

2022P: Electronic Resources

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 than face-to-face interactions.

The District expects everyone to exercise good judgment and use the computer equipment in a professional manner. Your use of the equipment is expected to be related to the District's goals of educating students and/or conducting District business. The District recognizes, however, that some personal use is inevitable, and that incidental and occasional personal use that is infrequent or brief in duration is permitted so long as it occurs on personal time, does not interfere with District business, and is not otherwise prohibited by District policy and procedures.

General Network Use

The district network includes wired and wireless computers and peripheral equipment, files and storage, e-mail, and access to internet resources (websites, online communities, social networking sites, blogs, web mail, wikis, etc.). The district reserves the right to prioritize the use of, and access to, the network.

- District reserves the right to prioritize use and access to the system.
- All use of the system must be in support of education and research and consistent with the mission of the district.
- Any use of the system must be in conformity to state and federal law, and district policy.
- No use of the system shall serve to disrupt the operation of the system by others; system components including hardware or software shall not be destroyed, modified, or abused in any way.
- No procedure is intended to preclude the supervised use of the network while under the direction of a teacher or other approved user, and acting in conformity to district policy.
- Violation of any of the conditions of use may be cause for disciplinary action.
- Requests for exceptions to the procedures must be made to the technology department at least seven (7) days prior to the need.

Acceptable network use by district students and staff includes:

- Creation of content, files, projects, videos, web pages, etc., and using network resources in support of educational research;
- Participation in blogs, wikis, bulletin boards, and social networking sites;
- 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;
- Staff use of the network for incidental personal use in accordance with all district policies and guidelines;
- Connection of personally owned devices to the district's wireless network after checking with the technology department to confirm that the devices is equipped with up-to-date anti-virus software, security patches, and is configured properly.

Connection of any personal electronic device is subject to all guidelines in this document.

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

- Personal gain, commercial solicitation and compensation of any kind;
- Liability or cost incurred by the district;
- Downloading, installing and using games, audio files, video files, or other applications (including shareware or freeware) without permission or approval from the technology department;
- Support or opposition for ballot measures, candidates and any other political activity;
- Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software and monitoring tools;
- Unauthorized access to other district computers, networks and information systems;
- Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;
- 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;
- Physically connecting unauthorized, non-district owned equipment or devices to district equipment or the district network. Any such equipment will be confiscated; and
- Bringing any device to school (whether or not the device is used) which contains inappropriate content, data, or applications. Any such device will be confiscated.

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 its 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 Safety

Personal Information and Inappropriate Content:

- Students and staff should not reveal personal information [including a home address, phone number, or password(s)] on websites, blogs, videos, wikis, e-mail, or as content on any other electronic medium.
- Students and staff should not reveal personal information about another individual on any electronic medium.
- No student pictures or names can be published on any class, school, or district website unless the appropriate permission has been verified according to district policy.
- If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

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 are permitted when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

All student work is copyrighted. Permission to publish any student work requires permission from the parent or guardian.

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.

- Filtering software is not 100% 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 or her use of the network and Internet and avoid objectionable sites;
- Any attempts to defeat or bypass the district's Internet filter or conceal Internet activity are prohibited: proxies, https, special ports, modifications to district browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content;
- E-mail inconsistent with the educational and research mission of the district will be considered SPAM and blocked from entering district e-mail boxes;
- 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 computers;
- 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
- Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.

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:

- Change passwords according to district policy;
- Do not use another user's account;
- Do not insert passwords into e-mail or other communications;
- Do not use the "remember password" feature of Internet browsers; and
- Keep operating systems updated and patched;
- Keep anti-virus and security software updated; and
- 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:

- The network;
- User files and disk space utilization;

- User applications and bandwidth utilization;
- User document files, folders and electronic communications; e-mail;
- Internet access; and
- 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 nightly – Monday through Friday. 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 acceptable use 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.

Date: May 2005
Revised: June 2009
Revised: September 2010
Camas School District

2022P: Electronic Resources – ADDENDUM

STUDENT USE OF PERSONAL COMPUTING DEVICES AT CAMAS SCHOOL DISTRICT

Beginning in the fall of 2011, Camas School District students will be allowed to access the wireless network with their personally owned computing devices (PCDs). A personal computing device is defined as an electronic communication device capable of internet access, word processing and other school-related applications. These could include the following: laptop, net book or tablet computer, e-reader or any other personal computing device that may be stand-alone or may use wireless communications between users across some form of telecommunications network.

The use of personal computing devices on campus is a privilege which the District grants to any student who is willing to assume the responsibility of abiding by the guidelines set forth in this document. This is an addendum to the District's Acceptable Use Policy (AUP), defined under Procedure 2022, and does not replace that document in any way. All policies set in place in the AUP continue to apply when the student uses their personal computing devices on campus.

Management and Supervision of Personal Computing Devices

There will be no expectation that students will be required to bring personal computing devices to school.

The Camas School District assumes no responsibility or financial liability for any damage the student or parent suffers, including but not limited to theft, physical damage, loss of data, or software malfunctions of the personal computing device. If a personal computing device appears to have been stolen, the student will immediately report the incident to school administration.

Permission for using and charging of the personal computing devices in any instructional area, including but not limited to classrooms, will be at the sole discretion of the supervising adult and/or classroom teacher and school administration.

Use of personal computing devices in designated common areas will be allowed but subject to the restrictions stated in the district policies and by school administration. If a student appears to be in violation of any district policy, staff members should refer the student to a school administrator.

Appropriate Use

Use of these devices in the school setting may be approved on a limited basis. Students are to use these devices in a responsible, efficient, ethical and legal manner for educational purposes only. School policy will further define acceptable use of the PCDs. The teacher/administration reserves the right to determine if a student's use of a personal computing device is inappropriate and/or disrupts the learning environment and may take appropriate disciplinary action, including but not limited to confiscation of the device, which will be returned to the student and/or parent(s)/guardian(s) in accordance with established building guidelines. In order to insure adequate bandwidth, students may only use PCDs for educational purposes and not recreational use.

Students may only connect PCDs to the specific wireless network. This network will provide access to the Internet, including all publicly available CSD resources. Connecting a PCD to a wired network, or any other available CSD wireless network is prohibited. Student use of the District's wireless network is bound by the District's Acceptable Use Policy (Procedure 2022).

If a student is suspected of violating the terms of the Acceptable Use Policy, the building administrator will determine the appropriate course of action, including but not limited to

- o Revoking PCD Internet connectivity for the student
 - o Searching the electronic device and the records on student technology equipment in accordance with Search or Seizure Policy and maintaining safety, order, and discipline. (Regulation 3230)
 - o Prohibiting the PCD from being brought on campus
 - o Prohibiting PCD use in specific locations or settings
 - o Assigning standard disciplinary consequences as listed in the Student Handbook
-
-

Timeline:

July 24, 2011

Board approval for bid

September 13, 2011

Tech Committee review of draft procedure addendum and FAQ

September 26, 2011

CHS Tech Committee review of draft procedure addendum and FAQ

October 10, 2011

Board review of draft procedure addendum and FAQ

October 24, 2011

Procedure 2022 Addendum brought to Board for consideration and approved

October 31, 2011

Implementation of Student Use of Personal Computing Devices