OSDNET ACCEPTABLE USE PROCEDURES

These procedures are written to support Policy 2022, Electronic Resources, and to promote positive and effective digital citizenship among students. 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 behavior online are no different than face-to-face interactions.

NETWORK USE

1) The District's electronic network (OSDNet) includes wired and wireless computers and peripheral equipment, files and storage, e-mail and internet content (blogs, web sites, web mail, web groups, Moodle, wikis, etc.). The District reserves the right to prioritize the use of, and access to, the network.
2) All use of the network must support education and research and be consistent with the mission of the District.
3) Access to this network includes the services provided to the District by the Washington State K-20 Educational Network to access public networks such as the internet. **All students will be provided access** to OSDNet services, including the internet, unless the parent/legal guardian notifies the District by contacting their school principal by the last school day in September, or within ten days of enrollment, that they do not wish their child to have access.
4) **Acceptable network use** by District students includes:
    a. Creation of files, projects, videos, web pages and podcasts using network resources in support of educational research;
    b. Participation in blogs, wikis, bulletin boards, social networking sites and groups, and the creation of content for podcasts, e-mail and web pages that support educational 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;
5) **Unacceptable network use** by District students includes but is not limited to:
    a. Personal gain, commercial solicitation and compensation of any kind;
    b. Liability or cost incurred by the District;
    c. Support or opposition for ballot measures, candidates and any other political activity;
    d. Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software, and monitoring tools;
    e. Unauthorized access to other District computers, networks and information systems;
    f. Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks, posts, files or comments on social media sites. The District reserves the right to remove any user-generated content from its sites at any time.

g. Information posted, 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 its sites at any time.
h. Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material; and
i. Attaching unauthorized equipment to the District network. Any such equipment will be confiscated and destroyed.

6) 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, misdeliveries 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

1) Students should not reveal personal information, including a home address and phone number, on web sites, blogs, podcasts, videos, wikis, email or as content on any other electronic medium.
2) Students should not reveal personal information about another individual on any electronic medium.
3) No student pictures or names can be published on any class, school or District web site unless the appropriate permission has been verified according to District policy.
4) 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). The District will determine and set levels of filtering for other objectionable materials.

1) Filtering software is not 100% effective. While filters make it more difficult for objectionable material to be received or accessed; filters are not a complete solution. Every user must take responsibility for his or 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 including 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) E-mail inconsistent with the educational and research mission of the District will be considered SPAM and blocked from entering District e-mail boxes;
4) 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;

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 users of OSDNet shall comply with current copyright laws and Policy 2025, Copyright Compliance.

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

NETWORK SECURITY AND PRIVACY

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 are responsible for all activity on their account and must not share their account password.

These procedures are designed to safeguard network user accounts:

1) Change passwords according to District policy;
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 account password, keep it out of sight;
5) Do not store passwords in a file without encryption;
6) Do not use the "remember password" feature of Internet browsers; and
7) Lock the screen, or log off, if leaving the computer.

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:

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 user should have any expectation of privacy when using the District's network. The District reserves the right to disclose any electronic message 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, student files are backed up on District servers nightly – Monday through Friday.

DISCIPLINARY ACTION

All users of the District's electronic resources are required to comply with the District's policy and procedures.

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

USERS RIGHT TO APPEAL

A user of OSDNet services who has violated his/her agreement to follow the OSDNet Acceptable Use Procedures and has been subjected to disciplinary action may appeal his/her case to: (1) the building's administrator, (2) the District Technology Director and/or (3) the Board of Directors.

PROCEDURE ESTABLISHED	*February 28, 1996*
REVISED	*June 12, 2002*
REVISED	*May 12, 2003*
REVISED	*June 24, 2008*
REVISED	*February 28, 2011*