Teach, Learn, Every Day, No Excuses

Oakdale Joint Unified School District
168 South Third Avenue, Oakdale, California 95361
(209) 848-4884 • Fax (209) 847-0155

OJUSD Student Network and Internet Use Agreement

I. Introduction

All Oakdale Joint Unified School District (OJUSD) schools provide students with access to technology. This Internet Use Agreement is intended to provide information about the types of technology used and the acceptable use policy for District technology resources. Use of OJUSD's technology resources is a privilege that the District extends to students in order to support and enrich their learning experiences. This handbook contains an Acceptable Use Policy that both students and their parents/guardians must agree to every school year.

II. Devices

OJUSD students work with a wide variety of devices throughout the school year, each designed to meet a different content delivery, content creation or collaboration need. Devices used by students may include, but are not limited to, personal computers (laptops, desktops and netbooks), iPods, iPads and other tablets, interactive white boards ("SMART boards"), digital projectors, document cameras, televisions, VCRs, DVD players, interactive response units, scanners, printers, photocopiers and assistive devices. Students use these devices to access the OJUSD network through both wired and wireless connections.

III. Content

While using District technology, students will be exposed to content from a variety of sources including, but not limited to content created by teachers and other students, applications and content purchased by the District and individual schools and content located on the internet. While the District is able exercise reasonable control over content created and purchased by the District, it has limited control over content accessed via the internet.

OJUSD believes that open access to the internet is important to the educational process and, further, that education in the proper use of technology, not restricted access, is the best way to protect our students on the internet. For this reason, PAUSD engages in very limited filtering of internet content. OJUSD employs a blacklisting service to restrict access to internet sites that are known to contain pornographic material. In addition, the district restricts access to other sites that it deems to have no educational value and to be potentially harmful to students. Parents should remember that, while best efforts to filter are made, no filtering system is 100% effective. OJUSD believes that the benefits to students from Internet access exceed the possible disadvantages.

OJUSD makes no warranties of any kind, either expressed or implied, for the technology resources it provides or the information students may access using those systems. OJUSD is not responsible for any damages users suffer while using OJUSD technology resources, including damages resulting from loss of data as a result of delays, non-deliveries, or service interruptions caused by the system, user errors or omissions, or by power failures. Users utilize information obtained from OJUSD technology resources at their own risk. OJUSD specifically denies any responsibility for the accuracy of information students may obtain from sources outside the District.

IV. Appropriate Use

The Oakdale Joint Unified School District expects that students will use District provided technology for purposes consistent with the curriculum. OJUSD technology resources should be used primarily for class assignments and other learning activities. Only school related files should be stored in student accounts. It is expected that students will use the District's technology resources efficiently, especially when other students are waiting to use them. Students are expected to take good care of District technology resources, leaving equipment and work areas in good condition.

OJUSD educates students on the appropriate use of each technology that the student is exposed to, including topics such as internet courtesy ('nettiquite'), proper research and citation methods and good email practices. Students are expected to adopt these practices, just as they would in any other subject area.

V. Technology Education: Safety & Privacy

The Oakdale Joint Unified School District will provide age appropriate training for each student in the safe use of technology, including maintaining their online reputation and ensuring their personal safety by keeping their personal information private. Students are expected to follow safe practices when using OJUSD technology.

VI. Local Policies & Practices These policies apply to all schools and students within OJUSD. Individual schools and teachers may develop local policies and procedures which may be more restrictive than District policies. Not all schools or teachers will use all types of software or hardware described in this document.

VII. Additional Policies

Additional policies may apply to the use of resources not available to all students. An examples of this is the Student Wireless Policies (where wireless is available) If in doubt, check with a teacher before using or attempting to use a resource.

VIII. Acceptable Use Policy

Please read and discuss the provisions of the Terms and Conditions with your child. When you and your child have accepted and signed this document it becomes a legally binding document.

OJUSD teachers and administration believe that providing access to technology enhances the educational experience for OJUSD students. To make that experience successful for everyone, students must abide by the following terms and conditions:

1. Security. Students shall not impair the security of OJUSD technology resources. This expectation includes but is not limited to:

a. Students are expected to safeguard all personal passwords. Students should not share passwords with others and should change passwords frequently. Students are expected to notify an administrator immediately if they believe their student account has been compromised.

b. Students are expected to access technology only with their account or with a shared account as directed by their teacher and not to allow others to use their account or to use the accounts of others, with or without the account owner's authorization.

2. Authorized Use. Students may use district technology resources when directed by a teacher or when technology has been designated for open student use (e.g. the library).

3. Inappropriate Use. OJUSD technology, hardware, software and bandwidth are shared and limited resources and all users have an obligation to use those resources responsibly. Students are provided access to OJUSD technology primarily for educational purposes. Incidental personal use of District technology is acceptable, but students should not use district technology for personal activities that consume significant bandwidth, for personal activities when others are waiting to use the equipment or for activities that violate school policy or local law. These include but are not limited to:

- Playing games or online gaming (e.g., World of Warcraft) unless approved by a teacher.
- Downloading software, music, movies or other content in violation of licensing requirements, copyright or other intellectual property rights.
- Installing software on district equipment without the permission of a teacher.
- Downloading, viewing or sharing inappropriate content, including pornographic, defamatory or otherwise offensive material.
- Conducting any activity that is in violation of school policy, the student code of conduct or local, state or federal law.
- Engaging in any activity that is harmful to other student(s), including cyberbullying.
- Participating in political activities.
- Using hacking tools on the network or intentionally introducing malicious code into the District's network.
- Using any software or proxy service to obscure either the student's IP address or the sites that the student visits.
- Disabling, bypassing, or attempting to disable or bypass any system monitoring, filtering or other security measures or accessing or attempting to access material or systems on the network that the student is not authorized to access.

4. No Expectation of Privacy. The District can and does monitor technology use and activity on the District's network, including but not limited to, sites visited, content viewed and email sent and received. The District may examine a student's account and activity and search the contents of a student's account if there is a reason to believe that school policies, regulations, or guidelines regarding access to the network or use of OJUSD technology have been violated.

5. Disruptive Activity. Students should not intentionally interfere with the performance of the District's network or intentionally damage any District technology resources.

6. Unauthorized Networks. Students may not create unauthorized wireless networks to access OJUSD's network. This includes establishing wireless access points, wireless routers and open networks on personal devices.

7. Consequences of Inappropriate Use. Students who misuse OJUSD's technology resources will be subject to discipline which may include loss of access to OJUSD technology resources and/or other appropriate disciplinary or legal action in accordance with the Student Code of Conduct and applicable laws.

IX. Use of the OJUSD Wireless Network

Acceptable Devices. Students may access the wireless network with any device with 802.11 connectivity. Students may only access the network with devices that are their own personal property.

Content. Filtered access to the Internet will be provided for student owned devices as well as access to any district web sites that would normally be accessible to students from home.

Personal Responsibility. The district assumes no responsibility for the loss of, theft of or damage to any personal device that a student connects to the student wireless network or any information on that device.

Security. Students shall not impair the security of the OJUSD network. This expectation includes but is not limited to:

a. Students are expected to maintain up to date antivirus and antispyware protection on all devices that are connected to the OJUSD wireless network. Devices without up to date security programs may be denied access to the network.

b. Students are expected to safeguard all network passwords. Students should not share network passwords with

others and should change passwords frequently. Students are expected to notify an administrator immediately if they believe their student account has been compromised.

c. Students are expected to log onto the wireless network only with their account and not to allow others to use their account or to use the accounts of others, with or without the account owner's authorization.

No IT Support. Students are responsible for setting up and maintaining the devices that they connect to the network. The district will not provide IT support for student owned devices.

Authorized Use. Students may use the wireless network when they are not in class. Students may not use the student wireless network in class unless authorized by the teacher of that class.

Inappropriate Use. The OJUSD network is a shared and limited resource and all users have an obligation to use that resource responsibly. Students are provided access to the OJUSD wireless network primarily for educational purposes. Incidental personal use of the network is acceptable, but students should not use the network for personal activities that consume significant network bandwidth or for activities that violate school policy or local law. These include but are not limited to:

a. Online gaming (e.g., World of Warcraft) unless approved by a teacher.

b. Downloading software, music, movies or other content in violation of licensing requirements, copyright or other intellectual property rights.

c. Downloading, viewing or sharing inappropriate content, including pornographic, defamatory or otherwise offensive material.

d. Conducting any activity that is in violation of school policy or local, state or federal law.

e. Participating in political activities.

f. Conducting for-profit business.

g. Using hacking tools on the network or intentionally introducing malicious code into the District's network.

h. Using any software or proxy service to obscure either the student's IP address or the sites that the student visits.

i. Disabling, bypassing, or attempting to disable or bypass any system monitoring, filtering or other security measures.

j. Accessing or attempting to access material or systems on the network that the student is not authorized to access.

No Expectation of Privacy. The District can and does monitor internet access and activity on the District's network, including but not limited to sites visited, content viewed and email sent and received. The District may examine a student's personal device and search its contents if there is a reason to believe that school policies, regulations, or guidelines regarding access to the network or use of the device have been violated.

Disruptive Activity. Students should not intentionally interfere with the performance of the wireless network and the District's overall network.

No Use of Wired Networks. Students may use only the OJUSD wireless network for personal devices. They may not attach personal devices to the OJUSD wired network.

X. Consequences of Violations

Students who misuse OJUSD's technology resources will be subject to discipline which may include loss of access to OJUSD technology resources and/or other appropriate disciplinary or legal action in accordance with the Student Code of Conduct and applicable laws. If a student is accused of any violation, s/he has all of the rights and privileges that exist with other kinds of school infractions.

Required Signatures

I understand and will abide by the provisions and conditions of this agreement. I understand that any violations of the above provisions may result in disciplinary action, the revoking of my user account, and appropriate legal action. I also agree to report any misuse of the information system to the site Principal. Misuse may come in many forms, but may be viewed as any messages sent or reviewed that indicate or suggest pornography, unethical or illegal solicitation, racism, sexism, inappropriate language, and other issues described above. I have read and understand each of the sections listed above and agree to follow these guidelines while using the network of the Oakdale Joint Unified School District.

Student Name: _____

Student Signature: _____ Date: _____

PARENT or GUARDIAN

I give my permission for the school to give computer and Internet access to my child and I have read and agree with the guidelines involved its use. I have read and understand each of the sections listed above and I further understand that this agreement will be enforce as long as my student attends this school district, unless I revoke it or there is a change in the policy.

Parent Signature: _____ Date: _____