



**Technology Usage Policies:** The following policies apply to all grade levels.

Students are encouraged to use the school's computers/network and the Internet connection for teacher-assigned, educational work. This policy covers all electronic devices, whether personal or school owned, that is used on school property, including on district-owned vehicles or during district sponsored trips.

Students using computers are expected to abide by the following rules:

1. Students may only access the district network and/or Internet by using their assigned network account. Use of another person's account/password is prohibited. Students may not allow other users to utilize their passwords. Students may not intentionally seek information on, obtain copies of or modify files, data or passwords belonging to other users or misrepresent other users on the network.
2. Students are permitted to use networked software and school-supplied software. Programs written by the student, which are part of an assignment in a school's course of study, may be run, as required, for that course of study's requirements with teacher supervision.
3. Students may not download programs from the Internet nor may they copy programs from any removable device or other outside media. Students may not install or delete programs on the school's computers.
4. Students may not use the Internet to engage in "hacking" or other unlawful activities.
5. Students may not create keyboard macros in Microsoft Word or any other program. Macros written by the student which are part of an assignment in a school's course of study may be run, as required, for that course of study's requirements with teacher supervision.
6. Students should only use computer programs approved by the classroom teacher.
7. The school staff may review computer files or messages that are created by the student. Material may be reviewed for grading and appropriate content. It may be reviewed for any harassing or threatening material (e.g., cyber bullying), trade secret protection and/or any vulgar or obscene content.
8. Students are not to send messages over the network or participate in online "chat rooms." Students may not use any email or instant messaging programs on a school's computer. A student may only use Internet e-mail when a teacher instructs him/her to do so.
9. Students are not to enter the network's operating system.
10. A teacher may authorize the copying of student-created work to a removable device or other outside media. The use of a removable device or other outside media is not permitted without permission from a teacher.
11. Students may not have food or drink when working on school computers.
12. All copyright laws are to be enforced.
13. Students are not to unplug or change any computer device or network connections.
14. Students are not to change any display screen settings.
15. Students are not to change any program's toolbars or settings.
16. Students are not to add or delete any program icons on the desktop or Start Menu.
17. Malicious use of computers or the school's network to develop programs that harass other users or infiltrate a computer or computer system and/or damage the software components of a computer or

computing system is prohibited. Students may not use computers or the school's network in such a way that would disrupt their use by others.

**18.** Students are not to remove, modify, damage or destroy any computer or networking equipment.

**19.** Students are not to modify or remove any identifying labels on computer equipment.

**20.** Students are not to modify or remove any printer settings.

**21.** Students are to advise school staff when they observe any violation of the school's policy for the use of the school's computers.

**22.** Students are to advise their teacher when a school's computer malfunctions in any way (example: a program is not opening or closing correctly). The teacher will notify the technical support staff so that the computer can be repaired.

**23.** The possession of, or the taking, disseminating, transferring or sharing of by way of example: nude, obscene, pornographic, lewd or otherwise illegal images or photographs, whether by electronic data transfers or other means (commonly called texting, emailing, sexting, etc.) may constitute a crime under state and/or federal law. Any person possessing, taking, disseminating, or sharing nude, obscene, pornographic, lewd or otherwise illegal images or photographs may be punished under this code of conduct and may be reported to the appropriate law enforcement agencies.

**24.** Cyberbullying is the act of harassment that takes place via some method of technological media. If a student is being harassed and the effect is on the school it does not matter where the offense originates, even if off grounds, if the effect of such acts makes a transition to school grounds it is under our best judgment to take appropriate action.

**25.** The use of electronic devices for recording purposes must have prior approval.

**26.** Students are permitted to use their cellular phones or electronic devices in designated areas during designated times only. Designated times and areas will be determined at the discretion of the building administration. Students using their cellular phones or electronic devices at times other than designated or in locations other than designated may be subject to school discipline. Contents of cell phones or electronic devices may be searched if there is a reasonable suspicion that it may have been used in an activity prohibited by the Code of Conduct. At the building leadership's discretion, students' confiscated cellular phones or electronic devices may only be returned to their parent or guardian.

**27.** OLSD will provide access to filtered Internet and my.olsd.us platform (Schoology, PowerSchool, Google Drive) email via wireless access for personal computing devices belonging to students for educational purposes. Please note OLSD will not be able to provide technical support for personal computing devices.

Students are not allowed to circumvent the Internet filter or click-through warnings. Personal computing devices are not to be attached to the OLSD network other than the wireless network provided for student use. Computing devices that have been determined to be a threat to the network integrity will be immediately removed from the network and will not be allowed back on until the technology department is assured that the cause for removal has been resolved. Passkeys are not to be shared with others. OLSD will not be responsible for lost, stolen or damaged property whether it be by accidental or malicious means including but not limited to other users, viruses, malware, spyware or bot traffic. Violators will be subject to disciplinary actions, removal from wireless network and/or confiscation of equipment. As a condition to using OLSD's wireless network, students should have no expectation of privacy in their use of the network, and by signing the handbook awareness statement specifically understand and agree that their personal

computing device may be confiscated and searched anytime school officials have reasonable suspicion of violations of the technology usage policy or any other Board policies, guidelines or laws. Students will receive the wireless passkey from a teacher or the school office upon submission of the handbook awareness statement with the appropriate signatures.

**Exceptions to the above rules are permitted only under direct teacher supervision.** Violations of these rules may result in disciplinary action, including but not limited to detention, Wednesday School, Saturday School, Suspension Alternative Program and/or suspension. Violations also may be referred to the appropriate legal authorities and/or other legal action may be pursued.

**Technology Usage Agreement:** If you do NOT desire for your child to use district-provided technology while at school, please submit a letter to your building principal. In the event that we do not receive this information, ALL students will be permitted to use district-provided technology according to the provisions listed in the Technology Usage Policy.