INSTRUCTION

Digital Resources and Internet Safety

These procedures are written to support the Digital Resources Policy of the School Board 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 (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.

Internet access is available to staff and students in the Central Kitsap School District. With this access comes a wealth of opportunities and resources to help students and staff learn, collaborate, innovate and communicate as part of a global online community.

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

Staff members are discouraged from maintaining a job-related presence on a third-party, non-District digital resource. If staff nonetheless elect to do so, staff assume personal responsibility for implementing the same legal and safety standards as the District enforces on its internal resources. Specifically, staff must ensure compliance with the Washington Public Records Act and the District's Management and Retention policy (6570). Additionally, staff shall not discuss individual students in public forums in manner that allows third parties to identify the student(s) in violation of FERPA (Family Education Rights and Privacy Act) or allow the release of non-directory information for any student or directory information for any student with a FERPA letter on file, regardless of the communication tool or provider of the digital resource.

Any staff-created digital forum for student interaction will be conducted in a group not available to the general public (i.e., protected by membership). If the third-party, non-District digital resource includes a limited forum for public comments, the staff member may not edit or remove comments based on viewpoint and the site must include this disclaimer:

> *The District reserves the right to remove inappropriate comments posted on social media it has created or owns and remove comments that are not relevant to the topic of the specific forum. Inappropriate comments include content that has obscene language or sexual content, threatens or defames any person or organization, violates the legal ownership interest of another party, supports or opposes political candidates or ballot propositions, promotes illegal activity, promotes commercial services or products, or that promotes, fosters, or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, status with regard to public assistance, national origin, physical or mental disability, or sexual orientation. The District will not, however, remove otherwise permissible comments based on the user's viewpoint on a topic or issue raised by the District. Any content posted to District-created or owned sites may be subject to public disclosure under the Washington State Public Records Act, ch. 42.56 RCW.*

<u>Disciplinary Action</u>

The District's acceptable use procedures are applicable to all Central Kitsap School District staff and students and refer to all information resources whether individually controlled, student-shared, stand alone, or networked. The administration, teaching staff, or network administrators may request the denial, revocation, or suspension of specific user accounts based upon such user's violation of these acceptable use procedures. Disciplinary action, if any, for students, staff, and other users shall be consistent with the District's standard policies and practices. Where use of external networks is involved, policies governing such use also are applicable and must be adhered to. Violations can constitute cause for revocation of access privileges,

suspension of access to District digital resources, disciplinary action, and/or appropriate legal action. Exact disciplinary measures will be determined on a case-by-case basis and shall be consistent with the District's standard policies and practices.

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.

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 Department of Information Services;

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. 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.

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 that student use conforms to the mission and goals of the district; and

F. The district may monitor student use of the district network, including when accessed on students' personal electronic devices and devices provided by the district.

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 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

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; and

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

Internet Safety Instruction

All students will be educated annually about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response:

A. Age appropriate materials will be made available for use across grade levels; and

B. Training on online safety issues and materials implementation will be made available for administration, staff, and families.

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.

Warranties

The District makes no warranties of any kind, whether expressed or implied, for the Internet service it is providing. The District will attempt to provide error-free and dependable access to technology resources. However, the District cannot be held liable for any information that may be lost, damaged, or unavailable due to technical or other difficulties. The District cannot be held responsible for financial obligations arising from unauthorized use of the Network. The District specifically denies any responsibility for the accuracy or quality of information obtained through its Internet services. Staff and students who make unauthorized and/or inappropriate use of the Internet while using the Network agree to hold the District harmless for the consequences of such use.

The Central Kitsap School District reserves the right to log Internet use and to monitor file server space utilization.

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 periodically and/or as directed by the district;

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).

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. The district reserves the right to monitor, inspect, copy, review, and store, without prior notice, information about the content and usage of:

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.

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.

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 in writing of potential use of any educational application or program to Department of Information Services, including the anticipated purpose of such application or program. Specific expectations of use will be reviewed with students.

Staff should also, as appropriate, provide notice to students' parents/guardians that the staff person has requested that students download or sign up for an application or program, including a brief statement on the purpose of application or program.

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 regularly. Refer to the district retention policy for specific records retention requirements.

Approved: June 14, 1995
Revised: September 19, 1995
Revised: April 8, 1998
Revised: June 28, 2000
Revised: May 23, 2001
Revised: November 26, 2003
Revised: April 29, 2015