

STUDENT ACCEPTABLE USE POLICY

A. Purpose

1. The Oxnard Union High School District is providing employees and students with access to the district's electronic communication system, which includes Internet access.
2. The purpose of the district's electronic communication system is to assist in preparing students for success in life and work in the 21st century by providing them with electronic access to a wide range of information and the ability to communicate with people from throughout the world. Additionally, the system will be used to increase district intracommunication, enhance productivity, and assist district employees in upgrading their skills through greater exchange of information with their peers. The district system will also assist the district in sharing information with the local community, including parents, social service agencies, government agencies, and businesses.
3. Users of the district's electronic communication system may not use the district system for commercial purposes, defined as offering or providing goods or services or purchasing goods or services for personal use. District acquisition policies will be followed for purchase of goods or services through the district system.
4. Users may not use the system for political lobbying. District employees and students may, however, use the system to communicate with their elected representatives and to express their opinions on political issues.
5. The term "educational purpose" includes use of the system for classroom activities, professional or career development, and limited high-quality self-discovery activities. Students will limit their use of the system for self-discovery purposes to no more than 3 hours per week.

B. District Responsibilities

1. The Superintendent or that person's designee will oversee the district system and the implementation of this policy and shall ensure that all district computers with Internet access have a technological protection measure that blocks or filters Internet access to visual depictions that are obscene, child pornography, or harmful to minors and that the operation of such measures is enforced. (20USC 6777, 47 USC 254)
2. In order to reinforce these measures, the Superintendent or that person's designee shall implement rules and procedures designed to restrict students' access to harmful or inappropriate matter on the Internet and to ensure that students do not engage in unauthorized or unlawful online activities. Staff shall supervise students while they are using online services and may have teacher aides, student aides, and volunteers assist in this supervision.
3. The Superintendent or that person's designee shall also establish regulations to address the safety and security of students and student information when using email, chat rooms, and other forms of electronic communication.
4. To the extent possible, the Superintendent or that person's designee shall block access to social networking sites on district computers with Internet access.

5. The Superintendent or that person's designee shall provide age-appropriate instruction regarding safe and appropriate behavior on social networking sites, chat rooms, and other Internet services. Such instruction shall include, but not be limited to, the dangers of posting personal information online, misrepresentation by online predators, how to report inappropriate or offensive content or threats, behaviors that constitute cyberbullying, and how to respond when subjected to cyberbullying.
6. The site principal or that person's administrative designee will serve as the building-level coordinator for the district system, will approve building-level activities, ensure that teachers receive proper training in the use of the system and the requirements of this policy, establish a system to ensure adequate supervision of students using the system, maintain the file of user agreements, and will be responsible for interpreting the Student Acceptable Use Policy at the site level.
7. The district's administrator of Information Technology will establish a process for setting-up individual and class accounts, set quotas for disk usage on the system, establish a retention schedule and establish a district virus protection process.

C. Technical Services Provided through District System

1. **World Wide Web.** The Web provides access to a wide range of information in the form of text, graphics, photographs, video, and sound from throughout the world. The Web is a valuable research tool for students and staff members.
2. **E-mail.** E-mail will allow employees and students to communicate with people from throughout the world. Users will also be able to subscribe to mail lists and engage in group discussions related to educational subjects.
3. **Telnet.** Telnet allows the user to log in to remote computers.
4. **File Transfer Protocol (FTP).** FTP allows users to download large files and computer software.
5. **Newsgroups.** Newsgroups are discussion groups that are similar to mail lists. With the oversight of the Coordinator of Educational Technology, the district will provide access to selected newsgroups that relate to subjects that are appropriate to the educational purpose of the system.
6. **Internet Relay Chat (IRC).** IRC provides the capability of engaging in "real-time" discussions. With the oversight of the Coordinator of Educational Technology, the district will provide access to IRC only for specifically defined educational activities.

D. Access to the System

1. The Student Acceptable Use Policy is intended govern all use of the district system. Student misuse of the district system will also be governed by the Student Discipline Code (Board Policy 5144).
2. **World Wide Web.** All District employees and students will have access to the Web through the district's networked computers. An agreement will be required for all students, which must be signed by the student and the student's parent or guardian.

3. Individual E-mail Accounts for Students. Students may be provided with individual e-mail accounts. An agreement will be required for an individual e-mail account. This agreement must be signed by the student and the student's parent or guardian.
4. Individual E-mail Accounts for District Employees. District employees will be provided with an individual account. No agreement will be required.

E. Parental Notification and Responsibility

1. The district will notify the parents about the district system and the Student Acceptable Use Policy. Parents must sign an agreement to allow their student access to the district system. Parents may request alternative activities for their child(ren) that do not require Internet access.
2. Parents have the right at any time to investigate the contents of their child(ren)'s e-mail files. Parents have the right to request the termination of their child(ren)'s individual account at any time.
3. The Student Acceptable Use Policy contains restrictions on accessing inappropriate material. There is a wide range of material available on the Internet, some of which may not be fitting with the particular values of the families of the students. It is not practically possible for the district to monitor and enforce a wide range of social values in student use of the Internet. Further, the district recognizes that parents bear primary responsibility for transmitting their particular set of family values to their children. The district will encourage parents to specify to their child(ren) what material is and is not acceptable for their child(ren) to access through the district system.

F. District Limitation of Liability

1. The district makes no warranties of any kind, either express or implied, that the functions or the services provided by or through the district system will be error-free or without defect. The district will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. The district is not responsible for the accuracy or quality of the information obtained through or stored on the system. The district will not be responsible for financial obligations arising through the use of the system.

G. Due Process

1. The district will cooperate fully with local, state, or federal officials in any investigation concerning to or relating to any illegal activities conducted through the district system.
2. In the event that there is an allegation that a student has violated the Student Acceptable Use Policy, the student will be provided with a written notice of the alleged violation and an opportunity to present an explanation before a school administrator.
3. Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network. If the alleged violation also involves a violation of other provisions of the Student Discipline Code, the violation will be handled in accordance with the applicable provision of the district discipline policies and procedures.

H. Search and Seizure

1. System users have a limited privacy expectation in the contents of their personal files on the district system.
2. Routine maintenance and monitoring of the system may lead to discovery that the user has or is violating the Internet Acceptable Use Policy, the Student Discipline Code, or the law.
3. An individual search will be conducted if there is reasonable suspicion that a user has violated the law or the Student Discipline Code. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation.
4. District employees should be aware that their personal files may be discoverable under state public records laws.

I. Copyright and Plagiarism

1. Laws related to copyrights will govern the use of material accessed through the district system. Because the extent of copyright protection of certain works found on the Internet is unclear, employees will make a standard practice of requesting permission from the holder of the work if their use of the material has the potential of being considered an infringement. Teachers will instruct students to respect copyright and to request permission when appropriate.
2. District practices pertaining to plagiarism will govern use of material accessed through the district system. Teachers will instruct students in appropriate research and citation practices.

J. Academic Freedom, Selection of Material, Student Rights to Free Speech

1. Board policies on Academic Freedom and Free Speech will govern the use of the Internet.
2. When using the Internet for class activities, teachers will select material that is appropriate in light of the age of the students and that is relevant to the course objectives. Teachers will preview the materials and sites they require or recommend for students' access to determine the appropriateness of the material contained on or accessed through the site. Teachers will provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers will assist their students in developing the skills to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.

K. District Web Site

1. District Web Site. The district will establish a Web site and will develop Web pages that will present information about the district. The Coordinator of Educational Technology will be designated the Webmaster, responsible for maintaining the district Web site.
2. School or Class Web Pages. Schools and classes may establish Web pages that present information about the school or class activities. The building principal will designate an individual to be

responsible for managing the school Web site. Teachers will be responsible for maintaining their class site.

3. **Student Web Pages.** With the approval of the building principal, students may establish personal Web pages. The principal will establish a process and criteria for the establishment and posting of material, including pointers to other sites, on these pages. Material presented in the student's Web site must be related to the student's educational and career preparation activities. Student Web pages must include the following notice: "This is a student Web page. Opinions expressed on this page shall not be attributed to the district."
4. **Extracurricular Organization Web Pages.** With the approval of the building principal, extracurricular organizations may establish Web pages. The principal will establish a process and criteria for the establishment and posting of material, including pointers to other sites, on these pages. Material presented on the organization Web page must relate specifically to organization activities and may include student-produced material. Organization Web pages must include the following notice: "This is a student extracurricular organization Web page. Opinions expressed on this page shall not be attributed to the district."

L. Student Acceptable Use Policy

The following uses of the district system are considered unacceptable:

1. **Personal Safety (Restrictions are for students only)**
 - a. Student use of district computers to access social networking sites is prohibited.
 - b. Users will not post personal contact information about themselves or other people. Personal contact information includes address, telephone, school address, work address, etc.
 - c. Users will not agree to meet with someone they have met online without their parent's approval and participation.
 - d. Users will promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.
2. **Illegal Activities**
 - a. Users will not attempt to gain unauthorized access to the district system or to any other computer system through the system or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing."
 - b. Users will not make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means. These actions are illegal.
 - c. Users will not use the district system to engage in any other illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of a person, etc.

3. System Security

- a. Users are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a user provide their password to another person.
- b. Users will immediately notify the administrator in charge of Information Technology if they have identified a possible security problem. Users will not go looking for security problems, because this may be construed as an illegal attempt to gain access.
- c. Users will avoid the inadvertent spread of computer viruses by following the district virus protection procedures if they download software.

4. Inappropriate Language

- a. Restrictions against inappropriate language apply to public messages, private messages, and material posted on Web pages.
- b. Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
- c. Users will not post information that, if acted upon, could cause damage or a danger of disruption.
- d. Users will not engage in personal attacks, including prejudicial or discriminatory attacks.
- e. Users will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending them messages, they must stop.
- f. Users will not knowingly or recklessly post false or defamatory information about a person or organization.

5. Respect for Privacy

- a. Users will not repost a message that was sent to them privately without permission of the person who sent them the message.
- b. Users will not post private information about another person.

6. Respecting Resource Limits

- a. Users will use the system only for educational and professional or career development activities (no time limit), and limited, high-quality, self-discovery activities. For students, the limit on self-discovery activities is no more than 3 hours per week.

- b. Users will not download large files unless absolutely necessary. If necessary, users will download the file at a time when the system is not being heavily used and immediately remove the file from the system computer to their personal computer.
- c. Users will not post chain letters or engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people.
- d. Users will check their e-mail frequently and delete unwanted messages promptly.
- e. Users will subscribe only to high quality discussion group mail lists that are relevant to their education or professional/career development.

7. Plagiarism and Copyright Infringement

- a. Users will not plagiarize works that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.
- b. Users will respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If users are unsure whether or not they can use a work, they should request permission from the copyright owner.

8. Inappropriate Access to Material

- a. Users will not use the district system to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature). For students, a special exception may be made for hate literature if the purpose of such access to conduct research and access is approved by both the teacher and the parent. District employees may access the above material only in the context of legitimate research.
- b. If users inadvertently access such information, they should immediately disclose the inadvertent access in a manner specified by their school. This will protect users against an allegation that they have intentionally violated the Student Acceptable Use Policy.

M. Use of Electronic Recording Devices

Use of electronic recording devices to facilitate specific instructional and administrative services is permitted based on established policies and practices. Such uses include but are not limited to the school or district identification card program and related uses, school or district publications and broadcast facilities, athletic programs and theatrical productions, scheduled distance learning classes, video conferences, digitally streamed class content (live or recorded), and video tape recording of classes or related academic events by Information Technology Services Media Distribution Services when requested to capture video, audio or still images.

Electronic devices may be used to record a lecture, presentation, interview or similar activity with prior permission of the individual being recorded. This permission does not extend to others who may be present. Absence of permission may constitute copyright infringement. Verbal permission may be

sufficient for recording within a class or meeting for personal use. However, written permission must be obtained prior to recording or transmitting someone's image or speech over the airwaves, in public, on the web, as part of a class assignment or any University sponsored activity or program.

It is the responsibility of the user, host, event sponsor or department to provide notification and obtain the necessary permissions in advance or at the time of the recording / transmission.

In accordance with American Disability Act applicable policies and laws, instructional materials and school or district information presented in electronic form must be accessible to persons with disabilities. This includes recordings of lectures, events, DVDs and other recordings shown in class or posted on the web. In general, this requires that the recording be captioned.

1. Expectation of Privacy

Taking photos or making audio or video recordings without permission in ANY context in which the person has a reasonable expectation of privacy is prohibited. Such physical areas on campus include but are not limited to private offices, restrooms, changing rooms, labs, classrooms, and conference rooms. In such areas, permission must be granted by all persons being photographed or recorded.

2. Surveillance Equipment and Software

Surveillance equipment and software may be placed on campus and monitored by authorized campus personnel to prevent or deter crimes and protect public safety and to facilitate official University investigations into criminal activities or violations of district policy. Such uses must be coordinated with the Police Department or Information Technology Services as appropriate.

ADOPTED: January 29, 1997

REVISED: May 9, 2012

OXNARD UNION HIGH SCHOOL DISTRICT
309 South K Street
Oxnard, California 93030
(805) 385-2500

TO: Oxnard Union High School District Parents and Students
SUBJECT: STUDENT ACCEPTABLE USE POLICY

Dear Parents and Students:

The Oxnard Union High School District is pleased to offer our students access to the District's computer network. This network is a powerful tool, connecting students to a rich, diverse and stimulating interchange of ideas and information via the Internet. It also offers other resources such as common business applications (word processing, spreadsheets, PowerPoint, databases), electronic courseware, printing and secure file storage for students. Students can survey on-line documents from government agencies or legislators. They can access research and other files posted by universities and libraries, consult college catalogs, or find the latest occupational and career information. From computers in classrooms, labs and libraries, students can take a "virtual tour" of the Smithsonian or Louvre Museums, and explore the history and culture of other countries.

However, like many of the best-planned excursions, often the most provocative and rewarding experiences are those that arise unexpectedly--the unforeseen side trips and detours. So it is with the Internet. While we recognize that despite our best filtering efforts, this opens students to the chance of encountering material that is profane, or otherwise controversial, we firmly believe the value obtained through the experience of Internet searching and global communication far outweighs any negative possibilities.

As a public educational institution, we have an obligation to ensure, as far as possible, the integrity of our use of the network. We also want to teach and encourage our students to become discriminating users of information. It is reasonable, then, for us to expect students to use the network in a responsible manner, consistent with school and district policy.

It is the intent of this document to clarify the Oxnard Union High School District's standards of conduct and define our disciplinary measures for any breach of policy. The signatures of both a parent or guardian and the student indicate that this document has been carefully read and understood, and that the signers agree that the student, and not the school, is held accountable for his/her actions, and agree to the terms and conditions of the Student Acceptable Use Policy described more fully on the attached page.

TERMS AND CONDITIONS OF INTERNET USE

STUDENT ACCEPTABLE USE POLICY Page 2 ISSUES OF CONCERN

1. General Conduct

Internet capabilities are provided to students to support learning, enhance instruction, and to give access to a vast exchange of information. The student is expected to follow all guidelines stated below as well as those given orally by the school staff. It is expected that all computers and network services are to be used in an appropriate, efficient, ethical and legal manner. Inappropriate use is defined as a violation of the intended educational purpose, and shall include use of the network for obscene or profane activities, for harassment or defamation. Students are expected to exit immediately any inappropriate files they may inadvertently encounter. Because on-line networks are used as part of a school activity, the Student Acceptable Use Policy is an extension of the school's behavior code, and normal disciplinary measures adopted by the school will be pursued for any infringements.

2. Legal Issues and Security

Security on any computer system is a high priority, especially when the system involves many users. It is a violation of California State Law to access any computer system or network for the purpose of fraud, or to maliciously access, alter, delete, damage, or destroy any computer system, program, or data. Anyone who commits acts of this kind will face disciplinary action by the school and legal action by the appropriate authorities.

Some examples of offenses are tampering with another's account or password, damaging files or data, attempting to log-on as another user, altering or degrading the system, maliciously uploading or creating computer viruses, using the system for theft of data, equipment, or intellectual property, the transmission of obscene or threatening material, or using the system for monetary gain.

Students who violate these standards will be denied access to the network and will invoke school disciplinary measures.

3. Copyright

Copyright laws exist to protect intellectual property rights. Any copyrighted material such as software, music, and videos must not be transmitted via the network, nor downloaded or stored on any school computers without express written permission of the copyright holder.

4. Plagiarism

Plagiarism is the taking of ideas or writings from another person and offering them as one's own. Students who take excerpts from on-line files and materials for use in their own documents must give credit to the author.

5. School Resources

The district's network has a limited capacity to handle user traffic. To efficiently use resources and prevent network congestion, students must not engage in frivolous activities nor download, stream, or view non-educational materials. Students will use the network for classroom based activities such as research, printing and saving files on their secure, file server share.

Please respect the fact that there are many students who need to use the network; use access time efficiently.

STUDENT ACCEPTABLE USE POLICY Page 3

Oxnard Union High School District

CONSENT AND WAIVER

Valid signatures are required for permission to use the network. Permission is effective for the duration of the student’s enrollment in the Oxnard Union High School District or until parent or guardian rescinds permission in writing to the school principal.

By signing this Consent and Waiver, I _____ (print name) and my parent(s) or guardian(s) agree to abide by its terms and conditions. We realize that network access is provided to students to further educational goals and objectives, and agree that student use shall be legal, efficient, and consistent with school purposes and with general standards of decency. In addition, we understand that students are expected to show consideration and respect for other users communicating on-line, as well as respect for equipment and school property.

We acknowledge there is some material accessible via the Internet that may be offensive, defamatory, graphic, inaccurate, illegal, or otherwise objectionable despite our best filtering and monitoring efforts. However, **we agree that the school and district shall not be held liable for any objectionable materials a student may encounter.** While the school will strongly attempt to maintain the integrity of network use, it is not ultimately responsible for restricting, monitoring or controlling the communications of individuals utilizing the network. By our signatures, we agree that it is the student who holds sole responsibility for his or her conduct on-line, for any materials accessed through the network, and for any costs incurred as a result of network use.

The school holds activities such as the following as just cause for taking disciplinary action, revoking network privileges, and/or making referral to legal authorities:

- Degrading or disrupting equipment or system performance
- Gaining intentional access to obscene or inappropriate files
- Using the network for any illegal activity, including violation of copyright or other licenses or contracts
- Accessing “chat lines” or “blogging”
- Using abusive or otherwise objectionable language in either public or private messages
- Harassing, insulting or attacking others
- Posting anonymous messages
- Wasteful use of limited resources provided by the school
- Causing undue congestion of the network through lengthy downloads of files, or by engaging in frivolous activities
- Accessing or tampering with the data of another user
- Gaining unauthorized access to resources or files
- Identifying one’s self with another person’s name
- Using an account or password of another user
- Using the network for financial transactions
- Theft of data, equipment, or intellectual property
- Invading the privacy of individuals

School disciplinary measures are outlined in student handbooks, the Parent Information Handbook, and in district policies and, based on circumstances, may include any or all of the following: parent conference, revoking of network use privileges, detention, in-school suspension, Saturday school, or expulsion.

Please read carefully the attached explanation of the policy, and call the high school principal if you have any questions or wish further information.

Student name _____ Student Number _____
Please Print

Student signature _____ Date _____

Parent or Guardian signature _____ Date _____