

# OSDNET ACCEPTABLE USE PROCEDURES

The Olympia School District has implemented an electronic communications network (OSDNet) that allows opportunities for students to communicate, learn, access and publish information. OSDNet includes the services provided by the district's service providers (K20 Education Network) to access public networks such as the Internet. **All students will be provided access to OSDNet services including the Internet unless parent/legal guardian notifies the district, by contacting their building principal by the last day of September or within ten days of enrollment, that they do not wish their child to have access.**

Successful operation of the network requires that all users to conduct themselves in a responsible, lawful, ethical and polite manner while using the network. The user is ultimately responsible for his/her actions while accessing network services. As a condition for the privilege of using OSDNet services, all users will abide by the procedures listed within this policy. These procedures include, but are not limited to, the following:

## PROCEDURES

### NETWORK USE

- 1) Use of the system will primarily be in support of education and research and consistent with the mission of the district. The District reserves the right to prioritize use and access to the system.
- 2) Any personal use of OSDNet resources will be at no cost to the District, must not interfere with the performance of official duties, must be brief in duration, and must not disrupt the conduct of District business.
- 3) Use of the system must be in conformity to state and federal law, K-20 Network policies and licenses, and District policies.
- 4) Malicious use of the system to harass or bully other users or gain unauthorized access to an entity on the system and/or damage the components of an entity on the network is prohibited.
- 5) Users are responsible for the appropriateness and content of material they transmit or publish on the system. Hate mail, harassment, cyber bullying, discriminatory remarks, or other antisocial behaviors are expressly prohibited.
- 6) Use of the system to access, store or distribute inappropriate, obscene or pornographic material is prohibited.
- 7) Use of the system for commercial purposes is prohibited. Use of the system for charitable purposes must be approved in advance by the Superintendent or designee.
- 8) The system constitutes public facilities and may not be used to support or oppose political candidates or ballot measures.
- 9) No use of the system will be permitted to disrupt the operation of the system by others or compromise the security or integrity of District information or software; system components including hardware or software may not be destroyed, modified or abused in any way.

### SECURITY

- 1) System accounts are to be used only by the authorized owner of the account for the authorized purpose. Users must not share their account access or password with another person or leave an open file or session unattended or unsupervised. Account owners are ultimately responsible for all activity under their account.
- 2) Users must not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the system, or attempt to gain unauthorized access to any entity on the K-20 Network system.
- 3) Communications may not be encrypted so as to avoid security review.

- 4) Users should change passwords regularly and avoid easily guessed passwords.

### **PERSONAL SECURITY**

- 1) Personal information such as addresses and telephone numbers should remain confidential when communicating on the system. Students should never reveal such information without permission from their teacher or other adult. No user may disclose, use or disseminate personal identification information regarding minors without authorization.
- 2) Students should never make appointments to meet people in person that they have contacted on the system without District and parent permission.
- 3) Students should notify their teacher or other adult whenever they come across information or messages that are dangerous, inappropriate or make them feel uncomfortable while using any OSDNet services

### **COPYRIGHT**

The unauthorized installation, use, storage or distribution of copyrighted software or materials on District computers is prohibited. All users of OSDNet will comply with current copyright laws and Board Policy 2025, Copyright Compliance.

### **FILTERING AND MONITORING**

- 1) Filtering services are in use for all computers with access to the Internet for all users. These services will block or filter access to visual depictions that are obscene, child pornography, or harmful to minors.
- 2) Educational staff will, to the best of their ability, student's use of the Internet in school, and will take reasonable measures to prevent access to inappropriate material on the Internet.

### **GENERAL USE**

- 1) Use of instructional software, including computer-based games, must be approved by the Technology Department and must be in support of District learning goals. All other computer-based games are prohibited.
- 2) Diligent effort must be made to conserve system resources. For example, users should frequently delete e-mail and unused files, and users should promptly disconnect videoconferences upon completion.
- 3) Nothing in these regulations is intended to preclude the supervised use of the system while under the direction of a teacher or other approved user acting in conformity with District policy and procedures.

**Violation of any of the conditions of use may be cause for disciplinary action.**

### **DISTRICT RIGHTS**

#### **OLYMPIA SCHOOL DISTRICT RESERVES THE RIGHT TO:**

- 1) Monitor all activity of OSDNet.
- 2) Review any materials stored in OSDNet files and to edit or remove any material that district administrators believe may be unlawful, obscene, abusive, or otherwise objectionable.

- 3) Determine whether specific uses of the network are consistent with these Acceptable Use Procedures.
- 4) Log network use and monitor storage disk space utilization by users.
- 5) Determine what is appropriate use.
- 6) Remove a user's access to the network at any time it is determined that the user is engaged in unauthorized activity or violating these Acceptable Use Procedures.
- 7) Cooperate fully with any investigation concerning or relating to any OSDNet activity.
- 8) Prioritize use and access to the system.
- 9) Modify and review the Acceptable Use Procedures.

#### **DISTRICT RESPONSIBILITIES/LIMITATIONS**

- 1) The District will take prudent steps to develop, implement and maintain security procedures to insure the integrity of individual and District files. The District will not guarantee that information on any computer system will be inaccessible by other users.
- 2) The District will attempt to provide error free and dependable access to technology resources associated with OSDNet. The District will not be held liable for any information that may be lost, damaged or unavailable due to technical or other difficulties.
- 3) The District will not deny or remove a user's right to use OSDNet resources without just cause.

#### **USER'S RIGHT TO APPEAL**

A user of OSDNet services who has violated the 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 District Board of Directors.

---