CENTRAL DISTRICT 51

Encourage Excellence Everyday
with Compassion, Commitment, and Community

TECHNOLOGY
HANDBOOK

2023-2024

Central District 51 Technology Handbook

Central School District 51 is committed to technology integration across the curriculum as one way to prepare 21st Century learners. To this end, Central District 51 provides a variety of technology across the district. In addition, Central 51 students in kindergarten through eighth grade have individual access to a Google Chromebook to support learning, and kindergarten through eighth grade Central students may have Chromebook access at home.

Central District 51 firmly believes that technology resources, including the use of the Internet, are of great importance in today's learning environment. In keeping with this belief, the district will continue to maintain and enhance evolving technology to meet current and future needs and provide age-appropriate technology instruction across the curriculum. The use of technology is a privilege for students, and Central 51 teachers, staff, and administration expect students to accept the responsibility that comes with the individual use of a Chromebook and the technology offered throughout the district.

In order to support the student use of Chromebooks and other technology offered throughout the district, Central District 51 recognizes the need to develop guidelines in relation to use of these resources. The following acceptable practice guidelines have been developed to protect Central District 51's investment in technology and to inform users of appropriate and responsible usage. Since access to the technology resources of Central District 51 is a privilege and not an entitlement or right, these guidelines are provided so that users are aware of the responsibilities they are about to acquire.

In order for each student to be loaned a Chromebook, students and families must read and electronically sign the attached acknowledgement via Skyward. The Technology Handbook is valid for the 2023-2024 school year. A new handbook will be provided and a new acknowledgement must be signed and returned when a student is loaned a Chromebook for the following year.

Use of the District Technology

Any and all use of Chromebooks and/or any technology resources owned by Central District 51 shall be consistent with the district's Acceptable Use of the District's Electronic Networks policies outlined in the student/parent handbook and in this document.

- All students are provided a Central District 51 Google account, including a username and password. Students must use that account when logging in to the Chromebook. This account is to be utilized only for educational purposes.
- Central District 51 takes the privacy of students' data seriously and is compliant with the Student Online Personal Protection Act (SOPPA). Students are only permitted to utilize their school login information to sign up for websites, applications, or online games that have been approved by Central District 51. In addition, the district must have a signed Data Privacy Agreement (DPA) with all website and application companies that have been approved for student use. The list of approved websites and applications is frequently updated and can be found here. Information about SOPPA and other aspects of student data protection can be found here.
- Central District 51 provides fourth through eighth grade students with a Google email account for educational use. Student use of email shall be under the supervision of a staff member and shall be consistent with the Central District 51 curriculum and educational mission. Students shall not be allowed to use the district's electronic mail communication for personal messages, anonymous messages, or communications unrelated to the school program.
- Students shall respect the privacy rights of others and not attempt to gain access to others' passwords, modify others' passwords, access any files and other data belonging to others, or misrepresent others on the network.

- Students are responsible for informing staff of any unauthorized use of their district accounts, receipt of inappropriate electronic transmissions, knowledge of copyright violations, and any other inappropriate issues involving the use of hardware or access.
- Students shall not attempt to access and/or bypass the district's network or technological resources in a way that compromises the security of the network or Chromebook.
- Unless instructed otherwise, the Chromebook is intended for use at school every day. Students in kindergarten through eighth grade will be loaned a Chromebook for use at school and at home and should plan to have the Chromebook at school every day. Extra Chromebooks may be loaned to students who forget Chromebooks but are not guaranteed. Chromebooks loaned to students must be returned before the end of the school day.
- Students are bound by the same policies, procedures, and guidelines outlined in this Technology Handbook whether using the Chromebook at home or school.
- Central District 51 filters will run on student Chromebooks outside of school. However, the district is not responsible for supervising students' use of the Chromebook and Internet activity outside of school. Parents/guardians are solely responsible for supervising the use of the device, including Internet access outside of the school.
- Central District 51 does not guarantee that Chromebooks will function outside the district at the same level as in the district. Configuration of any home network connection is the student's or family's responsibility and not the responsibility of the district. Any configuration applied to the Chromebook that impairs its performance in school may be removed by district staff.
- In some cases, the school administrator may revoke take-home privileges and require the student to "check out" a Chromebook from the library or designated school area.

Hapara

To help keep your child safer and more scholarly online, we have adopted online services provided by Hapara for kindergarten through eighth grade students. Hapara is a Chromebook Management Software that supports our Internet usage policy in the following ways:

- Safer Searching
    - Administrators, teachers, and technology personnel can easily prevent students from searching for (or seeing) harmful and/or inappropriate material.
- Activity Flagging
    - Helps our school detect potentially dangerous activity, such as self-harm or bullying.
- YouTube Filtering
    - Allows teachers and administrators greater control over which videos students see.
- Online monitoring
    - Help students stay "scholarly" and more focused when learning online
    - Help assess students' progress towards class assignments
    - Facilitate communication between teachers and students during class time
    - Schools have the option to protect and oversee student web activity both on and off campus.
    - Online monitoring doesn't just stop with the Chromebook. As long as students are logged in using their Central #51 Google account, Internet activity is tracked from any device.
- Theft Recovery
    - Helps authorized school administrators find and recover stolen Chromebooks.

Caring for the Chromebook

All Chromebooks remain the property of Central District 51 and must be maintained appropriately. Students shall care for the Chromebook as follows:

- Insert and remove cords and cables carefully to prevent damage to connectors.
- Use a clean, soft cloth to clean Chromebook. Please do not use cleansers of any type.

- Do not write or draw on, apply stickers or labels to, or otherwise mark up or deface the Chromebook.
- Handle the device carefully. Chromebook screens can be damaged not only when dropped, but also when twisted or subjected to pressure. Do not stack objects on top of the Chromebook.
- Keep all food and beverages away from the Chromebook.
- Do not leave the Chromebook in places of extreme temperature, humidity, or limited ventilation (i.e. in a car) for an extended period of time.
- Do not leave the Chromebook in an unsecured environment. Do not leave it in an unlocked locker, desk, or other location where someone else might take it.
- Each Chromebook comes with a Central District 51 identification sticker. Write this number down so that your student's Chromebook can be easily identified.
- Families are strongly encouraged to purchase a backpack with a sleeve for electronic devices or a case or sleeve for the Chromebook.

Returning the Chromebook

- The Chromebook is property of Central District 51 for the current school year the Chromebook is loaned to the student.
- For all students, Chromebooks and any related accessories must be returned to Central District 51 by the last day of the current school year unless otherwise directed.
- Upon withdrawal from Central District 51, the Chromebook must be returned along with any related accessories prior to the student's last day of attendance.
- The Chromebook and accessories must be returned in operable condition, with all parts intact and working order. If your student fails to return the Chromebook and any related accessories, the district may, in addition to seeking reimbursement from you, file a report with local law enforcement.

Chromebook Data and Software

- Work done on a Chromebook is typically saved in students' district Google Drive accounts.
- Central District 51 will provide software/apps/extensions required to use the Chromebook for school purposes. This software may not be removed. Central District 51 may add, update, and/or remove software at any time, for any reason, without prior notice. Students are not permitted to install additional software/apps/extensions on the Chromebook.
- Students are responsible for reporting any unauthorized software that they observe on the network or Chromebook. Failure to report unauthorized software may result in suspension of computer usage.
- The act of "jailbreaking," or otherwise disrupting the configuration of the Chromebook, voids the manufacturer's warranty and is a violation of this handbook. Removal of any Central District 51 installed configuration is prohibited and will be considered a violation of this handbook.
- Devices are owned in their entirety by Central District 51. All information, correspondence, and communication contained in the files that are used by students are property of Central District 51. The district reserves the right to inspect the Chromebook, school accounts, and their contents at any time and for any reason.
    - Users waive their right to privacy with respect to their files and communications and consent to access and disclosure to them by authorized Central District 51 personnel.

Repair, Loss, or Damage to Chromebook

- If a student's Chromebook becomes lost or damaged, the student or parent shall report it immediately to the Central District 51 Technology Department, the child's teacher, or building administration..
- Students and parents are responsible for cooperating with Central District 51 in the recovery, repair, or replacement of the student issued Chromebook.
- The District will repair or replace damaged equipment resulting from normal use. Payment for all other costs related to damage and breakages will be the responsibility of the student. Central will make its best

attempt to purchase replacement parts at the best possible price. Loss or theft of the device is also the student's responsibility and will result in the student being charged the full replacement cost to purchase a new device.

- The repair/replacement cost will be as follows:

  Chromebook Replacement - $180
  Chromebook Screen Repair/Replacement - $55
  Chromebook Keyboard Repair/Replacement - $45
  Chromebook Charger Replacement - $20

Acceptable Use of the District's Electronic Networks

This Acceptable Use of the District's Electronic Networks section is included in the 2022-2023 Central Primary School and Central Intermediate School Student/ Parent Handbooks. Student/Parent handbooks are signed upon school registration.

All use of the District's *electronic networks* shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. These procedures do not attempt to state all required or prohibited behavior by users. However, some specific examples are provided. The failure of any user to follow these procedures will result in the loss of privileges, disciplinary action, and/or legal action.

Terms and Conditions

The term *electronic networks* includes all of the District's technology resources, including, but not limited to:

1. The District's local-area and wide-area networks, including wireless networks (Wi-Fi), District-provided Wi-Fi hotspots, and any District servers or other networking infrastructure;
2. Access to the Internet or other online resources via the District's networking infrastructure or to any District-issued online account from any computer or device, regardless of location;
3. District-owned and District-issued computers, laptops, tablets, phones, or similar devices.

Acceptable Use – Access to the District's electronic networks must be: (a) for the purpose of education or research, and be consistent with the District's educational objectives, or (b) for legitimate business use.

Privileges – Use of the District's electronic networks is a privilege, not a right, and inappropriate use may result in a cancellation of those privileges, disciplinary action, and/or appropriate legal action. The system administrator or Building Principal will make all decisions regarding whether or not a user has violated these procedures and may deny, revoke, or suspend access at any time. His or her decision is final.

Unacceptable Use – The user is responsible for his or her actions and activities involving the electronic networks. Some examples of unacceptable uses are:

1. Using the electronic networks for any illegal activity, including violation of copyright or other intellectual property rights or contracts, or transmitting any material in violation of any State or federal law;
2. Using the electronic networks to engage in conduct prohibited by board policy;
3. Unauthorized downloading of software or other files, regardless of whether it is copyrighted or scanned for malware;
4. Unauthorized use of personal removable media devices (such as flash or thumb drives);
5. Downloading of copyrighted material for other than personal use;
6. Using the electronic networks for private financial or commercial gain;
7. Wastefully using resources, such as file space;
8. Hacking or attempting to hack or gain unauthorized access to files, accounts, resources, or entities by any means;
9. Invading the privacy of individuals, including the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature, such as a photograph or video;
10. Using another user's account or password;

11. Disclosing any network or account password (including your own) to any other person, unless requested by the system administrator;
12. Posting or sending material authored or created by another without his/her consent;
13. Posting or sending anonymous messages;
14. Creating or forwarding chain letters, spam, or other unsolicited messages;
15. Using the electronic networks for commercial or private advertising;
16. Accessing, sending, posting, publishing, or displaying any abusive, obscene, profane, sexual, threatening, harassing, illegal, or knowingly false material;
17. Misrepresenting the user's identity or the identity of others; and
18. Using the electronic networks while access privileges are suspended or revoked.

Network Etiquette – The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

1. Be polite. Do not become abusive in messages to others.
2. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
3. Do not reveal personal information, including the addresses or telephone numbers, of students or colleagues.
4. Recognize that the District's electronic networks are not private. People who operate District technology have access to all email and other data. Messages or other evidence relating to or in support of illegal activities may be reported to the authorities.
5. Do not use the networks in any way that would disrupt its use by other users.
6. Consider all communications and information accessible via the electronic networks to be private property.

No Warranties – The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Indemnification – By using the District's electronic networks, the user agrees to indemnify the District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any violation of these procedures.

Security – Network security is a high priority. If the user can identify or suspects a security problem on the network, the user must promptly notify the system administrator or Building Principal. Do not demonstrate the problem to other users. Keep user account(s) and password(s) confidential. Do not use another individual's account without written permission from that individual. Attempts to log-on to the network as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the networks.

Vandalism – Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of malware, such as viruses and spyware.

Telephone Charges – The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, texting or data use charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.

Copyright Web Publishing Rules – Copyright law and District policy prohibit the re-publishing of text or graphics found on the Internet or on District websites or file servers/cloud storage without explicit written permission.

1. For each re-publication (on a website or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the web address of the original source.
2. Students engaged in producing web pages must provide library media specialists with email or hard copy permissions before the web pages are published. Printed evidence of the status of *public domain* documents must be provided.

3. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the website displaying the material may not be considered a source of permission.
4. The *fair use* rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.
5. Student work may only be published if there is written permission from both the parent/guardian and student.

Use of Email – The District's email system, and its constituent software, hardware, and data files, are owned and controlled by the District. The District provides email to aid students in fulfilling their duties and responsibilities, and as an education tool.

1. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student to an email account is strictly prohibited.
2. Each person should use the same degree of care in drafting an email message as would be put into a written memorandum or document. Nothing should be transmitted in an email message that would be inappropriate in a letter or memorandum.
3. Electronic messages transmitted via the District's Internet gateway carry with them an identification of the user's Internet *domain*. This domain is a registered name and identifies the author as being with the District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of the District. Users will be held personally responsible for the content of any and all email messages transmitted to external recipients.
4. Any message received from an unknown sender via the Internet, such as spam or potential phishing emails, should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.
5. Use of the District's email system constitutes consent to these regulations.

Internet Safety

Internet access is limited to only those *acceptable uses* as detailed in these procedures. Internet safety is supported if users will not engage in *unacceptable uses*, as detailed in these procedures, and otherwise follow these procedures.

Staff members will supervise students while students are using District Internet access to ensure that the students abide by the *Terms and Conditions* for Internet access contained in these procedures.

Each District computer with Internet access has a filtering device that blocks entry 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 system administrator and Building Principals shall monitor student Internet access.

Student Authorization for Access to the District's Electronic Networks

Our School District has the ability to enhance your child's education through the use of electronic networks, including the Internet. Our goal in providing this service is to promote educational excellence by facilitating resource sharing, innovation, and communication. Students and their parents/guardians need only sign this *Authorization for Access to the District's Electronic Networks* once while the student is enrolled in the School District.

The District *filters* access to materials that may be defamatory, inaccurate, offensive, or otherwise inappropriate in the school setting. If a filter has been disabled or malfunctions it is impossible to control all material and a user may discover inappropriate material. Ultimately, parents/guardians are responsible for setting and conveying the standards that their child should follow, and the School District respects each family's right to decide whether or not to authorize Internet access.

With this educational opportunity also comes responsibility. The use of inappropriate material or language, or violation of copyright laws, may result in the loss of the privilege to use this resource. Remember that you are legally responsible for your child's actions. If you agree to allow your child to have a network account, sign the *Authorization* form below and return it to your school.

Upon school registration, students must have a parent/guardian read and agree to the following before being granted unsupervised access:

All use of the electronic networks shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. **The failure of any user to follow the terms of the *Acceptable Use of the District's Electronic Networks* will result in the loss of privileges, disciplinary action, and/or appropriate legal action.** The signatures at the end of this document are legally binding and indicate the parties who signed have read the terms and conditions carefully and understand their significance.

I have read this *Authorization* form. I understand that access is designed for educational purposes and that the District has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the District to restrict access to all controversial and inappropriate materials. I will hold harmless the District, its employees, agents, or Board members, for any harm caused by materials or software obtained via the network. I accept full responsibility for supervision if and when my child's use is not in a school setting. I have discussed the *Acceptable Use of the District's Electronic Networks* with my child. I hereby request that my child be allowed access to the District's electronic networks, including the Internet.

Upon school registration, students must also read and agree to the following before being granted unsupervised access:

I understand and will abide by the above *Acceptable Use of the District's Electronic Networks*. I understand that the District and/or its agents may access and monitor my use of the District's electronic networks, including the Internet, 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 legal action may be taken. In consideration for using the District's electronic network connection and having access to public networks, I hereby release the School District and its Board members, employees, and agents from any claims and damages arising from my use of, or inability to use the District's electronic networks, including the Internet.

Central District 51 Technology Agreement

The following must be completed and signed in order for students to utilize district technology.

- ❏ I have read and understand my role and responsibilities as a student/parent as outlined in this Technology Handbook.
- ❏ I acknowledge that my child's Chromebook and any other district technology must be returned in good working order consistent with the guidelines outlined in this handbook.
- ❏ I understand that if any district technology, owned and managed through Central District 51, is not used according to the district's Internet Acceptable Use policy and the policies outlined in this handbook, disciplinary action may result.
- ❏ To the fullest extent allowed by law, you agree to indemnify, defend, and hold harmless Central District 51, its Board of Education, and its individual Board members, officers, employees, and agents from any and all claims, damages, losses, causes of action, and the like relating to, connected with, or arising from the use of any Central District 51 Chromebook issued to your student.
- ❏ By signing the Handbook, you waive any and all claims you or your student (and each of your respective heirs, successors, and assigns) may have against Central District 51, its Board of Education, and its individual Board members, officers, employees, and agents relating to, connected with, or arising from the use of the Chromebook or this Handbook.

Student/Parent Signature: Date: