KEENEYVILLE SCHOOL DISTRICT 20

Parent/Student Technology Handbook & Acceptable Use Agreement

2024-2025 School Year

TABLE OF CONTENTS

KEENEYVILLE DISTRICT 20 TECHNOLOGY HANDBOOK

Use of Technology

School Board Policy 6:235

All information relating to the use of technology is contained in this document, the **PARENT/STUDENT TECHNOLOGY HANDBOOK AND ACCEPTABLE USE AGREEMENT**, which will be distributed to families at the beginning of each school year.

All kindergarten through 8th grade students will have access to Google Chromebooks for educational use in school. All students will take their devices home. This document provides students and their parents/guardians with information about the general use of technology, ownership of the devices, rights and responsibilities for possession of the device, educational use, and care of the Chromebook.

Parents/Guardians and students must sign the last page of this document, the PARENT/STUDENT TECHNOLOGY AND ACCEPTABLE USE AGREEMENT—SIGNATURE FORM. This form must be signed before a Chromebook is distributed to your student.

Students and their parents/guardians are reminded that using district technology is a privilege, not a right. District authorities may monitor everything on any district-owned computer, network, or electronic communication device. Inappropriate use of district technology can result in disciplinary consequences, limited use, or legal action, as stated in **DISTRICT 20'S PARENT/STUDENT HANDBOOK**.

Curriculum

Internet use shall be consistent with the district's curriculum and the students' varied instructional needs, learning styles, abilities, and developmental levels. The Internet is part of the curriculum and is not a public forum for general use.

Use of Generative Artificial Intelligence (AI) Technology

The use of generative artificial intelligence (AI) technology as a substitute for original student work will be considered plagiarism and subject to consequences outlined in the Academic Dishonesty section of the **PARENT/STUDENT HANDBOOK**. Teachers may assign students to use these tools at their discretion for certain acceptable purposes.

Ownership of the Chromebook

Keeneyville District 20 retains the sole right of possession of the Chromebook. Keeneyville District 20 lends the Chromebook to the students for educational purposes only for the academic year. Additionally, Keeneyville District 20 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. Keeneyville District 20 can monitor, view and report on internet activity on the device.

Returning Your Chromebook

End of Year

Students must turn in their Chromebooks and power cords at the end of the school year. Failure to turn in the Chromebook and power cord will result in the student being charged for the total replacement cost of the Chromebook and power cord. The district may also file a stolen property report with the local law enforcement agency. **Failure to return the Chromebook and power**

cord with the serial and asset tags will result in a charge of $15.00 up to the total replacement value.

Transferring/Withdrawing Students

Students who transfer out of or withdraw from the district must turn in their Chromebook and power cord to their school's main office on their last day of attendance. Failure to turn in the Chromebook and power cord will result in the student being charged the total replacement cost of the Chromebook and power cord. The district may also file a stolen property report with the local law enforcement agency.

Responsibility for Electronic Data

Users of district 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. There are 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 ChromeOS that the school supports and manages. The Chromebook operating system, ChromeOS, updates itself automatically. Students do not need to update their Chromebooks manually.

Chromebooks use the principle of "defense in depth" to provide multiple layers of protection against viruses and malware, including data encryption and verified boot. **There is no need for additional virus protection.**

Content Filter

The school utilizes an Internet content filter in compliance with the federally mandated Children's Internet Protection Act (CIPA). The school will protect and monitor all internet activity on all Chromebooks while on campus.

Parents/guardians are responsible for filtering and monitoring any internet connection students receive that is not provided by the school.

Student Data Privacy

District 20 partners with various education technology companies ("ed tech vendors") to provide services supporting your child's education, such as digital curriculum, educational resources, and analytical tools. District 20 is committed to protecting our students' information security and privacy.

District 20 is required by the Student Online Personal Protection Act (SOPPA) to enter into a written agreement with any ed tech vendor that operates a website, online service, online application, or mobile application that is designed, marketed, and used primarily for kindergarten through 12th grade purposes. The agreement defines how the vendor may and may not use student data, identifies what data the vendor collects, and describes the processes that should occur during a data breach. District 20 will only partner with vendors that are compliant with applicable laws and guidelines.

Current data privacy agreements and data elements shared between District 20 and compliant, approved ed tech vendors can be viewed on the district website. Parents will be notified within thirty (30) days of a data breach affecting more than 10% of the students.

Not all approved online resources will be used by all students at all grade levels, and directory information is only shared with an approved vendor when utilized by the student or classroom. The district will only provide the minimum amount of data required to maintain service functionally for each vendor. District 20 will only sell, rent, lease, or trade student data or share student data with external entities with a signed agreement.

SOPPA defines parents' and guardians' rights regarding their students' data, which can be viewed on the district website at https://www.esd20.org/district/technology/student-data-and-privacy/parent-rights.

Chromebook Information

Inventory

The school will maintain an inventory of all Chromebooks. This inventory will include the Chromebook serial number, asset tag code, student name, and student ID number assigned to the device. Asset tags may not be tampered with, and students may receive disciplinary action for tampering with a tag.

Each student will be assigned the same Chromebook for the life cycle of the device. New devices will only be issued by the device renewal cycle established by Keeneyville District 20.

Chromebook Use Student Expectations

No Expectation of Privacy

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

- There is no expectation of privacy when using the district's network, equipment, e-mail system, or the Internet. The district may monitor all communications and documents stored on or sent from its network.

- The district employs a safety management solution that uses a combination of artificial intelligence and trained safety experts to provide real-time analysis and review of students' use of online tools. It constantly scans accounts for harmful content and alerts school officials when students show signs of self-harm, depression, thoughts of suicide, substance abuse, cyberbullying, credible threats of violence against others, or other harmful situations.

Social Networking Websites

- School officials may not request or require a student or their parent/guardian to provide a password or other related account information to gain access to the student's account or profile on a social networking website.

- School officials may conduct an investigation or require a student to cooperate in an investigation if there is specific information about activity in the student's account on a social networking website that violates a school disciplinary rule or policy. During an investigation, the student may be required to share the reported content to allow school officials to make a factual determination.

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 a violation of this agreement and will be treated as a discipline issue at the administration's discretion.

Background 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. This will be treated as a discipline issue at the administration's discretion.

Sound

- Sound must always be muted unless permission is obtained from a teacher.
- Headphones may be used only if the instructional software has an audio component. For sanitary reasons, students will be given their own personal set of headphones.

Printing

- Students are encouraged to digitally publish and share their work with their teachers and peers when appropriate.
- Students will have a limited ability to print. The teacher must approve all printing. Failure to comply with this policy will result in disciplinary action at the administration's discretion.

Logging into a Chromebook

- Grades 3-8 students will log into their Chromebooks using their school-issued Google account. K-2 Students will use a "Clever" badge to log into their Chromebooks.
- Students should only share their account passwords with others if an administrator requests.

Managing and Saving Your Digital Work

- Most student work will be stored in internet/cloud-based applications and accessed from any computer with an internet connection and most mobile internet devices.
- Students should always remember to save frequently when working on digital media.
- The school will not be responsible for the loss of any student work.

Using Your Chromebook Outside of School

- Students are encouraged to use their Chromebooks at home and other locations outside of school.

- A Wi-Fi internet connection will be required for all Chromebook use.

- Students are bound by the **DISTRICT 20 ACCEPTABLE USE POLICY** and all other guidelines in this document wherever they use their Chromebooks.

Chromebook Care

- 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 and/or your building administrators as soon as possible.

- District-owned Chromebooks should **never** be taken to an outside computer service for repairs or maintenance.

- Students should never leave their Chromebooks unattended except locked in their hallway locker.

- No food or drink should be next to Chromebooks.

- Cords, cables, and removable storage devices must be inserted carefully into Chromebooks.

- Chromebooks must remain free of any writing, drawing, stickers, and labels other than those placed by the district. Students may be charged for these types of damages.

- Heavy objects should never be placed on top of Chromebooks.

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, or disks).

- Clean the screen with a soft, dry microfiber or anti-static cloth.

Storing During Extracurricular Activities

- Students are responsible for securely storing their Chromebooks during extracurricular events.

Copyright and File Sharing

- Students must follow all copyright laws regarding all media, including text, images, programs, music, and video. Downloading, sharing, and posting illegally obtained media

online is against **Access to Electronic Networks Policy 6:235**.

Technology Fee and Repairs

Annual Technology Fee

Each student must pay an annual $50 Technology Fee. This fee covers one repair per year: a repair is considered one thing broken on a device. For example, Lisa turned in her device to have it fixed. However, Lisa's device has a cracked screen, a missing "D" key on the keyboard, and a broken camera. Although she has only turned the device in once for repair, these are three separate repairs. The technology fee covers the most expensive repair, and the other fees are charged to the student. **Repairs can cost anywhere between $50 and total replacement costs.**

Loaner Chromebooks

Students may be issued loaner Chromebooks when they leave their Chromebooks for repair. A student borrowing a Chromebook must sign a loaner agreement and is responsible for any damage to or loss of the loaned device. **A student will only be issued one loaner device.**

Replacement Charges

If a device cannot be repaired, the student will be charged a replacement cost. If fixing the device is more expensive than replacing it, the student will be charged the total placement cost. The cost of the Chromebook can be anywhere between **$400-$500**.

Lost Chromebooks and Power Cords

Students are responsible for lost Chromebooks. The technology fee does not cover a lost Chromebook and is subject to total replacement costs.

A lost power cord is also not covered by the technology fee and is subject to total replacement cost.

KEENEYVILLE DISTRICT 20 ACCEPTABLE USE POLICY (AUP)
Access to Electronic Networks Policy 6:235

All use of the networked system and internet shall be consistent with the district's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. This Agreement does not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. ***The failure of any user to follow the terms of the policy, administrative procedures, and appropriate Agreements may result in the loss of privileges, disciplinary action, and/or appropriate legal action.*** The signature(s) at the end of this document is legally binding and indicates the party who signed has read the terms and conditions carefully and understands their significance.

Terms and Conditions

Acceptable Use

All use of the district's connection to the networked system and the internet must be in support of education and/or research, be consistent with the educational objectives, policies, rules, and regulations of the Board of Education, and be in compliance with and subject to district and building discipline codes.

Privileges

Using the district's networked system and internet connection is a privilege, not a right, and

inappropriate use will result in a cancellation of those privileges. The system administrator will make all decisions regarding whether or not a user has committed a violation and may deny, revoke, or suspend access at any time; their decision is final. Violating the codes of conduct or professional requirements may result in losing privileges and employee or student discipline. Due Process will be given commensurate with the seriousness of the offense.

Unacceptable Use

The user is responsible for the user's actions and activities involving the network. Some examples of unacceptable uses are given below. The list is not intended to be exhaustive. The administration may periodically revise the concepts of acceptable and unacceptable use. These revisions will become part of this document.

a) 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;

b) Using the electronic networks to engage in conduct prohibited by board policy;

c) Unauthorized downloading of software or other files, regardless of whether it is copyrighted or scanned for malware;

d) Unauthorized use of personal removable media devices (such as flash or thumb drives);

e) Downloading of copyrighted material for other than personal use;

f) Using the electronic networks for private financial or commercial gain;

g) Wastefully using resources, such as file space;

h) Hacking or attempting to hack or gain unauthorized access to files, accounts, resources, or entities by any means;

i) 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;

j) Using another user’s account or password;

k) Disclosing any network or account password (including your own) to any other person, unless requested by the system administrator;

l) Posting or sending material authored or created by another without their consent;

m) Posting or sending anonymous messages;

n) Creating or forwarding chain letters, spam, or other unsolicited messages;

o) Using the electronic networks for commercial or private advertising;

p) Accessing, sending, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexual, threatening, racially offensive, harassing, illegal, or knowingly false material;

q) Misrepresenting the user’s identity or the identity of others; and

r) Using the electronic networks while access privileges are suspended or revoked.

s) Promoting or encouraging the use of illegal or controlled substances;

t) Forgery or alteration of e-mail;

u) Unauthorized use of the network to play computer games, enroll in list serves, or participate in chat rooms.

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:

a) Be polite. Do not become abusive in your messages to others.

b) Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.

c) Do not reveal the personal addresses or telephone numbers of students or colleagues.

d) Recognize that electronic mail (e-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.

e) Do not use the network in any way that would disrupt its use by other users.

f) Consider all communications and information accessible via the network 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-delivery, missed deliveries, or service interruptions caused by 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

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 the cancellation of user privileges. Any user identified as a security risk may be denied network access.

Vandalism

Vandalism will result in the cancellation of privileges and other disciplinary actions. Vandalism is

defined as any malicious attempt to harm or destroy the 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 re-publishing text or graphics found on the Internet, District websites, or file servers/cloud storage without explicit written permission.

a) For each re-publication (on a website or file server) of a graphic or text file produced externally, a notice at the bottom of the page must credit the original producer and note how and when permission was granted. If possible, the notice should also include the web address of the original source.

b) 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.

c) 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 website manager displaying the material may not be considered a source of permission.

d) The fair use rules governing classroom student reports are less stringent and permit limited use of graphics and text.

e) Student work may only be published if there is written permission from both the parent/guardian and the student.

Use of Email

The district owns and controls the District's email system and its constituent software, hardware, and data files. The District provides email to aid students in fulfilling their duties and responsibilities and as an educational tool.

a) 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.

b) 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.

c) Electronic messages transmitted via the District's Internet gateway carry an identification of the user's Internet domain. This domain is registered and identifies the author as being with the District. Therefore, great care should be taken 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 email messages transmitted to external recipients.

d) 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 sure of that message's authenticity and the nature of the file so transmitted.

e) Use of the District's email system constitutes consent to these regulations.

Parent/Guardian Agreement Required

Each parent/guardian must sign **DISTRICT 20'S TECHNOLOGY ACCESS PERMISSION FORM** (included in the registration documents) as a condition for their student to access networked resources and use a live internet connection.

Each student or parent(s)/guardian(s) must also sign the last page of this document, the **PARENT/STUDENT TECHNOLOGY AND ACCEPTABLE USE AGREEMENT – *SIGNATURE FORM***.

Violations of the Acceptable Use Policy (AUP)

A student found to be in violation of the AUP will be subject to the school discipline policy found in the **PARENT/STUDENT HANDBOOK**.

Procedures for Consequences

- Teachers will make a referral for the misused Chromebook and will contact the school principal to verify and confirm the case.
- Once Chromebook misuse is confirmed, the principal will contact the student and determine the consequences. The school may keep the Chromebook for the necessary time (for repair or confiscation).

PARENT/STUDENT TECHNOLOGY AGREEMENT & ACCEPTABLE USE AGREEMENT – *SIGNATURE FORM*

Student Information (please print): _____ _____
Last Name *First Name*

Parent Information (please print): _____ _____
Last Name *First Name*

TECHNOLOGY AND ACCEPTABLE USE AGREEMENT
Access to Electronic Networks Policy 6:235

Student Agreement

Rules and regulations are necessary to offer technology opportunities to the students. To use technology resources, I agree to abide by the Keeneyville School District 20 Acceptable Use of District's Electronic Networks Policy 6:235.

_____ _____
Student Signature *Date*

Parent/Guardian Agreement

In consideration of the privileges and opportunities afforded by the use of the Keeneyville School District 20 technology and computer resources, I hereby release Keeneyville School District 20 and its agents from any and all claims of any nature arising from my student's use or inability to use Keeneyville School District 20 technology and computer resources.

_____ _____
Parent/Guardian Signature *Date*

I confirm that my student will be provided with the following:

- ❑ Chromebook with a value of approximately $450.
- ❑ Chromebook charging cord with a value of $50. I agree to replace this cord if it is lost or damaged.
- ❑ Chromebook case with a value of $30. I agree to replace this case if it is lost or damaged. (Elementary only)

_____ _____
Parent/Guardian Signature *Date*