Electronic Resources

Responsible 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 represents more than technology literacy. Successful, technologically-fluent digital citizens live safely and civilly in an increasingly digital world. They recognize that information posted on the internet is public and permanent and can have a long-term impact on an individual's life and career. Expectations for student and staff behavior online are no different from face-to-face interactions.

Responsible Use

Clover Park School District (CPSD) provides access to technologies for all users (staff, students and guests in some cases). Access to technology is a privilege, not a right, and as such, all users must seriously consider the responsibilities associated with the opportunity to use technology devoted to activities that support teaching and learning. The norms of behavior with regard to responsible use of technology are defined as Digital Citizenship. It is the responsibility of both CPSD staff and parents to help prepare students to be members and citizens of a digital society.

A digital citizen is one who:

1) Understands human, cultural and societal issues related to technology and practices legal and ethical behavior;

2) Advocates and practices safe, legal and responsible use of information and technology;

3) Exhibits a positive attitude toward using technology that supports collaboration, learning and productivity;

4) Demonstrates personal responsibility for lifelong learning; and

5) Exhibits leadership for digital citizenship.

Annually students will receive grade level appropriate instruction on digital citizenship and internet safety educating them about appropriate online behavior, interacting with other individuals on social networking websites, cyber-bullying awareness and response, and other relevant topics.

Annually, all staff must sign a Responsible Use and Internet Safety Agreement or take an online Responsible Use and Internet Safety course prior to using the network.

Definitions:

Technology

Technology shall be defined as any electronic device that can use a network connection, process information, display information or store information for long-term retrieval and the software and services used by these devices. This includes:

- All internet services and shared network services;
- Desktop, mobile computers, tablets, phones and other handheld devices;
- Videoconferencing, monitors, projection systems and telephones;
- Online collaboration services, message boards, email and other messaging services;
- Copiers, printers, peripheral equipment and external file storage devices;
- Social media, web-based or internet tools such as blogs, wikis, social networks, podcasts or other internet tools; and
- Additional technologies as developed.

Use of Personal Electronic Devices

In accordance with district policies and procedures, staff may use personal electronic devices (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.

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 be consistent with efforts to enhance learning, support education and research consistent with the district's mission and to provide support for district operations.

COPPA and Internet Tools Terms and Conditions

The Children's Online Privacy Protection Act (COPPA) is a federal law, enacted in 2000, related to online collection of personal information forms students under age 13. COPPA makes it clear to website owners what they must include in their privacy policy, when they must seek consent form parents for a child under 13 to use their services, and what the website owner's responsibilities are to protect the online privacy and safety of children. These rules apply regardless of whether the website is fee-based or not. COPPA does not preclude schools from acting as intermediaries between operators and parents in the notice and consent process, or from serving as the parent's agent in the process of collecting personal information online from students in the school context when parents have provided permission for student internet use.

CPSD's use and sharing of student data is solely for education purposes. District staff must maintain the confidentiality of student data in accordance with the Family Education Rights and Privacy Act (FERPA).

CPSD uses a variety of software systems in the classroom, including some that are hosted outside the district's facilities in "the cloud." When used appropriately and thoughtfully, these tools can help

create rich, flexible and engaging learning environment for CPSD students. Additionally, an important part of students becoming good digital citizens is having opportunities to access materials in the cloud and/or on the internet in a responsible and effective manner.

CPSD supports COPPA and requires websites the district uses adhere to this law. It is important that all CPSD staff members who work with children be aware of and follow COPPA and other state and federal regulations related to student internet access and related data use. Staff using web-based tools shall be aware of the Terms of Use and Privacy Policies for those systems. Staff, who want to use "outside" resources with students, shall obtain approval prior to use from the Information Technology Services and Teaching and Learning departments (see 2022-F1).

Acceptable network use by district students and staff include:

Must be approved for classroom use, prior to use and/or purchase. To seek approval for classroom use, please use the Technology, Software, and Website Request for Approval form (2022-F2). Information Technology Services and Teaching and Learning departments will evaluate websites and software for data privacy, licensing and alignment to instructional standards. Possible uses are listed below:

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 supporting education and research users will create online names that are appropriate and use appropriate language/content in all online posts;

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 and student use of the network for incidental personal use in accordance with all district policies and procedures. Such incidental work, while not prohibited, will not be provided any additional staffing resources to support or enable; or

E. Staff connection of any personal electronic device (wired or wireless) including portable devices with network capabilities to the district network after checking with the director of information technology services to confirm the device is equipped with up-to-date virus software, compatible network card and is configured properly. Connection of any personal electronic device is subject to all district procedures.

F. Users will help maintain a safe computing environment by notifying appropriate school or district officials of inappropriate behavior, vandalism, vulnerabilities, risks and breaches of CPSD policy involving technology. If the user is uncertain whether an activity is permitted or appropriate, he /she will ask a teacher/administrator before engaging in the activity.

Unacceptable network use by district students and staff includes but is not limited to:

A. Personal gain, commercial solicitation and/or compensation of any kind;

B. Actions resulting in liability or cost incurred by the district;

C. Downloading, installing and use of games, audio files, video files, games and/or other applications (including shareware or freeware) without permission or approval from the director of informational technology services;

D. Support for or opposition to ballot measures, candidates and/or any other political activity;

E. Hacking, cracking, vandalizing or the introduction of malware.

F. Unauthorized access to other district computers, networks and/or information systems;

G. Cyber bullying, hate mail, defamation, harassment of any kind, discriminatory jokes and/or remarks;

H. Information posted, sent and/or stored online that could endanger others (e.g., bomb construction, drug manufacturing);

I. Accessing, uploading, downloading, storage and/or distribution of obscene, pornographic or sexually explicit material; or

J. Attaching unauthorized devices to the district network. Any such device will be confiscated and additional disciplinary action may be taken.

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.

Internet Access Abuse/Unauthorized Use of Technology/Electronic Devices

This constitutes any action taken in violation of the district's acceptable use policy or any other district policy prohibiting harassing, intimidating or bullying behaviors, including, but not limited to:

- Using technology such as computers, cellular phones, handheld devices, smartphones, printers, network connections etc. owned by the district or used on district grounds, or at a district-sponsored event to harass, bully or intimidate any student, staff member or district volunteer.

- Using technology such as computers, cellular phones, handheld devices, smartphones, printers, etc. owned by the district or used on the district's grounds, or at a district-sponsored event that violates any student responsibilities and/or rights, see Policy 3200.

- Intentionally accessing and/or downloading vulgar or obscene materials.

- Communicating downloaded vulgar or obscene materials to others.

- Tampering with electronic hardware, data files or software or unauthorized access to, or use of, such technology.

Internet Safety

Personal Information and Inappropriate Content:

A. Students and staff should not reveal personal information, including a home address and phone number on websites, 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; and

D. If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

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, modifications to district browser settings and any other techniques designed 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 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; and

G. The district will provide a procedure for students and staff members to 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 CIPA will be considered in evaluation of the request. The district will provide an appeal process for requests that are denied.

Internet Safety Instruction

Personal information and inappropriate content:

1. Students and staff should not reveal personal information, including home address and phone number of websites, blogs, podcasts, videos, social networking sties, wikis, email, or as content on any other electronic medium;

2. Students and staff should not reveal personal information about another individual on any electronic medium without first obtaining permission;

3. 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; and

4. If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

Use of Social Media and Web-based Tools

Online communication is critical to students' learning 21st century skills. Social media, web-based or internet tools such as blogs, wikis, social networks, podcasts, email or other internet tools offer an authentic, real-world vehicle for student expression. Examples of social media include, but are not limited to Facebook, Twitter, YouTube, Google+, Instagram, LinkedIn and Flickr. The district's primary responsibility to students is their safety. The district holds staff and students using these tools to the same responsible use, terms of agreement, standards and expectations and must follow all established internet safety guidelines. When these tools are used by staff or students with district resources, the district reserves the right to monitor appropriate behavior and adherence to instructional guidelines. Anything deemed to be inappropriate will be subject to deletion. The district may also take other disciplinary actions as appropriate.

The district maintains the right to withdraw account access should there be reason to believe that the account has been misused or the individual has violated the district's policies or responsible use guidelines. Violation of district policy or these guidelines by staff, students and/or guests may result in disciplinary action as well as revocation of network and computer access privileges.

Social Media for Personal Use by Staff

Communication with Students:

To maintain a professional and appropriate relationship with students (Policy 5253-P1), district employees should not communicate with individual students who are currently enrolled in district schools on personal social media sites. Additionally, district employees should not communicate with students via social media tools in a manner that is not readily visible and accessible to the students' parents/guardians and the employee's supervisor. This provision is subject to the following exceptions: a) staff communication with their own family members; and b) if an emergency situation

requires such communication, in which case the district employee should notify his/her supervisor of the contact as soon as possible.

Guidance Regarding Personal Social Media Sites

District employees should exercise caution and common sense when using personal social media sites:

1. Employees are prohibited from inappropriate online socializing with students or from engaging in any conduct on social networking websites that violates the law, district policies, or other generally recognized professional standards. Employees whose conduct violates this policy may face discipline or termination, consistent with the district's policies, responsible use agreement and collective bargaining agreements, as applicable;

2. District employees are encouraged to use appropriate privacy settings to control access to their personal social media sites although there are limitations to privacy settings. Private communication published on the internet can easily become public; social media sites can change their current default privacy settings and other functions. As a result, employees are responsible for understanding the rules of the social media site being utilized;

3. District employees should not "tag" photos of other district employees, district volunteers, district contractors, or district vendors without the prior permission of the individuals being tagged;

4. Personal social media use, including off-hours use, has the potential to result in disruption at school and/or the workplace, and can be in violation of district policies and federal and/or state law;

5. The posting or disclosure of personally identifiable student information or confidential information via personal social media sites, in violation of these guidelines is prohibited; and

6. District employees should not use the district's logo in any postings or post district material on any personal social media sties without the written permission of a district administrator.

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 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.

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 school district or unless such work has been paid for under a written agreement with the school 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.

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, must not use the account of other users, and must exercise responsible password management.

The following practices 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 FERPA and State of Washington RCW 28A.604.

No Expectation of 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 and reserves the right to monitor, inspect, copy, review and store without prior notice information about the content and usage of:

A. The network;

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.

No student or staff user should have any expectation of privacy when using the district's network. 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.

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 (staff, students and visitors) 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 – 2022-F1). Violation of any of the conditions of use explained in the district's Electronic Information System (Networks) Individual User Access form (2022-F1) 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.

Date: 06.05.13
Revised: 06.05.15; 10.26.15; 08.29.17