Carterville CUSD #5
Parent/Student

Chromebook User Guide and Handbook

Use of Technology

Students in grades K-12 will have access to Google Chromebooks for educational use in school. A ratio of 1:1 has been established for grades 6-12 and a 1:2 ratio for grades K-5. In grades K-5, every attempt will be made to provide a device to students who do not have one at home. This document provides students and parents/guardians with information about the general use of technology, ownership of the devics, rights and responsibilities for possession of the device, educational use, care of the Chromebook, and being a good digital citizen. Additionally, the last page is a Chromebook Agreement form for parents to complete.

To understand the technology use expectations, students and their parents/guardians are responsible for reviewing the Carterville CUSD 5 Acceptable Use Policy.

Ownership of the Chromebook

Carterville Unit 5 retains sole right of possession of the Chromebook. Carterville CUSD 5 lends the Chromebook to the students for educational purposes only for the academic year. Additionally, Carterville Unit 5 administrative staff and faculty retain the right to collect and/or inspect Chromebooks at any time, including via electronic remote access, and to alter, add, or delete installed software or hardware.

Receiving Your Chromebook (Gr. K-12)

Parent/Guardian Distribution

All parents/guardians are requested to read and agree to the Carterville CUSD 5 Chromebook Handbook and Agreement before a Chromebook will be issued to their student. Procedures for receiving a Chromebook will be determined by school building, but student and guardian signature to the Chromebook agreement is required.

Returning Your Chromebook (Gr. K-12)

End of Year

At the end of the school year, students may be asked to turn in their Chromebooks and any peripherals and accessories. Failure to turn in a Chromebook will result in the student being charged the full $300.00 replacement cost. Additionally, a report of stolen property with the local law enforcement agency will be filed by the school or school designee.

Graduation and Withdraw

Prior to graduation, students will return their Chromebook to Carterville High School. Likewise, students who withdraw from the school district are responsible for turning in their Chromebook to the school office.

Transferring/Withdrawing Students

The students are solely responsible for any apps or extensions on their Chromebooks that are not installed by a member of the Carterville Unit 5 technology staff. Students are responsible for backing up their data to protect

from loss. Users of school technology have no rights, ownership, or expectations of privacy to any data that is, or was, stored on the Chromebook, school network, or any school-issued applications and are given no guarantees that data will be retained or destroyed.

Operating System and Security

Students may not use or install any operating system on their Chromebook other than the current version of Chrome OS that is supported and managed by the school.

Updates

- The Chromebook operating system, Chrome OS, updates itself automatically. Students do not need to manually update their Chromebook.

Virus Protection

- Chromebooks use the principle of “defense in depth” to provide multiple layers of protection against viruses and malware, including data encryption and verified boot.
- No additional virus protection is needed.

Content Filter

The school utilizes an Internet content filter that is in compliance with the federally mandated Children’s Internet Protection Act (CIPA). All Chromebooks will have all Internet activity protected and monitored by the school. If an educationally valuable site is blocked, students should contact their teachers to request the site be unblocked. Parents/guardians are responsible for filtering and monitoring any Internet connection students receive that is not provided by the school.

Software

Google Apps for Education/G Suite

- Chromebooks seamlessly integrate with the Google Apps for Education/G Suite productivity and collaboration tools. This Suite includes Google Docs (word processing), Spreadsheets, Presentations, Drawings, and Forms
- Google Classroom (Gr. 3-12) and Seesaw (Gr. K-2) are learning management systems that Carterville Unit 5 faculty will use to provide students with assignments, announcements, and other communications. Grades K-6 will also use ClassDojo for parent communication.
- Student work is stored in the cloud.

Chrome Web Apps and Extensions

- Students are responsible for the web apps and extensions they install on their Chromebooks. Inappropriate material will result in disciplinary action.

- Some web apps will be available to use when the Chromebook is not connected to the Internet.

Chromebook Identification

Records

- The school will maintain a log of all Chromebooks that includes the Chromebook serial number, name, and ID number assigned to the device.

Users

- Each student will be assigned the same Chromebook for the duration of his/her time at Carterville Unit 5.

Repairing/Replacing Your Chromebook

Vendor Warranty

- Chromebooks include a one-year hardware warranty from the vendor.
- The vendor warrants the Chromebook from defects in materials and workmanship.
- The limited warranty covers normal use, mechanical breakdown, and faulty construction. The vendor will provide normal replacement parts necessary to repair the Chromebook or, if required, a Chromebook replacement.
- The vendor warranty does not warrant against damage caused by misuse, abuse, or accidents.

Estimated Costs (subject to change)

The following are estimated costs of Chromebook parts and replacements:

- Complete Replacement Device & Accessories- $300.00
- Screen and/or Keyboard Repair - Cost per rate
- Protective Case $20.00
- Power Cord $20.00

No Expectation of Privacy

Students should have no expectation of confidentiality or privacy with respect to any usage of a Chromebook, regardless of whether that use is for school-related or personal purposes, other than as specifically provided by law. The school may, without prior notice or consent, log, supervise, access, view, monitor, and record use of student Chromebooks at any time for any reason related to the operation of the school. By using a Chromebook, students agree to such access, monitoring, and recording of their use.

Monitoring Software

Teachers, school administrators, and the technology department staff may use monitoring software that allows them to view the screens and activity on student Chromebooks.

Educational Use

School-issued Chromebooks should be used for educational purposes, and students are to adhere to the Acceptable Use Policy and all of its corresponding administrative procedures at all times.

Using Your Chromebook at School

Students are expected to bring a fully charged Chromebook to school every day; in addition, Chromebooks should be taken to all classes during the day unless specifically told otherwise by their teachers.

Chromebooks being repaired or forgotten at home

- Loaner Chromebooks may be issued to students when they leave their school-issued Chromebook for repair or forgotten at home.
- Chromebooks on loan to students having their devices repaired or when forgotten may not be taken home, unless permitted by the school administration.
- Loaner Chromebooks MUST NOT BE TAKEN from the school and MUST BE RETURNED on the same day borrowed.

Charging Chromebooks

- Chromebooks must be brought to school each day with a full charge.
- Students should charge their Chromebooks at home every evening.
- An uncharged Chromebook is in violation of this agreement.
- Violation may result in disciplinary action.

Backgrounds and Themes

- Inappropriate media may not be used as Chromebook backgrounds or themes. No images or graphics containing people can ever be used as a background or theme. The presence of such media will result in disciplinary action.

Sound

- Sound must be muted at all times unless permission is obtained from a teacher.
- Headphones may be used only if the instructional software has an audio component.
- Students should have their own personal set of headphones for sanitary reasons.

Printing

- Students will be encouraged to digitally publish and share their work with their teachers and peers when appropriate.
- All student work should be stored in an Internet/cloud application. Students will not print directly from their Chromebooks at school. Any printing that needs to be done must be accomplished at home or with the assistance of a staff member.
- Students may set up their home printers with the Google Cloud Print solution to print from their Chromebooks at home. Information about Google Cloud Print can be obtained here: http://www.google.com/cloudprint/learn/

Logging Into Chromebook

- Students will log into their Chromebooks using their school-issued Google Apps for Education/G Suite account.
- Students should never share their account passwords with others.

Using Your Chromebook Outside of School

Students are encouraged to use their Chromebooks at home and other locations outside of school. A WiFi Internet connection will be required for the majority of Chromebook use; however, some applications can be used while not connected to the Internet. Students are bound by the Carterville Unit 5 Acceptable Use Policy, Administrative Procedures, and all other guidelines in this document wherever they use their Chromebooks.

Chromebooks Left at Home

Students are required to bring their Chromebook to school every day. Repeat offenders who leave their device at home may receive a disciplinary action.

Chromebook Care

Taking Care of your Chromebook

Students are responsible for the general care of the Chromebook they have been issued by the school. Chromebooks that are broken or fail to work properly must be reported to a teacher or administrator as soon as possible so they can be taken care of properly. School-owned Chromebooks should NEVER be taken to an outside computer service for any type of repairs or maintenance. Students should never leave their Chromebook unattended except when locked in their hallway locker (when applicable).

General Precautions

- No food or drink should be next to a Chromebook; however, the school may designate acceptable use area(s).
- Cords, cables, and removable storage devices must be inserted carefully into Chromebooks.
- Chromebooks should not be used or stored near pets.
- Chromebooks should not be used with the power cord plugged in when the cord may be a tripping hazard.
- Chromebooks must remain free of any writing, drawing, stickers, and labels.
- Heavy objects should never be placed on top of Chromebooks.

Carrying Chromebooks

- Always transport Chromebooks with care and with the screen closed. Failure to do so may result in disciplinary action.
- Never lift Chromebooks by the screen.
- Never carry Chromebooks with the screen open.

Screen Care

- The Chromebook screen can be damaged if subjected to heavy objects, rough treatment, some cleaning solvents, and other liquids. The screens are particularly sensitive to damage from excessive pressure, heat, and light.
- Do not put pressure on the top of a Chromebook when it is closed.
- Do not store a Chromebook with the screen open.
- Make sure there is nothing on the keyboard before closing the lid (e.g., pens, pencils, ear buds).
- Only clean the screen with a soft, dry microfiber cloth or anti-static cloth.

Asset Tags and Logos

- All Chromebooks are labeled with a Carterville Unit 5 ID number.
- Asset ID tags and logos may not be modified or tampered with in any way.
- Students may be charged up to the full replacement cost of a Chromebook for tampering with a school asset ID/logo or turning in a Chromebook without a school asset tag or logo.

Chromebooks Left Unattended

Under no circumstances should Chromebooks be left in unsupervised areas. Unsupervised areas include the school grounds, the lunchroom, vehicles, bathrooms, computer labs, library, unlocked classrooms, stairways, and hallways. Any Chromebook left in these areas is in danger of being stolen. If a Chromebook is found in an unsupervised area, it should be taken immediately to the office. Multiple offenses will result in disciplinary action

Warranty and Insurance

The school will repair or replace damaged equipment resulting from normal use and accidents. The school will make its best attempt to purchase replacement parts at the best possible price. Abuse or neglect may result in damages. Costs incurred are the responsibility of the student. Parents are strongly encouraged to purchase insurance. Insurance information is available from the school's office.

In case of theft, vandalism, or other criminal acts, a police report MUST be filed with the local police department and a copy submitted to the office of the campus where the student attends.

Proper Care and Handling of Chromebooks in the Classroom

Chargers

- Avoid bending the charger cord at sharp angles.
- Don't strain the power cord at right angles to the power port. This can damage the charger cord and the computer itself.
- Position your charger so that you won't roll over the cord with a chair or catch the cord in the sharp edges of desk drawers.
- Disconnect all connected cords, USB memory sticks, and any adapters before putting your Chromebook into a carrying case, bag, or slot in a mobile cart.
- Be careful and gentle as you connect and disconnect the power cord.

Heat

- Always place your Chromebook on a flat, stable surface.
- Do not place it on top of stacks of paper, blankets, upholstery, or anything else that is an insulator.
- The bottom of your Chromebook is a cooling surface. Excessive heat buildup will lead to premature failure. The computer needs proper airflow to operate correctly.

Gravity

- Don't drop them. A drop can break the hinge, latch, or worse.
- Keep your Chromebook away from the edges of tables and desks.

Liquids

- Keep liquids away from your Chromebook. Liquids damage the electronic components quickly and easily. Always put water bottles or any other liquids on the floor while using these devices.

The Screen

- Your Chromebook’s LCD Display is a very expensive component, and physical damage to it is not covered by warranty. If you drop your Chromebook or slam the lid shut, it may crack. Make sure you don't have anything between the screen and keyboard as you close the case, such as a pencil.
- If you open the screen beyond its hinge limitation, it will break and be very costly to repair. It is not designed to open to a flat position. Keep Chromebook free from papers and other objects before closing it.
- Do not pick it up by the screen.
- Don't place items on top of your Chromebook as the weight can cause damage to the screen. Always keep magnetic devices away from your Chromebook.

Keep it Cleaned and Refreshed

- Don't use your Chromebook while you eat. Make sure your hands are clean when using your Chromebook.
- Don't use aerosol sprays, solvents, or abrasives.
- To refresh the device, shutdown your Chromebook and disconnect the power adapter. Use a damp, soft, lint free cloth to clean the computer's exterior. Avoid getting moisture in any openings. Do not spray liquid directly on the computer.

Proper Way to Carry Your Chromebook

- Be sure to use both hands if you are moving your Chromebook.
- Never lift or carry by the screen as you can either break the screen or damage the hinge. It is safer to close the Chromebook before moving.

Authorized Users

- The school Chromebook is assigned to you for your use alone. Please don't allow others to use your device. Remember you are responsible for any damage or misuse. Additionally, using someone else’s account is subject to discipline.

Keep Your Chromebook Secure

- Please keep Chromebook in a secure area when not in use. Do not leave your Chromebook sitting in an empty classroom or any other area without adult supervision. If using Chromebook cart, replace the Chromebook back to the assigned slot.

Stay Out of the Inside

- Under no circumstances should you open (or attempt to open) your school computer's case. Touching the wrong components may not only damage the computer--it may seriously hurt you. Report the failure to your teacher or IT person in your school. Let a district technician handle any repairs that require the case to be opened.

Digital Citizenship

Appropriate Uses and Digital CItizenship

While working in a digital and collaborative environment, students should always conduct themselves as good digital citizens by adhering to the following:

1. Respect Yourself-I will show respect for myself through my actions. I will select online names that are appropriate. I will use caution with the information, images, and other media that I post online. I will carefully consider what personal information about my life, experiences, or relationships I post. I will not be obscene. I will act with integrity.
2. Protect Yourself-I will ensure that the information, images, and materials I post online will not put me at risk. I will not publish my personal details, contact details, or a schedule of my activities. I will report any attacks or inappropriate behavior directed at me while online. I will protect passwords, accounts, and resources.
3. Respect Others- I will show respect to others. I will not use electronic mediums to antagonize, bully, harass, or stalk people. I will show respect for other people in my choice of websites. I will not visit sites that are degrading to others, pornographic, racist, or inappropriate. I will not enter other people's private spaces or areas.
4. Protect Others-I will protect others by reporting abuse and not forwarding inappropriate materials or communications. I will avoid unacceptable materials and conversations.
5. Respect Intellectual Property- I will request permission to use copyrighted or otherwise protected materials. I will suitably cite all use of websites, books, media, etc. I will acknowledge all primary sources. I will validate information. I will use and abide by the fair use rules.
6. Protect Intellectual Property- I will request to use the software and media others produce. I will purchase, license, and register all software or use available free and open source alternatives rather than pirating software. I will purchase my music and media and refrain from distributing these in a manner that violates their licenses.

Copyright and File Sharing

Students are required to follow all copyright laws around all media including text, images, programs, music, and video. Downloading, sharing, and posting online illegally obtained media is against the Acceptable Use Policy.

Keeping Safe on Social Networks

Quick tips for teens:

- Put everything behind password protected walls that only friends can see. Protect your password and make sure you really know who someone is before you allow them onto your friends' list.
- Blur or morph your photos a bit so they won't be abused by cyber bullies or predators.
- Don't post anything your parents, principal, or a predator couldn't see. What you post online stays online - forever!!!! So ThinkB4U Click!
- Don't do or say anything online you wouldn't say offline. Protect your privacy and your friends' privacy too. Get their okay before posting something about them or their pics online.
- Check what your friends are posting/saying about you. Even if you are careful, they may not be and may be putting you at risk.
- That cute 14-year-old boy may not be cute, may not be 14, and may not be a boy! You never know! Unless you're prepared to attach your blog to your college/job/internship/scholarship/sports team application, don't post it publicly!
- Stop, Block and Tell! (Don't respond to any cyberbullying message, block the person sending it to you, and tell a trusted adult).
- R-E-S-P-E-C-T! (Use good netiquette and respect the feelings and bandwidth of others). Keep personal information private (the more information someone has about you, the more easily they can bully you).
- Google yourself! (Conduct frequent searches for your own personal information online and set alerts to spot cyberbullying early.)
- Take 5! (Walk away from the computer for 5 minutes when something upsets you so you don't do something you will later regret).

For parents:

- Talk to your kids - ask questions (and then confirm to make sure they are telling you the truth!).
- Ask to see their profile page (for the first time)…tomorrow! (It gives them a chance to remove everything that isn't appropriate or safe…and it becomes a way to teach them what not to post instead of being a "gotcha" moment! (Think of it as the loud announcement before walking downstairs to a teen party you're hosting.)
- Don't panic…there are ways of keeping your kids safe online. It's easier than you think! Be involved and work with others in your community. (Think about joining WiredSafety.org and help create a local cyber-neighborhood watch program in your community.)
- Remember what you did when you were fifteen that your parents would have objected to had they known!

- This too will pass! Most kids really do use social networks just to communicate with their friends. Take a breath, gather your thoughts, and get help when you need it. (You can reach out to WiredSafety.org.)
- It's not an invasion of their privacy if strangers can see it. There is a difference between reading their paper diary that is tucked away in their sock drawer…and reading their blog. One is between them and the paper it's written on; the other between them and 700 million people online!
- Don't believe everything you read online - especially if your teen posts it on her blog! For more information, visit www.WiredSafety.org

Authorization for Electronic Network Access

In order to educate students in the most recent uses of technology, the District has implemented a number of ways for exploring information other than that found in traditional print form. The District believes it is in the students' best interest to enhance their ability to explore as many options as possible for obtaining information. Some of these methods of exploration can lead to materials that may be contrary to one's beliefs and may be offensive in nature.

Although the District cannot guarantee students will not be able to access this type of material, the District in no way condones or encourages access to this information. In an effort to control access of these materials, the following guidelines have been developed to help control access to offensive materials that may be found through the use of technology.

1. The District expects that instruction in the proper use of technology will enhance curriculum objectives and be an integral part of the instructional program, and, therefore, teachers and administration will monitor the proper use of all technology.
2. Students utilizing online services must have the permission of and be supervised by the District professional staff.
3. Access to technology is a student privilege, and the misuse of it can be punishable as any other offense against rules of proper conduct.
4. Vandalism, damage, or disabling the property of the District or of another person is strictly forbidden.
5. To access or impersonate another person's materials, information, or files is strictly forbidden.
6. All software to be permanently installed on computers must have the prior approval of the administration who will make sure a proper license exists for its use.
7. Privately owned software cannot be permanently installed on hard drives.
8. Personnel are not to change the configuration of computers without the permission of the administration.
9. District owned software cannot be taken off the school premises without the approval of the administration.
10. District owned software may not be copied and manuals may not be reproduced unless permitted or allowed by law.

Access to Electronic Networks
Electronic networks and associated accounts, including the Internet, are a part of the District's instructional program in order to promote educational excellence by facilitating resource sharing, innovation, and communication. The School District is not responsible for any information that may be lost, damaged, or unavailable when using the network or for any information that is retrieved or transmitted via the Internet. Furthermore, the District will not be responsible for any unauthorized charges or fees resulting from access to the Internet.

Acceptable Use
All use of the District's electronic network must be: (1) in support of education and/or research and be in furtherance of the Board of Education's stated goal, or (2) for a legitimate school business purpose. Use is a privilege, not a right. Students and staff members have no expectation of privacy in any material that is stored, transmitted, or received via the District's electronic network or District computers. General rules for behavior and communications apply when using electronic networks. Electronic communications and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by school officials.

Internet Safety
Technology protection measures shall be used on each District computer with Internet access. They shall include a filtering device that protects against Internet access by both adults and minors to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee.
The Superintendent or designee shall enforce the use of such filtering devices. The Superintendent or designee shall include measures in this policy's implementation plan to address the following:
1. Ensure staff supervision of student access to online electronic networks,
2. Restrict student access to inappropriate matter as well as restricting access to harmful materials,
3. Ensure student and staff privacy, safety, and security when using electronic communications,
4. Restrict unauthorized access, including "hacking" and other unlawful activities, and
5. Restrict unauthorized disclosure, use, and dissemination of personal identification information, such as names and addresses.

Prevention of and Response to Bullying, Intimidation, and Harassment
Bullying, intimidation, and harassment diminish a student's ability to learn and a school's ability to educate. Preventing students from engaging in these disruptive

behaviors and providing all students equal access to a safe, non-hostile learning environment are important District goals.
Bullying on the basis of actual or perceived race, color, national origin, military status, unfavorable discharge status from the military service, sex, sexual orientation, gender identity, gender-related identity or expression, ancestry, age, religion, physical or mental disability, order of protection status, status of being homeless, or actual or potential marital or parental status, including pregnancy, association with a person or group with one or more of the aforementioned actual or perceived characteristics, or any other distinguishing characteristic is prohibited in each of the following situations:
1. During any school-sponsored education program or activity.
2. While in school, on school property, on school buses or other school vehicles, at designated school bus stops waiting for the school bus, or at school-sponsored or school-sanctioned events or activities.
3. Through the transmission of information from a school computer, a school computer network, or other similar electronic school equipment.
4. Through the transmission of information from a computer that is accessed at a nonschool-related location, activity, function, or program or from the use of technology or an electronic device that is not owned, leased, or used by a school district or school if the bullying causes a substantial disruption to the educational process or orderly operation of a school. This item (4) applies only in cases in which a school administrator or teacher receives a report that bullying through this means has occurred, and it does not require a district or school to staff or monitor any nonschool-related activity, function, or program.

Definitions from Section 27-23.7 of the School Code (105 ILCS 5/27-23.7)
Bullying includes cyberbullying and means any severe or pervasive physical or verbal act or conduct, including communications made in writing or electronically, directed toward a student or students that has or can be reasonably predicted to have the effect of one or more of the following:
1. Placing the student or students in reasonable fear of harm to the student's or students' person or property;
2. Causing a substantially detrimental effect on the student's or students' physical or mental health;
3. Substantially interfering with the student's or students' academic performance; or
4. Substantially interfering with the student's or students' ability to participate in or benefit from the services, activities, or privileges provided by a school.

Cyberbullying means bullying through the use of technology or any electronic communication, including without limitation any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic system, photo-electronic system, or photo-optical system, including without limitation electronic mail, Internet communications, instant messages, or facsimile communications.

Cyberbullying includes the creation of a webpage or weblog in which the creator assumes the identity of another person or the knowing impersonation of another person as the author of posted content or messages if the creation or impersonation creates any of the effects enumerated in the definition of bullying. Cyberbullying also includes the distribution by electronic means of a communication to more than one person or the posting of material on an electronic medium that may be accessed by one or more persons if the distribution or posting creates any of the effects enumerated in the definition of bullying.

School personnel means persons employed by, on contract with, or who volunteer in a school district, including without limitation school and school district administrators, teachers, school guidance counselors, school social workers, school counselors, school psychologists, school nurses, cafeteria workers, custodians, bus drivers, school resource officers, and security guards.

Bullying Prevention and Response Plan

The Superintendent or designee shall develop and maintain a bullying prevention and response plan that advances the District's goal of providing all students with a safe learning environment free of bullying and harassment. This plan must be consistent with the following requirements:

1. The District uses the definition of bullying as provided in this policy.
2. Bullying is contrary to State law and the policy of this District. However, nothing in the District's bullying prevention and response plan is intended to infringe upon any right to exercise free expression or the free exercise of religion or religiously-based views protected under the First Amendment to the U.S. Constitution or under Section 3 of Article I of the Illinois Constitution.
3. Students are encouraged to immediately report bullying. A report may be made orally or in writing to the District Complaint Manager or any staff member with whom the student is comfortable speaking. Anyone, including staff members and parents/guardians, who has information about actual or threatened bullying is encouraged to report it to the District Complaint Manager or any staff member. Anonymous reports are also accepted.