OSDNET/TELECOMMUNICATION SYSTEMS ACCEPTABLE USE PROCEDURES

These procedures are written to support Policy 5254, Electronic Information Systems (Networks), and to provide staff with acceptable and appropriate usage guidelines for telecommunication and electronic network use. These procedures are intended to support the education of students. Violation of these procedures may be cause for disciplinary action, up to and including termination of employment.

NETWORK AND TELECOMMUNICATION USE

1) The District's electronic network (OSDNet) and telecommunication systems 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.), and all telecommunication devices (two-way radios, cell phones, wired phones, long distance capabilities, etc). The District reserves the right to prioritize the use of, and access to, these services.

2) Use of these services must support education and be consistent with the mission of the District.

3) **Acceptable use** by District staff includes:
   a. Creation of files, projects, videos, web pages and podcasts using network resources in support of District mission;
   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 District mission;
   c. The online publication of original educational material, curriculum related materials and student work with appropriate permissions. Sources outside the classroom or school must be cited appropriately; and
   d. Use for incidental personal use in accordance with all District policies and guidelines.

4) **Unacceptable use** by District staff 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. Disruption or damage of systems or changes to hardware, software, or monitoring tools;
   e. Unauthorized access to other District computers, networks and information systems;
   f. Harassing or discriminatory behavior of any kind;
   g. Information posted, sent or stored online that does not support the District mission;
   h. Accessing, uploading, downloading, storage and distribution of criminal, illegal, obscene, pornographic or sexually explicit material; and,
   i. Attaching unauthorized equipment to District network services. Any such equipment will be confiscated.

5) 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. 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.

6) The District reserves the right to remove any user-generated content from its sites at any time.

STAFF USE OF NON-OSD DIGITAL RESOURCES

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

To support compliance with the law and protect students and staff, the District has established a web page system (WebManager) 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, non-District web sites and text messages. Staff members who maintain a job-related presence on a third-party, non-District digital resources 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 archiving the site's content and metadata and certifying that they are maintaining such an archive at least annually with their supervisor and 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 Olympia 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 criminal, obscene 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.

INTERNET SAFETY: PERSONAL INFORMATION AND INAPPROPRIATE CONTENT

1) Staff should not reveal personal information, including a home address and phone number, on web sites, blogs, podcasts, videos, wikis, e-mail or as content on any other electronic medium.
2) Staff 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 staff members encounter dangerous or inappropriate information or messages, they should notify their supervisor or other appropriate District authority.

FILTERING AND MONITORING

Filtering software is used to block or filter access to obscene and/or criminal sites, including all access to 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) Every user will be held accountable for their use of the network and Internet and must avoid objectionable sites regardless of District implemented filtering;
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 mission of the district may be considered SPAM and blocked from entering district e-mail boxes;
4) The district expects appropriate adult supervision of Internet use by students;
5) Staff members who supervise students, control electronic equipment or have occasion to observe student use of said equipment online, must monitor the use of this equipment to assure that student use conforms to the mission and goals of the district; and
6) Staff must maintain an appropriate level of familiarity with the Internet to monitor, instruct and assist effectively and maintain student safety.

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

Practices that safeguard network user accounts include:

1) Changing passwords only according to District policy;
2) Never sharing your login information with others;
3) Never inserting passwords into e-mail or other communications;
4) Protecting written documentation of your account password;
5) Storing passwords in a file with encryption;
6) Limiting use of the "remember password" feature of internet browsers; and,
7) Locking the screen, or logging 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 telecommunication systems, network systems, e-mail and internet access as a tool for education 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 telecommunication equipment, network and e-mail use.

No staff user should have any expectation of privacy when using the District's network or other resources. 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. Staff and student files are backed up on District servers.

DISCIPLINARY ACTION

All users of the District's electronic, telecommunication and other resources are required to comply with the Policy 5254 and these procedures. Violation of any of the conditions of use 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 OSDNet User Agreement 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, 2011
REVIEWED.......................................September 12, 2011

OLYMPIA SCHOOL DISTRICT NETWORK (OSDNET)
USER AGREEMENT FORM

The Olympia School District Network (OSDNet) includes local area network services such as printing and file sharing, and the services provided by the District's service providers to access public networks such as the Internet. This network and the District's technology will enable educators and students to communicate, learn, share, collaborate and create, to think and solve problems, and to manage their work.

As a condition of my right to use OSDNet services, I understand and agree to abide by the OSDNet Acceptable Use Procedures.

_____

Last Name   First Name   Middle Initial

_____

School/Site   Preferred Password
                                     (6 character minimum, 8 character maximum)

_____

                                     Signature of User   Date