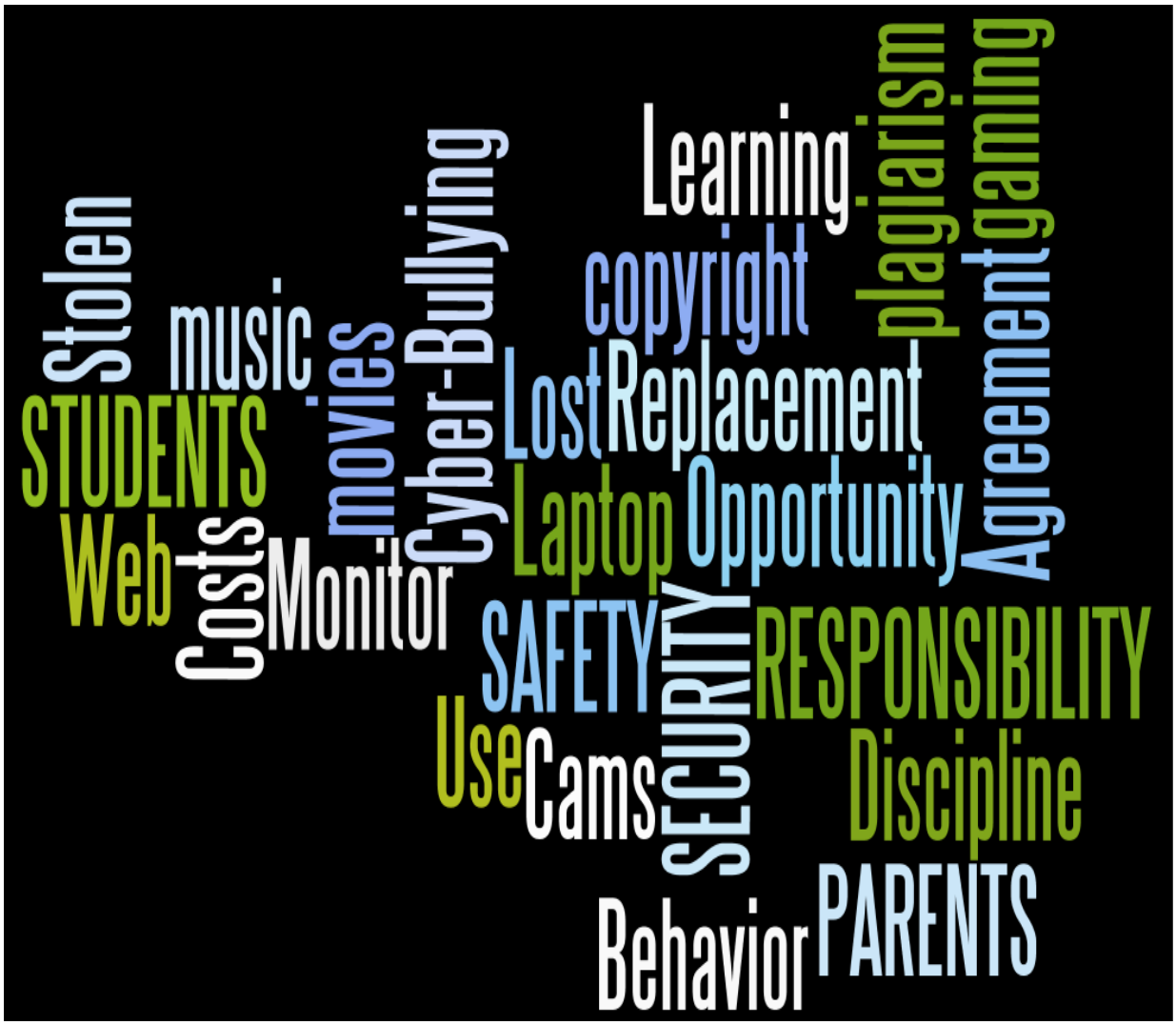
FERNDALE
SCHOOL DISTRICT

Making a Difference…..



STUDENT/PARENT HANDBOOK

Ferndale School District

Ferndale School District

Parent/Student Handbook for 1:1 Technology Integration

Table of Contents

Parent/Student Handbook for 1:1 Technology Integration

Ferndale 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 all 6th, 7th, and 8th grade students in the Ferndale School District daily access to a computer to enhance and extend learning opportunities inside, as well as outside the classroom.

Ferndale 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 Ferndale 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)

HP Elitepad 900

Productivity Case

AC Adapter (with power cord)

Student Computers - Checkout

Each student enrolled at Ferndale Middle Schools will be issued a laptop in the library

sometime towards the start of the school year. Students who have not returned a signed technology agreement will not be issued a device.

Ferndale 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.

The productivity case and charger for the device is also the possession of Ferndale School District. Students will receive a device with their name and identification number. No additional modifications by the student are allowed.

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. The goal is to issue the exact same device to students (including the productivity case and power cord) in the fall of the next school year.

Student Responsibilities

The primary goal of Ferndale 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.

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.

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

- *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.
- Proper etiquette and codes of conduct must be used in electronic communication. All communications via electronic resources should be assumed to be public record.
- All electronic accounts are to be used only by the authorized owner of

the account. Keep passwords and personal information private.
- Observe and respect license and copyright agreements.
- Return the laptops to the school at the end of the school year for system updates and reimaging.

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 on laptops
    - 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 does not apply to locations outside of the school district. It is therefore important for parents/guardians to determine if setting up Internet filters at home would be appropriate for their family.
- 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 immediately report the incident to an adult.

Digital Citizenship will be taught in every technology class in the Ferndale School District. Within this curriculum students will 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 use online resources in an ethical manner.

Student Use in the Classroom

- Students will be required to take their computer to class each day, unless told differently by the teacher for that specific 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 be designing many of their lessons and classroom based on students having access to their computer, so 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.
- All computers have a tracking feature enabled. The sooner we know about the missing device, the faster we can find it.
- If a computer is lost, stolen, or vandalized while not at a Ferndale School District sponsored event, the parent shall file a police report.
- Always lock computers in your PE locker during PE and/or after school sports.

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 Ferndale 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:
  - Extreme heat or cold
  - Food and drinks
  - Small Children
  - Pets

Traveling To and From School

- Completely shut down the computer before traveling. (The device charges more efficiently out of the Productivity Case)
- 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 truck 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 Ferndale 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 that are to be placed the area in front of the stage during lunch. (Horizon MS Students)
- Students can use computers only after they have eaten lunch and are in a designated work space.

Lockers

- Computers should be stored upright.
- Never pile things on top of the device.
- 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. <u>These cameras are to be used for educational purposes only</u>, under the direction of the teacher. If a student is caught using these applications inappropriately further discipline action may be enforced by the administration.

Listening to Music

- At School: Listening to music on your computer is <u>not allowed during school hours</u> without permission from the teacher. Permission will be given only for media used to complete a school assignment.
- At Home: Listen 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 the any identification placed on the computer.

FERNDALE SCHOOL DISTRICT NO. 502

ADMINISTRATIVE PROCEDURES

No. 2314 P-1

Attachment 1

TECHNOLOGY RESOURCES USE AGREEMENT (STUDENT)

Parent or Guardian:
The students in Ferndale School District (FSD) have direct access to the Internet and the FSD network. With this privilege comes responsibility. All students must be informed of the rules regarding Internet and network use and agree to abide by these rules. The District utilizes software and content filtering to prevent students from accessing inappropriate online materials. Users of the district network are required to sign a "Technology Resources Use Agreement." Please read and discuss this information with your student and sign on the back. Parents and students will be required to complete the "Technology Resources Use Agreement" upon first technology usage (usually at elementary school level), at the beginning of each of the middle grades six, seven and eighth, then finally as they enter high school in the ninth grade. Also note, individual schools may require annual completion.

Student:

The use of the network is a privilege and inappropriate use may result in a cancellation of those privileges. Security on any computer system is a high priority, especially when the system involves many users. If the user identifies a security problem on the system, the user must notify staff and must not demonstrate the problem to other users. Students are responsible for good behavior on school computer networks just as they are in a school classroom or a school hallway.

Please sign this document and **return it** to the

School or as **directed by your teacher**

The following information was extracted/adapted from the "**Ferndale School District Board Procedure #2314 P-1 Technology Resources."** Copies of the complete board policy no. 2314 and procedures are available on the FSD website.

Personal Internet Safety:

1. **Do Not** reveal personal contact information about yourself (address, phone number, etc) while online
2. **Do Not** agree to meet people that you have been in contact with over the Internet without parent permission
3. **Do Not** give out private or confidential information about yourself or others

4. **Tell** your teacher or other school employee about any message you receive that is inappropriate or makes you uncomfortable

Acceptable Use:

The use of this account **must be** in **support** of **education** and **educational research.**

Unacceptable Use:

Examples of Activities (but not limited to), which are **NOT PERMITTED**:

1. Displaying sexually explicit, pornographic, obscene, lewd or other inappropriate messages or pictures
2. Using obscene language or material
3. Participating in offensive and/or threatening attacks via "Cyber Bullying" against individuals or groups
4. Damaging computers, computer system or computer networks
5. Violating copyright laws
6. Using other users' passwords
7. Trespassing on other users' work: systems, folders, work or files
8. Excessive use of limited resources (beyond time authorized by administrators)
9. Personal email or free "web surfing" during school hours
10. Employing the network for commercial, personal or political purposes
11. Modifying software on district equipment or installing personal technology on the network without written permission
12. Accessing any computer not explicitly authorized for use

Student Email

Ferndale School District recently created email accounts for all students, which includes email access if needed. FSD is providing this service because it is obligated, through e-rate and federal regulations; "to ensure that all students use computers, networks and communications (including e-mail) in schools for school related purposes in an appropriate manner." The mastery of effective and proper e-mail communications is expected of FSD students and is embedded in the Washington State K-12 Essential Academic Learning Requirements and Grade Level Expectations in Educational Technology such as EALR 2: Digital Citizenship, Component 2.3, "communicate with peers and teachers using email." Consequently, FSD students will be expected to utilize their FSD e-mail account for district and school communication.

This account will be assigned to students as they enter the district and will be available for school/educational usage throughout their career in Ferndale School District. However, this account will only become "active" for student use beginning at 6th grade (earlier in the case of specific teacher request to be used in his/her classroom). In addition to email, this account will provide access to collaboration tools (word processor, calendar, spreadsheets), as well as other educational related tools.

Student- (signature required)

I understand and will abide by the Technology Resources Use Agreement Policy and agree to use the network responsibly. I further understand that any violation of the regulations contained therein may result in disciplinary action and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked and school disciplinary action or appropriate legal action may be taken.

Student Full Name (please print) _____

Signature _____ Date _____

Parent or Guardian Permission – (If student is under the age of 18, a parent or guardian must also read and sign this agreement)

As a parent or guardian of this student, I have read the Technology Resources Use Agreement Policy. I understand that this access is designed for educational purposes only. I recognize that it is impossible for Ferndale School District to completely restrict access to offensive, inappropriate or other controversial information and materials available through Internet or other sources from the network, and I will not hold the school district responsible for information and materials obtained by this student from the network. I understand this agreement will be kept on file at the school.

I also understand that from time to time the teacher or school may wish to publish examples of student projects, unidentified photographs of students and other work on an Internet accessible server via staff, school or district website.

Please circle.

My child may use the Internet and email (with teacher supervision) at school according to the rules outlined.

Yes No

My child's work may be published on the Internet for classroom/school purposes.

Yes No

Parent/Guardian Name (Please print) _____

Signature _____Date_____

****For additional information, please contact your student's principal or FSD Technology Department****

Implemented 10-12-1995
Revised 06-10-2010

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.).