INSTRUCTION
Electronic Resources and Internet Safety

Cascade School District Network Acceptable Use Guidelines/Internet Safety Requirements
These procedures are written to support the Electronic Resources Policy of the board of directors and to promote positive and effective digital citizenship among students and staff. 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 and staff behavior online are no different from face-to-face interactions.

Use of Personal Electronic Devices
In accordance with all district policies and procedures, students and staff may use personal electronic devices (PED’s) (e.g. laptops, mobile devices and e-readers) to further the educational and research mission of the district. School staff will retain the final authority in deciding when and how students may use personal electronic devices on school grounds and during the school day. Absent a specific and articulated need (e.g. assistive technology), students do not have an absolute right to possess or use personal electronic devices at school.

Network
The district network includes wired and wireless devices and peripheral equipment, files and storage, e-mail and Internet content (blogs, websites, collaboration software, social networking sites, wikis, etc.). The district reserves the right to prioritize the use of, and access to, the network.

All use of the network must support education and research and be consistent with the mission of the district.

Acceptable network use by district students and staff include:
A. Creation of files, digital projects, videos, web pages and podcasts using network resources in support of education and research;
B. Participation in blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for podcasts, e-mail, and webpages that support education and research;
C. 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;
D. Staff use of the network for incidental personal use in accordance with all district policies and procedures; or
E. 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.

Unacceptable network use by district students and staff includes but is not limited to:
A. Personal gain, commercial solicitation, and compensation of any kind;
B. Actions that result in liability or cost incurred by the district;
C. Downloading, installing and use of games, audio files, video files, games, or other applications (including shareware or freeware) without permission or approval from the supervisor;
D. Support for or opposition to ballot measures, candidates, and any other political activity;
E. Hacking, cracking, vandalizing, the introduction of malware, including viruses, worms, Trojan horses, time bombs and changes to hardware, software and monitoring tools;
F. Unauthorized access to other district computers, networks and information systems;
G. 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;
H. Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
I. Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material; or
J. Any unlawful use of the district network, including but not limited to stalking, blackmail, violation of copyright laws, and fraud.

The district will not be responsible for any damages suffered by any user, including but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions caused by his/her own negligence or any other errors or omissions. The district will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the district’s computer network or the Internet.

Personal Information and Inappropriate Content
A. 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, e-mail or as content on any other electronic medium;
B. Students and staff should not reveal personal information about another individual on any electronic medium without first obtaining permission;
C. 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;
D. If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority; and
E. Students should be aware of the persistence of their digital information, including images and social media activity, which may remain on the Internet indefinitely.

Filtering and Monitoring
Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children’s Internet Protection Act (CIPA). Other objectionable material could be filtered. The determination of what constitutes “other objectionable” material is a local decision.

A. Filtering software is not 100 percent effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his/her use of the network and Internet and avoid objectionable sites;
B. Any attempts to defeat or bypass the district’s Internet filter or conceal Internet activity are prohibited (e.g., proxies, https, special ports, modification to browser settings and any other techniques to evade filtering or enable the publication of inappropriate content);
C. E-mail inconsistent with the educational and research mission of the district will be considered SPAM and blocked from entering district e-mail boxes;
D. The district will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to district devices;

E. Staff members who supervise students, control electronic equipment or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of the district;

F. Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively;

G. The district may monitor student use of the district network, including when accessed on students’ personal electronic devices and devices provided by the district, such as laptops, netbooks, and tablets; and

H. The district will provide a procedure for students and staff members to anonymously request access to Internet websites blocked by the district’s filtering software. The procedure will indicate a timeframe for a designated school official to respond to the request. The requirements of the Children’s Internet Protection Act (CIPA) will be considered in evaluation of the request. The district will provide an appeal process for requests that are denied.

**Internet Safety**

Students will be educated about appropriate online behavior, including interacting with other individuals on social media sites and in online forums, and cyberbullying awareness and response.

A. The Cascade School District’s wireless network will provide filtered Internet access. Cascade School District is neither responsible nor liable for student access to any other network accessed while the device is operated on district property or at any school-sponsored activity or event off school property (including Internet service provided by any commercial service provider).

B. A PED shall not be used in a manner that disrupts the educational process, including but not limited to, posing a threat to academic integrity.

C. Devices shall not be used to violate confidentiality or privacy rights of another individual, including but not limited to, taking photographs or audio or video recordings of others without their permission or sharing, posting, or publishing photographs, videos or recordings of other without their permission.

**Copyright**

Downloading, copying, duplicating, and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of materials for educational purposes is permitted when such duplication and distribution falls within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

**Ownership of Work**

All work completed by students as part of the regular instructional program is owned by the student as soon as it is created, unless such work is created while the student is acting as an employee of the district or unless such work has been paid for under a written agreement with the district. If under an agreement with the district, the work will be considered the property of
the district. Staff members must obtain a student’s permission prior to distributing his/her work to parties outside the school or the district. Sources outside the classroom or school must be cited appropriately.

All work completed by employees as part of their employment will be considered property of the district. The District will own any and all rights to such work including any and all derivative works, unless there is a written agreement to the contrary.

**Network Security and Privacy**

**Network Security**

Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account for authorized district purposes. Students and staff are responsible for all activity on their account and must not share their account password. The following procedures are designed to safeguard network user accounts:

A. Change passwords according to district policy;
B. Do not use another user’s account;
C. Do not insert passwords into e-mail or other communications;
D. If you write down your user account password, keep it in a secure location;
E. Do not store passwords in a file without encryption;
F. Do not use the “remember password” feature of Internet browsers; and
G. Lock the screen or log off if leaving the computer.

**Student Data is Confidential**

District staff must maintain the confidentiality of student data in accordance with the Family Educational Rights and Privacy Act (FERPA).

**Privacy**

The district provides the network system, e-mail, 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:

A. The district network, including when accessed on students’ personal electronic devices and on devices provided by the district, such as laptops, netbooks, and tablets;
B. User files and disk space utilization;
C. User applications and bandwidth utilization;
D. User document files, folders and electronic communications;
E. E-mail;
F. Internet access; and
G. Any and all information transmitted or received in connection with network and e-mail 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.

**Educational Applications and Programs**

District staff may request students to download or sign up for applications or programs on the students’ personal electronic devices. Such applications and programs are designed to help
facilitate lectures, student assessment, communication, and teacher-student feedback, among other things.

Prior to requesting students to download or sign up for educational applications or programs, staff will review “terms of use”, “terms of service,” and/or “privacy policy” of each application or program to ensure that it will not compromise students’ personally identifiable information, safety, and privacy.

Staff will also provide notice for approval in writing of potential use of any educational application or program to the technology director and building principal, including the anticipated purpose of such application or program. Specific expectations of use will be reviewed with students.

Archive and Backup
Backup is made of all district e-mail correspondence for purposes of public disclosure and disaster recovery. Barring power outage or intermittent technical issues, staff and student files are backed up on district servers regularly. Refer to the district retention policy for specific records retention requirements.

Disciplinary Action
All users of the district’s electronic resources are required to comply with the district’s policy and procedures (and agree to abide by the provisions set forth in the district’s user agreement). Violation of any of the conditions of use explained in the district’s user agreement, Electronic Resources policy or in these procedures could be cause for disciplinary action, including suspension or expulsion from school and suspension or revocation of network and computer access privileges.

Accessibility of Electronic Resources
Federal law prohibits people, on the basis of disability (such as seeing and hearing impairments), from being excluded from participation in, being denied the benefits of, or otherwise being subjected to discrimination by the district. To ensure that individuals with disabilities have equal access to district programs, activities, and services, the content and functionality of websites associated with the district should be accessible. Such websites may include, but are not limited to, the district’s homepage, teacher websites, district-operated social media pages, and online class lectures.

District staff with authority to create or modify website content or functionality associated with the district will take reasonable measures to ensure that such content or functionality is accessible to individuals with disabilities. Any such staff member with questions about how to comply with this requirement should consult with the superintendent.

Staff Social Media Guidelines
Cascade School District (the “District”) recognizes the importance of social media as a means of communication. The District encourages the appropriate use of social media as a means to communicate, whether as an individual or as a school or District program, with community members of the District.

The District acknowledges that its employees have the right under the First Amendment as private citizens to speak out on matters of public concern. However, the District has the right to regulate the speech of employees in specific circumstances. Accordingly, it is essential that
employees conduct themselves in such a way that their personal and/or educational use of social media does not adversely affect their position or cause disruption to the educational process with the District.

The purpose of these guidelines is to establish protocols for the use of social media by employees and to outline expectations for its use. “Social Media” means a broadly accessible internet-based communication platform used to interact with other users and share content among a network. Examples of social media include but are not limited to Facebook, Twitter, Instagram, YouTube, Flikr, Blogs, and Wikis.

A. Guidelines for all use of social media (personal and educational)

- Your behavior on social media should reflect the same standards of honesty, respect, and consideration and are expected to adhere to in all forms of communications and interactions;
- Do not submit or post confidential or protected information about the District, its students, alumni, or employees. You should assume that most information about a student is protected from disclosure by both federal law (the Family Educational Rights and Privacy Act (FERPA) and state law. Disclosure of confidential or protected information may result in liability for invasion of privacy or defamation and may result in disciplinary action up to, and including, discharge from employment;
- Report, as required by law, any information found on a social networking site that falls under the mandatory reporting guidelines;
- Do not use language that could be considered defamatory, obscene, proprietary, or libelous; that could incite others to imminent violence; or that constitutes a true threat;
- Do not post or otherwise publish content that is or could reasonably be perceived as bullying, discrimination, or harassment in violation of district policy;
- Exercise caution with regards to exaggeration, colorful language, guesswork, copyrighted materials, legal conclusions, and derogatory remarks or characterizations;
- Consider whether a particular posting puts your professional reputation and effectiveness as a district employee at risk;
- Be cautious of security risks when using third-party applications within a social media site;
- Run updated malware protection to avoid infections of spyware and adware that social media sites might place on your personal computer;
- Be alert to the possibility of phishing scams that arrive through a social media site. As always, scrutinize all emails from unknown senders and be wary of any unsolicited attachments sent by unknown sources or senders;

B. Guidelines for the personal use of social media

In addition to Section A, above, employees using social media for personal (non-district-related) purposes are expected to:

- Refrain from using social media for personal use during work time;
- Refrain from accepting current district students as “friends” on personal social media sites;
- Refrain from communicating or otherwise disseminating any confidential information you have access to as a result of your employment with the District;
- Be aware that people classified as “friends” can download and share your information with others;
- Assume that anything posted to a personal social media site can be accessed by anyone and will be available forever.
Sharing school or District social media posts to your personal social media page (i.e. retweeting a @_________ announcement to your personal Twitter page) is acceptable and encouraged if it is something of interest to you;

Set and maintain appropriate social media privacy settings. Be aware that social media sites can change their privacy policies and standards at any time, possibly exposing posts that you believed were private to the public;

Avoid using a social media site to post content that may be considered defamatory or obscene, and do not post content that violates copyright or other intellectual property laws;

Refrain from using a social media site to post information about a district student or employee in a way that is or could be reasonably perceived as discriminatory, harassing, or otherwise derogatory;

Refrain from texting a student or group of students. Any exceptions must be approved by the building principal. If you believe texting a student or group of students is necessary for student safety, then the student’s or students’ parents or guardians must be included in the text.

C. Guidelines for the educational use of social media

Educational use of social media refers to using district or school social media accounts. A district or school account refers to social media pages that pertain to district schools, classes, programs, clubs, or sports.

In addition to Section A, above, employees using social media for educational use are expected to:

Comply with all district policies and state laws on the use of district-owned hardware, software, and network;

Notify your supervisor or the superintendent if you wish to establish a social media site for a school, class, or program;

If using Facebook, create an organization page for your school, class, or program—DO NOT use a personal Facebook page for school-related purposes;

Establish expectations for acceptable use on your social media site that are compliant with the District’s expectations for acceptable use (see example at end of document);

Refrain from posting anything on a school or district affiliated social media page that advocates for or against a political candidate or ballot measure;

Refrain from posting or otherwise publishing images that include students or student photographs without parental release forms on file;

Pay close attention to the site’s security settings and allow only approved participants access to the site;

Remember that behavior that is inappropriate in school or the classroom is considered inappropriate online;

Seek consent before using the District’s logo or school-specific logos or mascots. The use of the District’s logo should be approved by the superintendent or their designee. The use of a school’s logo or mascot should be approved by the principal or their designee;

Remember that all district or school social media accounts and subsequent posts, comments, and direct messages are subject to the Washington State Public Records Laws. Accordingly, it is the responsibility of the employee who operates the social media account to work with the District’s Public Records Officer should a request be made.
Employees found to have engaged in inappropriate use of social media or other electronic communication may be subject to disciplinary action by the District, up to and including termination.

Establishing a school or District-related social media site
If you wish to establish a district or school social media account, you must first notify your supervisor or the superintendent’s office. If you have questions about content you would like posted to a district or school social media account, please contact your supervisor.

Acceptable Use Guideline Example
The following acceptable use guideline is posted to the District’s Facebook page, and provides an example that can be adopted for other District-related social media sites:

Cascade School District has created this Facebook page to serve as an additional means to share news, provide information, and facilitate communication within our school district community. We thank all the Facebook users who “like” our page and contribute to our online community. Messages posted to this Facebook page do not necessarily represent the views of Cascade School District. Cascade School District reserves the right to remove comments and/or report users who post comments that, in the District’s sole discretion, bully, intimidate, or harass any individual; contain obscenity, nudity, or gratuitous violence; are commercial solicitations; are factually erroneous, libelous, or wildly off-topic; are from anonymous blog trolls; constitute incitement to violence or violation of law or district policy, or which constitute true threats; or that otherwise violate state law, district policy, or the social media site’s own policies.

Reviewed: February 15, 2000, Revised: August 22, 2005
Adopted: September 12, 2005, March 27, 2006, March 9, 2015, Mar 11, 2019, Jan 23, 2023