

For your own protection and understanding, please read completely through this document before choosing your action.

Staff use of non-ISD digital resources

Under Washington state law, employees of the Issaquah School District are liable for their professional code of conduct and obligations as government and school employees *whenever they act within their job capacity*. To protect themselves, employees should carefully consider these implications even when using non-ISD 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 produced while using non-ISD 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-ISD digital resources. This applies, for example, to staff-student text messages or interactions on Facebook.

To ensure compliance with the law and protect students and staff, the District has established a secure, archived, searchable Internet platform—Issaquah Connect—that employees are encouraged to use to maintain any job-related Web presence. In the event staff chooses to act within their job capacity by using third-party, non-District digital resources, the District will *not* be able to provide support. Examples include social media sites such as Facebook and Twitter, non-District Web sites and text messages. 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) by archiving the site's content and metadata and certifying that they are maintaining such an archive at least annually with their supervisor. They will be accountable for searching the archive and producing applicable records when requested by the District. Additionally, staff using third-party, non-District digital resources 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. Any staff-created 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 this disclaimer:

The Issaquah School District reserves the right to remove any user-generated content it deems inappropriate or not relevant to the topic of the forum. This includes language 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 is not topically related to the particular posting, or contains contents that promote, foster, or perpetuate 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 viewpoint. Any content posted to this site may be subject to public disclosure under the Washington State Public Records Act, ch. 42.56 RCW.

Network

The Issaquah School District network includes wired and wireless computers and peripheral equipment, files and storage, e-mail and Internet content (Connect, Moodle, social media sites, blogs, web sites, web mail, web groups, wikis, etc.). The District reserves the right to prioritize the use of, and access to, the wired and wireless networks.

Use of the networks must support education and research and be consistent with the mission of the District.

The Issaquah School District wireless network is designed as a convenience for students and employees. Use of the wireless network is governed by Policy 2022 and its procedures. The resources of the wireless network are limited. Users must exercise prudence in the shared use of the wireless network.

Acceptable wired and wireless network use by District students and staff includes:

- Creating files, projects, videos, web pages and podcasts using network resources in support of educational research;
- Participating in blogs, wikis, bulletin boards, social media sites, Connect, Moodle, web groups and the creation of content for podcasts, e-mail and web pages that support educational research;
- With parental permission, publishing original educational material online, curriculum related materials and student work including on Connect and Moodle. Sources outside the classroom or school must be cited appropriately;
- Using the wired and wireless networks by staff for incidental personal use in accordance with all District policies and guidelines and the Children's Internet Protection Act;
- Connecting of staff personal laptops to the District network after checking with Executive Director of Educational Technology or designee to confirm that the laptop is equipped with up-to-date district virus software and is configured properly. Connection of any personal electronic device is subject to this Policy.

Unacceptable wired or wireless network use by District students and staff includes but is not limited to:

- Using either network for personal gain, commercial solicitation and compensation of any kind, including using or knowingly allowing another user to use any computer, computer network, computer system, program, or software to devise or execute a scheme to defraud or to obtain money, property, services, or other things of value by false pretenses, promises or representations;
- Creating liability or cost to the District;
- Downloading, installation and use of games, audio files, video files or other applications (including shareware or freeware) without permission or approval from the Executive Director of Educational Technology or designee;
- Supporting or opposing ballot measures, candidates and any other political activity;
- Distributing of unsolicited advertising, hacking, cracking, vandalizing, the introduction and or propagation of computer viruses, worms, Trojan horses, time bombs and changes to hardware, software, and monitoring tools, distributing quantities of

information that overwhelm a system (including “chain letters,” “network games,” or “broadcasting” messages);

- Using either network to make unauthorized access to other District computers, networks and information systems, or any other resource via the networks;
- Attempting to harm, destroy, or interfere with the proper operation of computing hardware, operating systems, application software or data;
- Invading the privacy of individuals or entities (e.g., use of someone else’s handle or account) or misrepresenting other users on the wired and/or wireless network.
- Cyberbullying, hate mail, defamation, illegal, harassing, inappropriate, or obscene purposes or in support of such activities, including discriminatory jokes, remarks, posts, files, or comments on social media sites, Connect, or Moodle. This is determined solely by the District and the District reserves the right to remove any user generated content from sites it owns at any time;
- Submitting, publishing, displaying, or forwarding any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or messages;
- Seeking to gain or gaining unauthorized access to information resources, obtaining copies of, or modifying files or other data, or gaining and communicating passwords belonging to other wired and/or wireless network users;
- Posting information sent or stored online that could endanger others (e.g., bomb construction, drug manufacture). The District reserves the right to remove any user generated content from sites it owns at any time;
- Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material, as determined at the District’s sole discretion;
- Attaching unauthorized equipment to the District’s wired and/or wireless networks. Any such equipment will be confiscated and destroyed.
- Using a personal device enabled as a wireless access point in violation of the federal law Children’s Internet Protection Act (CIPA)

The District reserves the right, subject to applicable law, to disconnect and check any electronic device of involvement in a violation of Policy 2022 or any other District policy that may apply. A violation may result in account deactivation and additional disciplinary action.

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 wired and/or wireless networks or the Internet. All users agree to defend, indemnify and hold the District harmless from and against all liabilities, damages, losses and costs (including but not limited to fees of attorneys and technology consultants) arising out of or relating to any claim by a third party relating in any way to their violation of this policy.

Internet Safety

All district schools will provide yearly education for all students in appropriate online behavior on social networking sites, blogs, forums, wikis, chat rooms, and other online

venues. In addition each school will educate students on being aware of cyberbullying awareness and how to respond to it.

Annually each school will certify completion of Internet Safety Training by e-mail confirmation to the Executive Director of Educational Technology no later than March 1.

Personal Information and Inappropriate Content

- Students shall treat their personally identifiable information and that of others in all wired and/or wireless network communications as confidential. Personally identifiable information is defined as complete names, addresses, telephone numbers, and identifiable photos. This includes postings on Connect, Moodle, social media sites, web sites, blogs, podcasts, 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 web site, Connect, or Moodle unless the appropriate permission has been verified according to District policy.
- No user shall disclose, use, or disseminate personally identifying information regarding minors without authorization.
- 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. The District may determine all functionality, features and access, may block or filter any information (including but not limited to Internet sites or emails), and may, in its sole discretion, restrict, suspend, revoke or otherwise limit use privileges.

- 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 and are considered a violation of this policy: 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.

Copyright

Use of the District wired and wireless networks must be in compliance with all copyright law.

Violation of such matters as institutional or third-party copyright, license agreements, or other contracts is prohibited. The unauthorized use of and/or copying of software is illegal and prohibited. The unauthorized installation, use, storage, or distribution of copyrighted software or materials over or on the wired or wireless Network is prohibited.

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. Any copyrighted material posed on Connect or Moodle or any other District owned sites will be removed immediately. 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.

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.

These 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;
- If you write down your account password, keep it out of sight;
- Do not store passwords in a file without encryption;
- Do not use the "remember password" feature of Internet browsers; 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 Education Rights and Privacy Act (FERPA).

No Expectation of Privacy

The District provides the network system, e-mail, Connect, Moodle, and Internet access as a tool for education and research in support of the District's mission. All content on the network system, e-mail, Connect, and Moodle belongs to the District.

Issaquah School District Staff User Release Form

Instruction
2022 F3
6/6

No student or staff user should have any expectation of privacy when using the District's wired or wireless networks. While limited personal use of the wired and wireless networks is permitted, users acknowledge that such information and usage is not private, is subject to review and monitoring, must be limited and not interfere with the performance of the District's mission, and must comply with this Policy. The District reserves the right to monitor, intercept, retrieve and otherwise use and disclose, all access, use, transmissions, communications (including content) and information ever in or passing through the wired or wireless network, with or without the consent of the user. This includes but is not limited to all uses by students and employees. It also includes (without limitation) use of software to log, analyze and document any aspect of the wired or wireless networks, including (without limitation) uses and transmissions. The District, law enforcement and others may receive reports of monitoring and discipline or legal actions may be based upon it, including (without limitation) termination of access, employment or enrollment. The District also reserves the right to disclose monitoring information for other lawful purposes.

All files 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 and Web-based records 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. A complete archive of Issaquah Connect is made every 24 hours and will be stored to preserve a full, two-year archive of Issaquah Connect content.

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 Consent Form.

Violation of any of the conditions of use explained in the User Consent Form, Electronic Resources Policy or in these procedures by students could be cause for disciplinary action, including suspension or expulsion from school and suspension or revocation of network and computer access privileges.

Violation of any of the conditions of use explained in the User Consent Form, Electronic Resources Policy or these procedures by District employees could be cause for disciplinary action up to and including termination of employment.

Printed Staff Name _____

Date _____

Staff Signature _____

Current Site _____

Formerly: Policy 2314 F

Revised: 09.13.10; 07.16.11; 10.31.11