangers posed by the internet and ways in which the internet may be used safely.

SOCIAL NETWORKING

1. District staff who have a presence on social networking websites are prohibited from posting data, documents, photographs or inappropriate information that is likely to create a material and substantial disruption of classroom activity.

2. District staff are prohibited from accessing personal social networking sites on school computers or during school hours except for legitimate instructional purposes.

3. The Board discourages district staff from socializing with students on social networking websites. The same relationship, exchange, interaction, information, or behavior that would be unacceptable in a non-technological medium is unacceptable when done through the use of technology.

VIOLATIONS

Violations of this policy or a procedure promulgated under its authority shall be handled in accordance with the existing disciplinary procedures of this District.

Legal References

1. TCA 39-14-602
2. TCA 10-7-512
3. Children's Internet Protection Act (Public Law 106-554)
4. TCA 49-1-221

Cross References

Use of Electronic Mail (e-mail) 1.805
Web Pages 4.407

Union County Board of Education

Monitoring:	Descriptor Term:	Descriptor Code:	Issued Date:
Review: Annually, in April	**Care of School Property**	**6.311**	**10/19/11**
		Rescinds:	Issued:
		JCDG	**05/18/95**

Students shall help maintain the school environment, preserve school property and exercise care while using school facilities.

All district employees shall report all damage or loss of school property to the principal or designee immediately after such damage or loss is discovered. The principal or designee shall make a full and complete investigation of any instance of damage or loss of school property. The investigation shall be carried out in cooperation with law enforcement officials when appropriate.

School property is defined as buildings, buses, books, equipment, records, instructional materials or any other item under the jurisdiction of the Board.

When the person causing damage or loss has been identified and the costs of repair or replacement have been determined, the director of schools shall take steps to recover these costs. This may include recommending the filing of a civil complaint in court to recover damages. If the responsible person is a minor, recovery will be sought from the minor's parent or guardian.

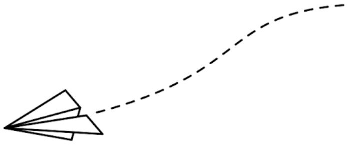
In addition, the district may withhold the grades, diploma, and/or transcript of the student responsible for vandalism or theft or otherwise incurring any debt to a school until the student or the student's parent/guardian has paid for the damages.[1] When the minor and parent are unable to pay for the damages, the district shall provide a program of voluntary work for the minor. Upon completion of the work, the student's grades, diploma, and/or transcripts shall be released. Such sanctions shall not be imposed if the student is not at fault.

Legal Reference:

[1] TCA 37-10-101 through 103

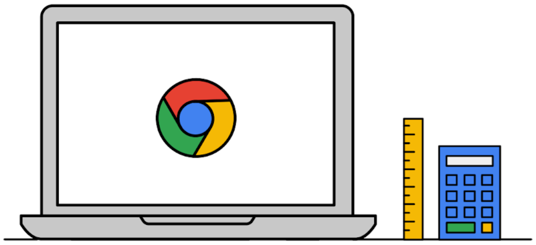
Cross References:

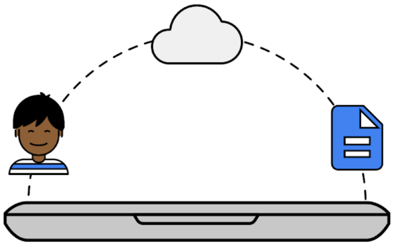
Visitors to the School 1.501
Security 3.205
Student Fees and Fines 6.709



What you've always wanted to know about Chromebooks in your child's classroom

Your child is using a Chromebook at school, and you have some questions. A Chromebook may be different than the computer you have at home, so we want to help you understand what a Chromebook is and how it's used at school.



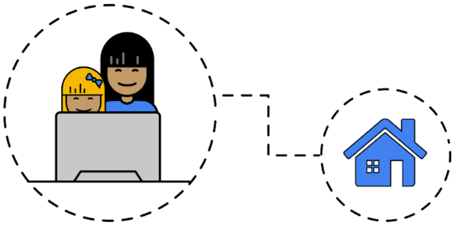


So...what is a Chromebook?

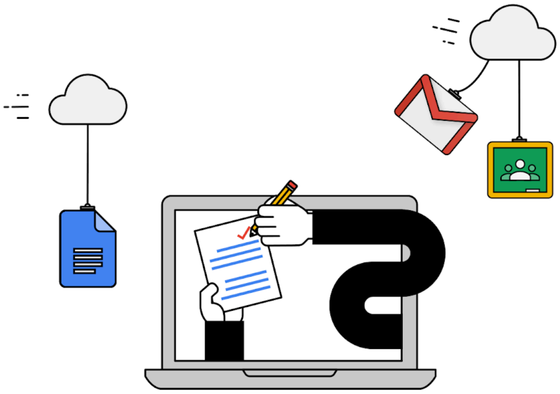
It's a laptop that runs on the Google Chrome operating system. The Chrome operating system is designed to work on the cloud, so that means everything—your files, your apps, even your desktop—lives online (not on your laptop) and is the same wherever you sign in. That means never misplacing your files or losing your work in progress (it's all right on the cloud). No wifi? Chromebooks also store files locally and work offline.

Why did our school choose Chromebooks?

Chromebooks are, by far, the #1 devices in schools because they're easy to use, versatile, and secure—we know trust is earned by protecting privacy and providing worry-free security. It helps that Chromebooks come as laptops and tablets with big screens and small screens, and entry models are affordable. They are built to be shareable. This means you and your child can use the same Chromebook and each have your own profile and files. In fact, in many schools, students share Chromebooks with each other.



Students can use their EDU accounts to continue **learning at home**



What does your child actually do on a Chromebook?

That varies from school to school, but the answer may be, "just about everything." Popular tools like Gmail and Google Docs make classroom collaboration easy, and there are apps to learn skills like video-making, podcasting, and coding. You may also have heard your child talk about Google Classroom. It's a tool some teachers use to help organize student classwork and assign homework and projects.

Here are some amazing things you can do on a Chromebook

Video editing
Tell stories with videos you produce yourself

Coding
Learn to code no matter what grade you're in

Drawing
Create art on your laptop

Want to know more? Here are some conversation starters with your child.

Do you have your own Chromebook at school, or do you share?

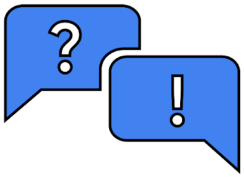
What is your favorite thing to do on a Chromebook?

What rules does your school have about using Chromebooks?

When do you use your Chromebook in school?

How has a Chromebook changed your school day?

What's the most amazing thing you can do or create with a Chromebook?



If you want to know more about Chromebooks, check out google.com/chromebook/for-families

Google for Education

Chromebooks Privacy and Security

google.com/edu/privacy

What are Chromebooks?

Chromebooks for Education are lightweight, durable laptops designed for the classroom. Made for learning and online exploration, Chromebooks are perfect for schools that are evolving to keep up with the increasingly digital world.

Chromebooks are simple, affordable, easy to share, and extremely secure, making them the #1 selling device to US classrooms.

#1

Chromebooks are the #1 device in US K-12 schools

50

School districts in all 50 states & DC use Chromebooks

13

Manufacturers make over 30 models of Chromebooks

What are the benefits of Chromebooks?

Simple

Administrators control Chromebooks from the cloud and not locally, which makes them very easy to manage. This also makes them scalable so administrators can deploy as many laptops as their school might need, whether it's 10 or 10,000.

Affordable

Designed with affordability in mind, Chromebooks start at just $149. More importantly, research finds that the total cost of owning and supporting Chromebooks is over 60% less than alternative devices.

Shareable

Chromebooks are designed to provide a secure experience, even if they're shared among multiple users. Many applications store student files on the web and local files are 128-bit encrypted. This means that every student's work and information is kept completely private and also that students are able to access all their own classwork, apps, books, and videos securely just by signing into any Chromebook.

Secure

Multiple layers of security are built into every Chromebook so that they are safe for use right out the box — no antivirus software required. Along with the built-in security features, Chromebooks employ ongoing security measures such as regular automatic updates and Chromebook users have access to 24/7 support directly from Google.

Chromebooks Privacy & Security

Privacy and security features helped make Chromebooks the top selling device to US K–12 schools for the past two years. Administrators can manage settings to give students as much or as little access as the school desires. Chromebooks adhere to the Student Privacy Pledge so that schools can use these in compliance with COPPA and FERPA. Specifically, we ensure that no data entered into a Chromebook is used to target advertisements to students.

Chromebook security features

Chromebooks use the philosophy of "defense in depth" to provide their users with multiple layers of protection, so if any one layer is bypassed, others are still in effect. Your Chromebook has the following security features built-in:

Automatic updates: Chromebooks automatically manage their updates because the most effective way to protect against malware is to ensure all software is up-to-date.

Verified Boot: Upon startup, Chromebooks perform a self-check called "Verified Boot" and will repair themselves if they detect their system has been corrupted in any way.

Sandboxing: On a Chromebook, each web page and application runs in a restricted environment called a "sandbox," so if it is directed to an infected page, the rest of the machine won't be affected.

Data Encryption: Chromebooks are completely 128-bit encrypted for every user, so every user's space is unique, totally secure, and never accessible by another user.

How is data used and protected for students on Chromebooks for Education?

Chrome Sync enables Google Account holders to log into any Chromebook or Chrome browser and find all their apps, extensions, and bookmarks. For students, this means that they can get to work right away on any computer. This makes Chromebooks popular for schools that can't afford a device for every child. When our systems do compile and collect data, it is only used after the information has been completely scrubbed for information about individual users. This data is used to improve the services we provide. For example if data shows that millions of people are visiting a webpage that is broken, that site would be moved lower in the search results. If they choose to, administrators can disable Chrome Sync and users can choose what information to sync. G Suite for Education users' Chrome Sync data is not used to target ads to individual students.

Are Chromebooks secure for my students?

Chromebooks are designed with multiple layers of security to keep them safe from viruses and malware. In fact, a full 10% of boot time is dedicated to re-verifying that the device has not been tampered with. Because they can be managed from the web, Chromebooks make it easy for school administrators to configure policies and settings, like enabling safe browsing or blocking malicious sites.

Are Chromebooks compatible with online testing?

Chromebooks are a secure platform for administering student assessments. During an exam you can disable features such as web browsing, external storage access, screenshots, and the ability to print. Both PARCC (see TestNav) and the Smarter Balanced Assessment consortia have verified that Chromebooks meet their hardware and operating system requirements for students.

Can others steal school-assigned Chromebooks?

Chromebook Device Settings include a Lost/Stolen mode, so you can lock a device that has been stolen and prompt a message of how to return the device. You can also apply sign in restrictions so only school users can sign in with their education account. You fully control your Chromebooks and can choose that they be used only by your school and always with your your settings.

Learn more about Google for Education's commitment to privacy and security at google.com/edu/privacy

G Suite for Education

Privacy and Security Information

google.com/edu/privacy

The mission of Google is to organize the world's information and make it universally accessible and useful. Ensuring teachers and students everywhere have access to technology to learn and work together fits naturally with that mission. That is why we provide educators with powerful solutions that are affordable, safe and easy to use.

The G Suite for Education core services are the heart of Google's educational offering to schools. The core services are Gmail, Calendar, Classroom, Contacts, Drive, Docs, Groups, Sheets, Sites, Slides, Talk/Hangouts and Vault. We know that trust is earned through protecting teacher and student privacy and providing the best security measures. This handout tells more about the core services and explains our privacy and security commitments.

YOU'RE IN GOOD COMPANY

60 million
Students and teachers use G Suite for Education

7 of 8
Ivy League Universities use G Suite for Education

5 million
Businesses use G Suite

HOW SOME OF OUR TOOLS ARE USED IN SCHOOLS:

Google Docs, Sheets and **Slides** enable students to collaborate with their peers and teachers in real-time, allowing them to share their work, get feedback, and make edits instantaneously. They can be kept private, shared with others (such as a parent, or the entire class), or even made public. Best of all they can be accessed from any computer or tablet, anywhere, anytime.

Teachers can save time and better engage their students by using **Google Classroom** to send assignments and resources digitally. In addition, Classroom allows teachers to ensure their students are submitting their work on time. Students using Classroom can easily see when their assignments are due, and are given clear notifications when their work is late, helping them stay on track and organized.

Google Sites allows teachers and students to create their own websites, without needing to code. Often, this tool is used to let students create personalized e-portfolios, so that teachers and parents may track their student's development with ease. Teachers can also use Google Sites to create quick and easy webpages for their class, sport, or club.

The tools in Google's **Admin Console** allow administrators to personalize the G Suite for Education experience for their schools, teachers, and students. For example, an administrator may block Gmail for kindergarteners, but may allow older students to email people within the same school. Administrators may also choose to block certain webpages, ensuring their students stay safe and productive.

Google Vault gives schools the ability to archive emails and Documents. This means that if a student or teacher accidentally deletes a file it can be recovered quickly and painlessly. Vault is also an important part of legal compliance for schools — if there is ever a legal matter that requires old emails to be reviewed, Vault allows administrators to find them easily and quickly.

Protecting Student Data and Privacy

Does Google own school or student data?
No. Google doesn't assume ownership of any customer data in G Suite core services, and it says so in our contracts (under "Intellectual Property").
We provide powerful, easy-to-use management tools and dashboards to help administrators keep track of their organization's services, usage and data.
We only keep your personal information as long as you ask us to keep it. If an education department, school or university decides to stop using Google, we make it easy for them to take their data with them.

Are there ads in G Suite for Education?
No. There are no ads in G Suite for Education core services and we do not collect or use student data for advertising purposes or create advertising profiles. K-12 G Suite for Education users also don't see ads when they use Google search while signed in to their G Suite for Education accounts. Some of Google's additional services such as Blogger and YouTube do show ads to students, however we give Administrators the ability to restrict access to these services.

Has Google signed the Privacy Pledge?
Yes. In order to reaffirm the commitments we've made to schools, Google has signed the Student Privacy Pledge introduced by the Future of Privacy Forum (FPF) and The Software & Information Industry Association

Our Commitment and Compliance

Is my organization compliant with Family Educational Rights and Privacy Act (FERPA)?
Yes. G Suite for Education core services comply with the Family Educational Rights and Privacy Act (FERPA) and our commitment to do so is included in our agreements.

Can G Suite for Education be used in compliance with the Children's Online Privacy Protection Act (COPPA)?
Yes. We contractually require that schools using G Suite for Education get the parental consent required by COPPA. Our services can be used in compliance with COPPA as long as a school has parental consent.

How do we know you are keeping your word?
We make contractual commitments in our G Suite for Education agreement and commit to comply with privacy and security standards. And whether it's real time dashboards to verify system performance, our ongoing auditing of our processes or sharing the location of our datacenters, we're committed to providing all our users utmost transparency. It's your data, and we want you to know what happens with it so that you can always make informed choices.

Security and Privacy

Which third parties have reviewed Google's security practices?
Independent auditors and third party organizations have verified that our privacy practices and contractual commitments for G Suite for Education comply with data standards*. Ernst & Young verified that our privacy practices and contractual commitments for G Suite for Education comply with ISO/IEC 27018:2014.

* ISO/IEC 27018:2014 and SSAE 16 / ISAE 3402 Type II SOC 2

How does Google keep data secure?
We are fully committed to the security and privacy of your data and protecting you and your school from attempts to compromise it. Our systems are among the industry's most secure and we vigorously resist any unlawful attempt to access our customers' data.

Google's data centers use custom hardware running a custom hardened operating system and file system. Each of these systems has been optimized for security and performance. Because Google controls the entire hardware stack, we are able to quickly respond to any threats or weaknesses that may emerge.

Google encrypts Gmail (including attachments) and Drive data while on the move. This ensures that your messages are safe not only when they move between you and Google's servers, but also as they move between Google's data centers.

Learn more about Google for Education's commitment to privacy and security at google.com/edu/privacy

Staying Safe Online

We also have a lot of information about how you can keep yourself and your students safe online at home too, even when they are using tools outside of school. To learn more, visit our Family Safety Center at google.com/safetycenter

G Suite for Education

google.com/edu/privacy

Acceptable Use Policy/Chromebook Handbook

Student: I understand and will abide by the Acceptable Use Policy (pg. 9) and Chromebook procedures. I understand that UCPS and/or its agents may access and monitor my use of the Internet, including my email and downloaded material without prior notice to me. I further understand that should I commit any violation, my access privileges may be revoked and school disciplinary action and/or appropriate legal action may be taken. In consideration for using UCPS's electronic network connection and having access to public networks, I hereby release UCPS and its school board members, employees, and agents from any claims and damages arising from my use or inability to use the Internet or school email.

______________________________ _______________

Signature of student Date

Acceptable Use Policy/Chromebook Handbook

Parent: I understand and will abide by the Acceptable Use Policy (pg. 9) and Chromebook procedures. I understand that access is designed for educational purposes and that Union County Public Schools have taken precautions to eliminate controversial material. However, I also recognize it is impossible for UCPS to restrict all controversial and inappropriate materials. I will hold harmless UCPS, it's employees, agents or School Board members, for any harm caused by materials or software obtained via the network. I accept full responsibility if and when my child's use is not in a school setting. I have discussed the terms of this Authorization with my child. I Hereby request that my child is allowed access to the District's Internet and school email account. I also give permission for Union County Public Schools to create/maintain a G Suite for Education account for my child and for Google to collect, use, and disclose information about my child only for the purposes described on pages 12-14. The Board of Education policies that are relevant to the use of technology devices include but are not limited to 4.406, Internet Safety and Use of Digital Technology, found at Internet Safety and Use of Digital Technology.

______________________________ _______________

Signature of Parent/Guardian Date