INSTRUCTION

Digital Resources

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 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 than face-to-face interactions.

Staff use of non-CKSD Digital Resources

Under Washington state law, employees of the Central Kitsap School District are responsible for their professional code of conduct and obligations as government and school employees whenever they act within their professional capacity. To protect themselves, employees should carefully consider their professional conduct even when using non-CKSD digital resources such as personal cell phones, e-mail accounts, websites and social-networking sites and services. Employees acting in their job capacity should expect that any record created while using non-CKSD digital resources will be subject to disclosure according to the Public Records Act (RCW 42.56). Employees should likewise understand their obligation to report any suspicion of abuse or neglect (per state law) or infraction of school rules (per professional codes of conduct) that arise from communication with students using non-CKSD digital resources. This applies, for example, to student-staff initiated text messages or contacts on Facebook. Employees should refrain from using personal web pages, email accounts, social networks, other electronic or private messaging capabilities of any social media to communicate directly with currently enrolled students.

Staff members who maintain a job-related presence on a third-party, non-District digital resource 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 Public Records Act and the District's Management and Retention policy (6570). Additionally, staff shall not discuss students in public forums or allow the release of non-directory information for any student or directory information for any student with a FERPA (Family Education Rights and Privacy Act) letter on file regardless of the communication tool.

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.

Digital Information Systems (Networks)

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 District's network (Network) must support education and be consistent with the mission of the District.

Acceptable Use

Access to the Internet is provided to support the educational, informational, and research needs of District staff and students and is a privilege, not a right. The use of the Internet must be consistent with the educational objectives of the District and must follow the prescribed acceptable use procedures established by the District. Because Internet use also means using the networks of other organizations, users must also comply with the rules and procedures appropriate for those networks. Actions that may be routinely allowed on one network may be controlled, or even forbidden, on other networks. It is the user's responsibility to abide by the policies and procedures of these other networks.

Staff and students accessing the Internet from a District site are responsible for all online activities that take place through the use of their account. Any violation of the efficient, ethical, and legal utilization of the Internet resources, as determined by the District, may result in termination of the user's Internet account and could jeopardize future access and/or result in disciplinary consequences. District-provided Internet access has not been established as a public access or public forum, and the District has the right to place reasonable restrictions on the material accessed or posted through use of the Network.

Acceptable use by District students and staff of the Network includes:

1. Creation of files, digital media, programs, scripts, web pages and other online content using Network resources in support of education and research;

2. Participation in blogs, wikis, forums, social networks and groups and other online communication platforms that support education and research;
3. 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;
4. Staff use of the Network for incidental personal use in accordance with all District policies and procedures; or
5. Connection of personal electronic devices to the Network, subject to all procedures in this document.

The following are considered examples of unacceptable uses of the Network:

1. Personal pecuniary gain, commercial solicitation and generation of compensation of any kind;
2. Actions that result in liability or material costs incurred by the District;
3. Downloading, installing and use of games, audio files, video files, games or other applications (including shareware or freeware) without permission or approval from the District's Department of Information Services;
4. Support for or opposition to ballot measures, candidates and any other political activity;
5. Tampering with software or hardware, including the introduction of malware;
6. Unauthorized access to other District computers, networks and information systems;
7. Cyberbullying, defamation, harassment of any kind, discriminatory jokes and remarks;
8. Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
9. Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material; or
10. Attaching unauthorized devices to the Network. Any such device will be confiscated and additional disciplinary action may result.
11. Any other action that violates state or federal laws.

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 user's errors or omissions. The District will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the District's Network or the Internet through the Network.

Training

Each District student who receives an Internet account will be part of a required training session with a District staff member pertaining to the proper use of the Internet, the use of District equipment, appropriate use and means of accessing the Internet, Internet policies, and District electronic communications and social networking policies. Each District staff member who has or will receive an Internet account can access the Digital Information System (Network) Policy and these guidelines on the District web site, and is encouraged to avail themselves of classes

on using the Internet as a teaching tool offered by colleges, OESD 114, or District-sponsored workshops.

Disciplinary Action

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 student 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.

Security

Personal information and inappropriate content:

A. Students and staff should not reveal their own personally identifiable 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 personally identifiable information about another individual on any electronic or digital medium without first obtaining consent from that individual's parent/guardian;
C. Students and staff shall not discuss specific, identifiable students in public forums or allow the release of non-directory information for any student or directory information for any student with a FERPA (Family Education Rights and Privacy Act) letter on file. Any staff-created digital forum for student interaction will be conducted in a group not available for 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 the disclaimer listed previously in this Procedure; and
D. If students or staff encounter dangerous or inappropriate content or experience or witness cyberbullying while accessing the Network, they are expected to 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.

1. Filtering software, including spam filters, 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;
2. 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);
3. The District will employ a spam filter to block undesirable email from District mailboxes.
4. Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.
5. 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.

Internet Safety Instruction

All students will be educated about appropriate online behavior, including interacting with other individuals on social networks, chat rooms, or other virtual communities, and cyberbullying awareness and response.

1. Age appropriate materials will be made available for use across grade levels.
2. Training on online safety issues and materials implementation will be made available for administration, staff and families.

Copyright

In order to protect intellectual property rights and the continued availability of Network access, Central Kitsap School District Internet users shall adhere to the District Copyright Policy/Procedure 2205/2205P. All communications and information accessible via the Internet should be assumed to be private property with the corresponding copyright. Computer software, including games and music (MP3s), protected under the copyright laws will not be obtained or transmitted via the Network, nor will it be stored on any District computers without the express written permission of the copyright owner and District permission. Non-copy protected audio and video files for personal use should not be stored on the Network. Staff can install legally obtained and/or original software that supports the educational, informational, and research needs of Central Kitsap School District on their desktop hard drive with the understanding that:

1. If something goes wrong, the computer will be restored to its original state and user-installed programs will be lost.
2. Periodically it is necessary for technology staff to reconfigure computers, and individually installed software will be lost and will need to be reinstalled by the user.

Viruses and Other Malicious Software
All files to be downloaded to a District computer or brought from home have the potential for being infected with a computer virus or other malicious software and, therefore, must be scanned.

Privacy
Routine maintenance and monitoring of the Network may lead to discovery that a user has violated the law or a District rule. Staff and students should be aware that what they do on the District electronic systems, including the Internet, is not private and that they should have no expectation of privacy while using the Network.

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.

E-Mail
The use of District e-mail by staff and students must be consistent with the educational and informational needs of the District and with all applicable District policies and procedures.

Internet Access
To gain access to the Internet, students age 17 years and under must have the written permission of their parents.

Electronic Communications
Acceptable Use Procedures/Guidelines
1. All forms of electronic data (e-mail, information shared via social network messages, SMS and MMS messages, all computer documents and files, faxes, and voice mail) regarding the business of the District are considered public records, regardless of the ownership of the equipment used to create it, and will therefore be subject to disclosure upon request under the Public Records Act (RCW 42.56) or through a lawsuit against the District or any District employees. Staff members who maintain a job-related presence on a third-party, non-District digital resource 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 Public Records Act by

periodically archiving the site's content and associated metadata. They will be accountable for searching the archive and producing applicable records when requested by the District pursuant to a lawful request, and authorizing the District to do so directly.

2. All electronic communications sent or received through the Network must meet the same standards of integrity, professionalism and consideration expected of staff and students in all face-to-face interactions and comply with state and federal laws.

3. Equipment owned by and software licensed to the District or third- party applications or networks used for the business of the District shall not be used to communicate:
   a. Messages that promote or oppose a ballot measure or candidate for political office, except as part of the bargaining agreement with the District.
   b. Messages that promote or oppose a religion.
   c. Messages that promote a commercial venture or the sale, lease, trade, or other transfer of goods or services for value on behalf of a commercial venture.

4. District e-mail or other electronic communications platforms used to conduct District business may not be used for any purpose that violates federal law, state laws, District Policy or District Procedure.

5. It is permissible for staff to use e-mail or social media for incidental personal purposes that do not require substantial expenditures of time, but such use remains subject to the conditions and expectations set forth in these procedures and all related policies and procedures.

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