Tumwater School District
Procedures

ELECTRONIC RESOURCES

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.

All use of the network must support education and research consistent with the mission of the district and conform to state and federal law, network provider policies, licenses and district policy.

By use or accessing of the Tumwater School District network all individuals agrees that upon such use or access to abide by the policies and procedures in this document as well as to abide by all of the other policies and procedures of the Tumwater School District.

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.

Every effort must be made to conserve network resources. For example, users should frequently delete unused files from home and shared directories.

Staff may use the network for incidental personal use in accordance with all district policies and procedures.

No Expectation of Privacy

The district provides the network system, e-mail and Internet access exclusively as a tool for education and research in support of the district's mission. The district reserves the right to monitor, inspect, copy, review, modify, delete and store data without prior notice including the content and usage of:

1. The network;
2. User files and disk space utilization;
3. User applications and bandwidth utilization;
4. User document files, folders and electronic communications;
5. E-mail;

6. Internet access; and
7. 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.

Student Data is Confidential

District staff must maintain the confidentiality of student data in accordance with district policy and the Family Educational Rights and Privacy Act (FERPA).

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

1. Personal gain, commercial solicitation and compensation of any kind;
2. Actions that result in liability or cost incurred by the district;
3. Downloading, installing and use of non-educational games, audio files, video files or other applications (including shareware or freeware) without permission or approval from the district Technology Department;
4. Support for or opposition to ballot measures, candidates and any other political activity;
5. Use of the network for charitable purposes unless pre-approved by the superintendent or his/her designee;
6. Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software and monitoring tools;
7. Disabling or removing of installed firewalls, virus scanners, and other attack detection software is strictly prohibited unless prior approval is given by the district Technology Department;
8. Unauthorized access to other district computers, networks and information systems;
9. Cyber bullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;
10. Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
11. Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material;
12. System components including hardware or software will not be destroyed, removed, modified, and/or installed, without the approval of the district Technology Department; and
13. Attaching unauthorized devices to the district enterprise 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.

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:

1. Users shall change passwords regularly and avoid easily guessed passwords;
2. Do not use another user's account;
3. Do not insert passwords into e-mail or other communications;
4. If you write down your user account password, keep it in a secure location;
5. Do not use the "remember password" feature of Internet browsers; and
6. Lock the screen or log off if leaving the computer.

Use of Personal Electronic Devices

While in accordance with all district policies and procedures, students and staff may use personal electronic devices to further the educational and research mission of the district. Public network access is available at schools with Wi-Fi deployments for personal electronic devices. Use of the public network must also be in accordance to district policy and procedures.

Connection of personal electronic devices (wired or wireless) including portable devices with network capabilities to the district private enterprise network is permitted only after approval by the district Technology Department to confirm that the device is equipped with up-to-date virus software, compatible network card and is configured properly.

The district Technology Department will retain the final authority in deciding when and how students and may use personal electronic devices on school grounds and during the school day.

Internet Safety

Personal Information and Inappropriate Content:

1. Students and staff shall 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;
2. Students and staff shall not reveal personal information about another individual on any electronic medium without first obtaining permission;
3. Photographs of students are considered "directory information" and maybe used in district publications or on the website. Parents who did not wish photographs that include their children to be published may request in writing to their school office;
4. Student work maybe electronically posted with parent and student permission;

5. The district will provide education to students regarding appropriate on-line behavior in accordance with the Children’s Internet Protection Act. Education will be coordinated through the Media Specialist at each school site; and
6. If students encounter dangerous or inappropriate information or messages, they shall 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 district decision.

1. 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;
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. Communications may not be encrypted as to avoid security review.
4. E-mail inconsistent with the educational and research mission of the district could be considered SPAM and blocked from entering district e-mail boxes;
5. 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
6. Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.

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.

Purchasing

The purchasing and/or installation of all software and hardware for use on the district network must be approved and processed through the district Technology Department.

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.

Disciplinary Action

All users of the district's electronic resources are required to comply with the district's policy and procedures. Violation of policies and procedures could be cause for disciplinary action or legal action.

ADOPTED: January, 2005
REVISED: January 26, 2012; March 27, 2014