STUDENT/PARENT HANDBOOK

Cashmere School District 2018/2019

Cashmere School District

Parent/Student Handbook for 1:1 Technology Integration

Table of Contents

Page

Vision 1

Student/Parents Rights and Responsibilities 1

Student Computers – Checkout 1

Student Responsibilities
- Students Will 2
- Network Resources 3
- Access and Monitoring 3
- Digital Citizenship 3
- Classroom Expectations 4
- Loss or Theft of Computer 4
- Ear Buds/Headphones 4
- Printer Use 4

Computer Use, Care, and Classroom Routines
- Care of Computer at Home 4
- Traveling To and From School 4
- Cleaning the Computer 5
- Classroom Use 5
- Hallways & Cafeteria 5
- Lockers 5
- Email 5
- Web Cams 5
- Music 5
- Gaming 6
- Prohibited Actions 6

Internet Safety for Students 7-9

Parent/Student Handbook for 1:1 Technology Integration

Cashmere School District

Vision: The 1:1 laptop initiative provides all students with the tools necessary to be successful consumers, producers, and creators of new information in a 21st century classroom. The goal of this initiative is to provide students in grades 3rd to 12th in the Cashmere School District daily access to a computer to enhance and extend learning opportunities inside, as well as outside the classroom.

Cashmere School District is committed to integrating technology in the classroom to:

- Promote student engagement and enthusiasm for learning.
- Encourage collaboration among students, teachers, parents, community members, and people throughout the nation through interactive networking and collaboration opportunities.
- Reduce the use of printed worksheets and workbooks.
- Guide students in their learning and production of knowledge.
- Allow students access to information, along with the opportunity to connect it to their learning in a meaningful manner.

Student/Parent Rights and Responsibilities

At the beginning of the year each student and parent signed a technology agreement (Contained in this booklet) stating that they would follow Cashmere School District's policies and procedures regarding any technology used at school or is checked out at school to be used at home.

By signing this technology agreement, students and parents agreed to use all School District equipment in a safe and ethical manner. The equipment subject to this agreement includes:

All computer and electronic devices used at school (Desktop Machines, Laptops, iPads, iPods, flash drives, headphones, and other accessories)

Student Computers - Checkout

Each student enrolled in 3rd thru 12th Grade will be issued a device within the first week of the school year.
Students who have not returned a signed technology agreement **will not** be issued a device.

Cashmere School District retains the right of possession of each device and grants the

student permission to use the device according to the guidelines in our District Technology Agreement. All student machines have been imaged with the same software, network privileges and configurations by the District's technology team. **Students are not allowed to download or make any modifications to their device**. Any new programs that needs to be installed or upgraded on student machines must be approved by the district curriculum team and installed by our technology department.

Students must return the device at the end of the school year. The District will perform annual maintenance to ensure optimal performance. Any stored data will be erased from the machine. Students are responsible (financially) for any damage to the device that may have occurred throughout the school year but had not been previously reported. Students will pay a $10 maintenance fee at the beginning of the school year (sliding fee scale).

The following are costs for repairs to the Chromebook:

1. Full replacement of Chromebook = $250.00
2. Screen = $55.00
3. Hard Drive = $35.00
4. Motherboard = $180.00
5. Keyboard/Touchpad = $25.00
6. Front Cover= $10.00
7. Back Cover = $5.00
8. Screen Bezel = $5.00
9. Webcam = $10.00
10. Power Cable = $15.00
11. Battery = $35.00
12. Case = $10.00
13. Screen Connector Cable = $5.00

Student Responsibilities

The primary goal of Cashmere School District's 1:1 Initiative is to provide all students with equal access/opportunities to learn new information and enrich learning experiences in and outside the classroom. While technology can provide new and exciting learning experiences for all students, it is important that students understand their responsibilities and use all technology in a safe and ethical manner in order to maintain the privilege of using the computer and/or other electronic devices in the District.

To ensure a full understanding of student rights and responsibilities parents/students need to know:

The following information outlines how students will use technology in a safe and ethical manner (as outlined in the technology agreements), as well as information on behaviors that would be considered unacceptable and in violation of our technology agreement.

Network resources include all aspects of the District's technology equipment- including computer, printers, scanners, and other peripherals, as well as, e-mail, Internet services, servers, network files and folders, and all other technology-related equipment and services.

- *These rules apply to the use of the District's network resources while on or off campus.*

Students will:

- Only access the system for educational purposes during school hours (this includes the use of cameras, videos, and printers in the building).
- Create files, projects, videos, webpages, podcasts, and other activities using electronic resources that are directly related to classroom content and curriculum, or as directed by a teacher/administrator.
- Use proper etiquette and codes of conduct in electronic communication. All communications via electronic resources should be assumed to be public record.
- Keep passwords and personal information private and only access their authorized account.
- Observe and respect license and copyright agreements.
- Return the device to the school at the end of the school year, or at any time they withdraw from the District.

Students may not use network resources:

- To create, send, share, access or download material which is abusive, hateful, threatening, harassing or sexually explicit. Electronic communication (from school or home) that is identified as cyberbullying is illegal, and will be dealt with by the building and/or district administration.
- To download, stream or listen to Internet based music, video, and large image files that are not for school work, as this slows the performance of the network for all users. The District's technology department will monitor the network for violations.
- To give out personal information including home address and/or telephone number.
- To access the data or account of another user.
- To download, copy, duplicate, or distribute copyrighted materials without specific written permission of the copyright owner.
- To video staff or other students without their consent or knowledge. This includes:
    - Video recording
    - Webcams
    - Cameras
    - Cell phones
    - Or any other digital device
- To attempt to defeat or bypass the District Internet filters that are in place to block inappropriate content, or to conceal inappropriate activity.
- To use any electronic resources for unlawful purposes.

Student Access and Monitoring:

- The computer is the property of the school, and the school has the right to search the computer at any time.
- The District's filter allows the district to block websites which are inappropriate for students while on school district property. When not at school, students can access the Internet if they have Internet access available to them in their home or other locations. **The school's filter will apply to locations outside of the school district**; nevertheless, it is important for parents/guardians to monitor internet activity at home.
- Students who access inappropriate sites during the school day or are accessing sites that are not related to the class they are in will face disciplinary action from the teacher and/or administration.
- If sites are accessed by accident (which does occur at times) it is recommended that the student immediately move to another site, and report the incident to an adult.

Digital Citizenship will be taught in class in the Cashmere School District. Within this curriculum students will be educated on acceptable standards of online behavior. While we do our best to provide filters on our system to ensure the safety of our students it is important that parents and teachers work together to continue the conversation of how students can stay safe using online resources in an ethical manner.

Student Expectations in the Classroom

- Students will be required to take their computer to class each day.
- It is the student's responsibility to charge their computers at home each night and bring their devices fully charged each morning. Teachers will design many of their lessons and classroom activities based on students having access to their computer. If a student does not have their computer and/or it is not charged, they will still be required to participate in the day's activity with alternative tools/materials.

Loss or Theft of Computer

- Computers that are lost or stolen need to be reported to the office immediately.
- If a computer is lost, stolen, or vandalized while not at a Cashmere School District sponsored event, the parent/district shall file a police report.
- If it is determined that the loss or damage is due to student negligence, the student and/or parent is financially responsible for the replacement of the device.

Ear Buds/Headphones

- The use of ear buds and/or headphone in class and/or during study times are at the teacher/supervisor's discretion.
- Ear buds **will not** be provided by Cashmere School District.

Student Printer Use

- Students will have access to printers in the school, but will need to have teacher/supervisor permission before printing.
- Students are only allowed to print one copy of any document unless given permission by their teacher/supervisor.
- Anything that is printed from the student computers will be directly related to teaching and learning.

Computer Use, Care, and Classroom Routines

Care of Computer at Home

- Charge the computer fully each night.
- Store the computer on a desk or table – never leave on the floor.
- Follow rules and procedures for internet usage as set up by your household.
- Protect the computer from damage such as:
  - Extreme heat or cold
  - Food and drinks
  - Small Children
  - Pets
  - Water (rain, inclement weather)

Traveling To and From School

- Completely shut down the computer before traveling.
- Do not leave the computer in a vehicle. If you have to leave your backpack in a car for an extended period of time, storage should be in a locked trunk where it will not be subject to extreme hot or cold.
- Use your backpack for transport.
- Computers can be used on school buses. Students are expected to comply with the Cashmere School District Technology Agreement signed at the beginning of the year. No cameras (still or video) can be used during this time.

Cleaning the computer

- Use a soft, dry, lint free cloth when cleaning the computer. Never use cleaning products containing acetone or ammonia.

Classroom Use

- Keep the computer on the center of your desk (not in your lap).
- Close the lid of the computer before standing up or moving the device.
- Always use two hands when carrying or transport the device.
- Shut down the computer or put it to sleep before walking away from it (this will prevent other students from accessing your documents/files in your absence).
- Follow all directions given by the teacher.

Hallways & Cafeteria

- Keep your computer in your backpack when moving to different classes.
- Never leave your computer unattended for any reason.
- Computers will need to be stored in student backpacks and a safe place during the lunch period.

Lockers (If available)

- Computers should be stored upright.
- Never pile things on top of the device.
- Always lock computers in your PE locker during PE and/or after school sports.
- Never leave it on the bottom of your locker.
- Be sure to lock your locker before leaving your device.

E-Mail

- E-mail is to be used for educational purposes only during school hours. The use of email for non-educational purposes by any student during school hours may result in a disciplinary referral that will be referred to school administration.

Web Cams

- Each computer is equipped with a camera that has the capability of capturing still images and video. These cameras are to be used for educational purposes only, under the direction of the teacher. If a student is caught using these applications inappropriately discipline action may be enforced by the administration.

Listening to Music

- At School: Listening to music on your computer is not allowed during school hours without permission from the teacher. Permission will be given only for media used to complete a school assignment.
- At Home: Listening to music on your computer is allowed at home with permission from parents/guardians.

Gaming

- At School: Online gaming is not allowed during school hours unless you have been given access and permission by a teacher. Any games must be in support of the curriculum.

- At Home: Students are not allowed to download any material on their computer. Online gaming is subject to household rules and policies.

Prohibited Actions

Students are prohibited from:

- Putting stickers or additional marking on the computers, cases, batteries, or power cord/chargers.

- Removing or interfering with any identification placed on the computer.

Internet Safety for Children

The Internet is a wonderful place to find information and connect with people and friends. It does pose safety and privacy risks, though, especially to minors.

What you can do to protect your children online:

- Talk about Internet safety as soon as they begin using the Internet. It is never too early.
- Consider placing the computer in a common area of the house.
- Stay involved in their online world by monitoring with whom they email and chat. Get to know the websites they're visiting.
- Know their usernames and screen names and make sure they are appropriate.
- Use safe search engines. For younger kids in particular, use age-appropriate filtering and monitoring software.
- Educate yourself about computers, the Internet and potential risks to children online.

What your children should not do:

- Tell your child to never share their passwords with anyone, including friends.
- Teach them not to fill out forms without your knowledge, or open emails from strangers.
- Do not allow your child to go into private chat rooms.

Social Networking

Social networks have become very popular among adults and children alike. These sites allow users to communicate and share information. They can be accessed anywhere there is an Internet connection, including on smartphones.

The basics on some popular social networks:

- **Facebook** is a free social networking site used by people all over the world. Its policy requires users to be at least 13 years old, but many younger kids join by pretending to be older. By default, adults' posts are public; kids' posts can be seen by friends of their friends.
- **Twitter** is a real-time information network where people get the latest news, ideas, and opinions about what interests them. There's no age limit. Tweets are public by default.
- **LinkedIn** is a social site that allows professionals to network with business connections, search for jobs and hiring managers, join groups, etc. Users need to be at least 18 years old. LinkedIn users have a private and a public profile, the visibility of which they can control.
- **YouTube** is a free video sharing site and social network. Anybody can upload, watch and share videos on YouTube.
- **Snapchat** is a photo messaging application developed by Stanford University students. Using the app, users can take photos, record videos, add text and drawings, and send them to a list of recipients. These sent photographs and videos are known as "Snaps".
- **Instagram** is an online photo-sharing, video-sharing and social networking service that enables its users to take pictures and videos, apply digital filters to them, and share them on a variety of social networking services, such as Facebook, Twitter, Tumblr and Flickr.
- If your child wants to use social networks, talk to them about your expectations: how they should behave; what is safe and what isn't;

when they can go to the site and how much time they can spend there (yes, social networks can be addictive).

How to protect your children's privacy and reputation:

- Go through Facebook's privacy settings together and select levels you're both comfortable with. Encourage your children to require their approval before they can be tagged in posts (one of Facebook's privacy settings). Set Tweets to be protected (private) by default.
- Teach them to never post personal information such as addresses, phone numbers, or where they are. The same goes for their friends' information.
- Discourage the use of webcams. Tell them to never send any image or video to a stranger.
- Under no circumstances should they upload a photo that contains nudity (it's illegal).
- Most importantly, teach them online common sense: think before you post or tweet. Would you want the entire school to see this post, photo, or video? If you would not say something to someone's face, do not say it in an online message.

How to protect your children's safety:

- Teach them to only accept requests from Facebook friends and Twitter followers they know personally ("Don't talk to strangers").
- Instruct your children to never agree to meet face-to-face someone they only know online.
- Keep lines of communication open. Your kids might not tell you everything, but that doesn't mean you shouldn't ask.

Cyberbullying

Cyberbullying is using the Internet to harass or bully someone, for example, by spreading false rumors or sharing inappropriate images online.

How to prevent cyberbullying:

- Speak with your children about what is appropriate to say and do online. Be kind online.
- Review your child's online information from time to time. Seeing what others say on your child's pages can help you stop cyberbullying.
- Try to spot changes in your child's behavior that might suggest cyberbullying such as avoiding computers or appearing stressed when receiving an email or text.

What to do if you feel your child is a victim of cyberbullying:

- Tell your children not to respond to cyberbullying, but to stop, block and tell.
  1) Stop interacting with the bully.
  2) Block the bully from sending any more messages.
  3) Tell an adult they trust.
- Document everything. Save emails and other communication.
- Seek help. If you feel your child is in immediate danger, report the incident to law enforcement immediately.

Protecting your identity

- Using strong passwords protects your valuable personal information and keeps you safe.

Password Do's and Don'ts:

- Do use a mix of letters, symbols and numbers.
- Do not use sequences (123 or abc) or personal information such as your birth date.
- Do not use easy dictionary words.
- Do not reuse old passwords.

Email "Phishing"

This is when scammers send emails that pretend to come from a real company to try to trick you into revealing private information, like addresses or account numbers.

How to avoid Phishing:

- Don't reply to messages that ask about personal or financial information.
- Check the link: If you do not trust the website or sender, DO NOT click on any links in the email.

Spyware and Viruses

This is when a computer program gathers your information without your knowledge or permission. Spyware can make your computer work poorly (slow browsing, program crashes, etc.).

Dear Parents:

Your child has the opportunity to receive an electronic mobile device, network account or access, and needs your permission to do so. Among other advantages, your child will be able to communicate with other schools, colleges, organizations and individuals around the world through Internet and other electronic information systems and networks. Internet is a system, which links smaller computer networks, creating a large and diverse network. Internet allows your child, through electronic mail (e-mail) and other means to reach out to many other people to share information, learn concepts and research subjects. These are significant learning opportunities to prepare your child for the future.

With this educational opportunity also comes responsibility. It is important that you and your child read the enclosed informed consent form, school district procedures and other material, and discuss it together. When your child is given an account and password to use on the computer, it is extremely important that the rules be followed. Inappropriate use will result in the loss of the privilege to use this educational tool, and other disciplinary action if appropriate. Parents, remember that you are legally responsible for your child's actions.

Please stress to your child the importance of using only his or her mobile device, account password, and of keeping the password a secret from other students. Your child should never let anyone else use his/her mobile device, password to access the network. Your child is responsible for any activity that happens in his/her mobile device and account.

We have established procedures and rules regulating the materials that students may search for on the network, but please be aware that there is unacceptable and controversial material and communications on the Internet that your child could access. It is not possible for us to always provide direct supervision of all students. We cannot filter material posted on network-connected computers all over the world; we encourage you to consider the potential of your child being exposed to inappropriate material in your decision of whether or not to sign the informed consent form.

We also reserve the right to review e-mail sent or received on the district system to improve student safety and system integrity, and you and your child must waive the copyright on any material posted through the network.

If you have any questions please contact me at 782-3355. If you want your child to have the opportunity to receive an Electronic Network account or access, please return signed informed consent forms to your child's school as soon as possible.

Sincerely,

Glenn Johnson,
Superintendent

ELECTRONIC INFORMATION SYSTEM (K-20 NETWORK)
INDIVIDUAL USER ACCESS INFORMED CONSENT FORM

In consideration for the privilege of using a mobile device, the network and in consideration for having access to the public networks, I hereby release Cashmere School District, the K-20 Network, and other intermediary providers, if any, and operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my, or my child's use, or inability to use, the K-20 Network including, without limitation, the type of damages identified in the Cashmere School District's Acceptable Use Guidelines. Further, my child and I agree to abide by the District's Policy and Procedures for Electronic Information Systems, and the Parent/Student Handbook for 1:1 Technology Integration which we have reviewed and understand, and we acknowledge that failure to comply with the policy and procedures may result in revocation of network use privileges. My child and I acknowledge and agree that Cashmere School District has the right to review, edit or remove any materials installed, used, stored or distributed on or through the network or District's system including e-mail and other electronic messages and we hereby waive any right of privacy which my child or I may otherwise have into such material. My child and I acknowledge and agree that any copyright my child may have in material posted on the Internet through the school district's system is waived.

Signature of User	Signature of Parent/Guardian (required if user is under age 18)
Printed Name of User	Printed Name of Parent/Guardian
Address	Address
City/State/Zip	City/State/Zip
Phone	Phone
Date Signed	Date Signed

***** Students over eighteen do not need a parent's signature

OFFICIAL USE ONLY/DO NOT WRITE BELOW THIS LINE

Account Number _____

Approved by: _____ Date: _____