CASCADE
SCHOOL DISTRICT

# TECHNOLOGY HANDBOOK

*for Students and Parents*

2019-2020

# Table of Contents

## Letter from the Superintendent

Welcome to Cascade School District's official first full school year of one-to-one technology!

In 2017, Cascade School District communities voted "yes" and paved the way for each student to have access to an educational technology device. This was a giant leap in bringing our district into 21st century learning. No longer would only the students whose parents could afford a computer have access to individualized learning; no longer would students have to wait for their turn at a computer station. This vote led to a great improvement in providing every Cascade student the opportunity to learn the skills necessary to compete in the 21st century workplace.

During the 2019-2020 school year, we are looking forward to diving into our technology initiative even further. For example, we will implement a **Learning Management System (LMS)** called *Canvas* at Cascade High School. Canvas is a digital learning platform used in colleges and high schools across the country which gives teachers a space to put all of their classroom resources and assignments, and gives students a place to engage in virtual conversations and turn in their homework, among other features.

Please be on the lookout for Canvas and other opportunities for students across the district to engage and create with technology this school year. Our School Board and I thank everyone who helped make this dream a reality and who continue to support our communities' children.

Dr. Tracey Beckendorf-Edou
Superintendent

## History of the Cascade School District Technology Initiative

In April of 2012, the communities of Cascade School District voted their support of a technology levy by 62%. That funding was used to pay for classroom technology, including interactive white boards, ceiling mount projectors, and updated staff and student computers. It was also used to pay for technology infrastructure such as cabling, Wi-Fi, and servers. The remainder of that funding was used to pay for staff development, in order to help staff be better prepared to teach 21st century skills.

The communities of Cascade School District again supported a technology and safety levy in 2017, this time by 55%. The technology portion of that funding provided software and hardware upgrades, continued technology training, improving network support services, and more. The 2017 levy was vital in allowing Cascade School District to move in the direction of **one-to-one** technology for students.

Since Washington State does not fund technology, these investments have been vitally important in providing technology equipment for learning, classroom training, and access to online resources.

## One-to-One

"One-to-one" means that each student has access to a technology device. In Cascade School District, this means that kindergarten, first grade and second grade students have access to an iPad, and students in grade 3 on up have access to a laptop. At Alpine Lakes, all students are assigned to one device located in classroom sets. At Icicle River Middle School, students are assigned one device that they will use for all three grade levels. At Cascade High School, students can use laptops that are

available in classroom sets. In addition, they can check out laptops in the library and in the career center. Currently, all devices stay at school.

## How Does One-to-One Help Learning?

Technology is a basic educational tool today. Students use technology in order to successfully learn, produce, and create information in a 21st century classroom. In addition, having a one-to-one classroom and district levels the playing field so that all students learn technology skills necessary for future college and careers. In essence, having a one-to-one initiative reduces what is called the **digital divide**. A **digital divide** means the gulf between those who have ready access to computers and the Internet and those who do not.

Cascade School District is committed to classroom technology because it promotes students engagement and learning enthusiasm; encourages collaboration among people within and without the district through interactive networking; guides student learning and knowledge production; and opens student access to information and opportunities to connect to this learning in meaningful and relevant ways.

Digital learning will never replace classroom teachers and the value of hands-on activities and play. Digital learning is one part of the classroom experience but it is not intended to be the only aspect of the classroom experience. Cascade School District therefore supports **blended learning**, which is a style of education in which students learn in a mix of hands-on, face-to-face, and electronic methods.

## District Policies and Procedures

School Board policies that are relevant to the use of technology devices include but are not limited to: 2022, Electronic Resources and Internet Safety; 2024, Online Learning; and 2255, Alternative Learning Experience Programs.

## Expectations

Throughout the remainder of this document, the term **Technology Device** includes the tablet, keyboard, desktop, iPad, power supply/charger, printer, and/or digital inking pen(s).

## Technology Device Use

- The technology device is the property of the Cascade School District and may be collected and inspected at any time. Students have no right to privacy for any material on a district technology device.
- Each technology device has a unique label. Students should not modify or remove the label. *Students must not write on, draw on, add stickers, etch, or engrave the technology device.* No other form of tampering will be permitted.
- It is the student's responsibility to back up projects and content. Students may want to purchase a flash drive for this task or plan to store their materials in the cloud in Office 365.
- If a student's technology device is not working or is damaged, the student **must** report the problem immediately to their teacher, who will then report it to the Help Desk.
- If a label has been damaged or has fallen off, the student must return the device to the teacher, who will then report it to the Help Desk so that a new label can be made and placed on the

device.
- Students are responsible for using the technology device according to school and district policies and procedures.

# Technology Device Guidelines

## CARE & MAINTENANCE

- Devices should NEVER be picked up by the lid. Students should close the technology device before it is picked up.
- Liquids and food should not be used/consumed in the vicinity of the technology device.
- Cleaners, sprays, alcohol, ammonia or abrasives should not be on the technology device.
- Devices should be cleaned with a soft, lint-free cloth.
- The device should not be in a place where someone could accidentally sit or step on it.
- Devices need to be charged in the charging station in each classroom.

## NEGLIGENCE

- The district reserves the right to charge the user the full cost of repair or replacement of the device when damage or loss occurs due to negligence.
- An administrator will meet with the student to investigate and discuss with the parent/guardian as necessary.
- The replacement cost of the machine cannot be satisfied by families themselves purchasing their own replacement device.
- The cost of repairs will be assessed for each reported incident.

Multiple offenses will be handled appropriately and in consultation with the district office if necessary.

# Acceptable Use Policy

## GUIDELINES FOR USE OF TECHNOLOGICAL RESOURCES

The following actions are permitted:

- Creation of files, digital projects, videos, web pages and podcasts using network resources in support of education and research;
- Participation in blogs, wikis, bulletin boards, and groups and the creation of content for podcasts, email, and webpages that support education and research;
- With parental permission, the online publication of original educational material, curriculum-related materials and student work. Sources outside the classroom or school must be cited appropriately;
- Connection of personal electronic devices (wired or wireless), when authorized, including portable devices with network capabilities, to the district's network. Connection of any

personal electronic device is subject to all procedures in this document and district policy.

The following actions are not permitted:

- Using Virtual Private Networks (VPNs) to bypass district content filtering;
- Using district technological resources for personal gain, commercial solicitation, and compensation of any kind;
- Actions that result in liability or cost incurred by the district;
- Downloading, installing and use of games, audio files, video files, games, or other applications (including shareware or freeware) without permission or approval;
- Support for or opposition to ballot measures, candidates, and any other political activity;
- Hacking, cracking, vandalizing, the introduction of malware, including viruses, worms, Trojan horses, time bombs and changes to hardware, software and monitoring tools;
- Unauthorized access to other district computers, other user accounts, networks and information systems;
- Unauthorized videotaping at school;
- Action constituting harassment, intimidation or bullying, including cyberbullying, hate mail, defamation, discriminatory jokes and remarks. This may also include the manufacture, distribution, or possession of inappropriate digital images;
- Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
- Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material; or
- Any unlawful use of the district network, including but not limited to stalking, blackmail, violation of copyright laws, and fraud.

## CONSEQUENCES

1. Upon the first violation, a student will lose access privilege for a period of no less than one week (5 school days). Verified parent notification by student.
2. Upon the second violation, a student will lose access privilege for a period of no less than one month (20 school days). There will be parent notification/parent conference prior to reinstatement of system privileges.
3. Upon the third violation, a student will lose all privileges to the system for the remainder of the school year. There will be student reinstatement of the privilege the following school year after a parent conference is held.
4. Serious violations to student safety or the integrity of the computer system can result in immediate and permanent removal from the computer system.
5. If a law is broken, law enforcement will be involved.

## STUDENT INTERNET SAFETY

Students will be instructed as to safe and responsible use of the Internet using readily available and age appropriate tools and information, as the curriculum permits. Students must abide by all laws, this Acceptable Use Policy and all district security policies when using the district network.

## *Filter*

As a component of district Internet safety measures, all district-owned electronic resources, including computer networks and Wi-Fi's, in all district facilities capable of accessing the Internet, use content filtering to prevent access to obscene, racist, hateful or violent material. However, given the ever-changing nature of the Internet, the district cannot guarantee that a student will never be able to access objectionable material. Therefore, it is important that students practice good **digital citizenship**.

**Digital citizenship** includes the norms of appropriate, responsible, and healthy behavior related to current technology use. Successful, technologically-fluent digital citizens recognize and value the rights, responsibilities, and opportunities of living, learning, and working in an interconnected digital world. They cultivate and manage their digital identity and reputation, and are aware of the permanence of their actions in the digital world. Expectations for student behavior online are no different from face-to-face interactions.

## *Cyberbullying*

Per release of the FCC (Federal Communications Commission) and CIPA (Children's Internet Protection Act) to prohibit inappropriate online behavior, students shall not use cell phones, instant messaging, email, chat rooms, social networking sites, or other types of digital technology to bully, threaten, discriminate, or intimidate others.

If a student or staff member receives a text, email, blog comment, social network post, or message via other Web 2.0 tool that makes them feel uncomfortable or is not respectful, they must report the incident to the school administrator or building designee, and must not respond to the comment. This policy includes "cyber baiting", a term used for students deliberately provoking a teacher until they lose their composure in order to capture video that is then posted in a public forum online.

## *Personal Information and Inappropriate Content*

- Students and staff should not reveal personal information, including a home address and phone number, on web sites, blogs, podcasts, videos, social networking sites, wikis, email or as content on any other electronic medium;
- Students and staff should not reveal personal information about another individual on any electronic medium without first obtaining permission;
- No student pictures or names can be published on any public class, school or district website unless the appropriate permission has been obtained according to district policy;
- If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority; and
- Students should be aware of the persistence of their digital information, including images and social media activity, which may remain on the Internet indefinitely.

## *Parent/Guardian Consent*

We recognize that parents/guardians of minors are responsible for setting and conveying the standards their children should follow when using media and information sources. Accordingly, before a student may independently access the Internet, the student's parent/guardian must be made aware of the possibility that the student could obtain access to inappropriate material while engaged in independent use of the Internet.

The parent/guardian and student must consent to the student's independent access to the Internet

and to monitoring of the student's communication by school personnel.

## PRIVACY

The district provides the network system, email, and Internet access as a tool for education and research in support of the district's mission. Students and staff will have no expectation of privacy when utilizing district technology. The district reserves the right to inspect, without notice, review and log all activity using district technology, including:

- The district network, including when accessed on students' personal electronic devices (e.g. cell phones) and on devices provided by the district, such as laptops, netbooks, and tablets;
- User files and disk space utilization;
- User applications and bandwidth utilization;
- User document files, folders and electronic communications;
- Email;
- Internet access; and
- Any and all information transmitted or received in connection with network and email use.

The district reserves the right to disclose any electronic messages to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of the State of Washington.

## SECURITY/CARE OF PROPERTY

Security on any computer system is a high priority, especially when the system involves many users. Users are responsible for reporting information security violations to appropriate personnel. Users should not demonstrate the suspected security violation to other users. Unauthorized attempts to log onto any school system computer on the network as a system administrator may result in cancellation of user privileges and/or additional disciplinary action. Any user identified as a security risk or having a history of problems with other systems may be denied access. Users of school district technology resources are expected to respect school district property and be responsible in using the equipment. Users are to follow all instructions regarding maintenance or care of the equipment. Users may be held responsible for any loss or damage caused by intentional or negligent acts in caring for computers while under their control. The school district is responsible for any routine maintenance or standard repairs to school system computers.

# Parent/Guardian Suggestions for Home Use of Technology

- Monitor your child's home use of the Internet.
- Provide a place in an open area of your home, such as the kitchen or family room, where technology devices will be used.
- Use the Internet with your child to help develop safe Internet habits.
- If you have provided your child with a cell phone, tablet or laptop, frequently ask to see your child's technology device and ask how it is being used.
- If your child is contacted by an adult for immoral purposes, contact law enforcement.

- Review with your child the programs installed on any technology device and ask them what each program does.
- You may want to take a look at resources available at Common Sense Media: https://www.commonsensemedia.org/.
- **If you come in contact with any inappropriate photographs of juveniles on your child's technology device, do not forward them. Secure the device and immediately bring it to law enforcement.**
- Do not hesitate to contact your school if you have any questions or concerns.