Oregon City Schools

Acceptable Use & Internet Safety Policy Agreement - Student

Statement of Purpose

Oregon City Schools (hereafter referred to as the District) is pleased to offer our students access to the Internet and other electronic networks. Students are encouraged to use the technology available to in the District. The District's technology is an important educational resource, where provides opportunities for collaboration and exchange of information; facilitates personal growth in the user of technology; and enhances information access, retrieval, evaluation, usage and communication skills. However, it is important to remember that access is a privilege, not a right, and carries with it responsibilities for all involved.

This Acceptable Use and Internet Safety Policy (hereafter referred to as the policy) is an agreement between the student, parent/guardian and the District. The intent of this document is to ensure that parents are knowledgeable about and that students will comply with the policy approved by the District.

Consequences for Violation of Policy

A user violates this policy by his/her own action or by failing to report any violations by other users that come to their attention. Consequences for violations of the policy will be in accordance to the school discipline policies. All school rules, regulations and consequences specified in the student handbooks regarding violations such as use of profanity, harassment, theft, misuse, vandalism, etc. will apply. Violations of this policy can also lead to loss of device use privileges. Students will be liable for any damages caused by misuse of access privileges.

Terms of Agreement

Personal Responsibility, Use and Acceptance - In exchange for the use of District devices and other hardware, Internet access, email, electronic subscriptions/research/productivity resources, and internal electronic resources (hereafter referred to as the network), we (parents/students) understand and agree to the following items (as signified by physically or digitally signing the agreement). Students who use or otherwise access the network via wireless or hard-wired connection (hereafter referred to as users) are responsible for their behavior on the network just as they are in a classroom, school hallway or other District property. The user consents to the terms of this policy whenever he/she accesses the network. The District reserves the right to remove files, limit or deny access and/or refer a student for other school disciplinary action and/or, if necessary, criminal prosecution as a result of any improper use, determined by the District, and is not limited by the examples of misuse given in this policy.

A. Access to all network devices and services will require a unique user account. Before a user is allowed access to the network the agreement signature page of this Policy must be digitally signed via the District's online registration or physically completed and returned to the Director of Technology.

B. The use of the network is a privilege not a right. The District may revoke this privilege at any time, and for any reason.

C. The use of District and/or network resources are for the following purposes (in order of priority):
    a. support of the academic program
    b. telecommunications for academic purposes and
    c. general information and research

D. The District devices and/or network are intended for the exclusive use by registered users. Anonymous use is not permitted and access (including passwords) may not be shared or transferred. Any improper use of your account, even if you are not the user, is your responsibility. The user is responsible for the use of his/her account/password and/or access privilege. Any problems that arise from the use of a user's account are the responsibility of the account holder. users are responsible for logging out of their individual account (on shared devices) at the end of each use. Use of an account by someone other than the registered account holder is forbidden and may be grounds for loss of access privileges and for other school disciplinary actions. users must report any misuse of the network, including security/password breaches, to the Technology Department or building administrator.

E. Proper use of District devices are your responsibility. Any misuse, failure, damage or loss involving such equipment must be reported to the Director of Technology. You may be held financially responsible for the expense of any equipment repair or replacement needed due to a lack of due care.

F. Under no circumstances should District devices be moved from their intended location without permission of the Director of Technology.

G. Users shall not take any action that would compromise the security or adversely affect the integrity, functionality, or reliability of any computer, network, or messaging system. users shall report to the District's Director of Technology any actions by any user which would violate the security or integrity of any computer, network, or messaging system whenever such actions become known to them in the normal course of their work duties. This shall not be construed as creating any liability for students or staff members for the computer-related misconduct of students or other staff members.

H. The District reserves all rights to any materials stored in files which are generally accessible to others and will remove any material which the District, at its sole discretion, believes may be unlawful, obscene, pornographic, abusive, or otherwise objectionable. Students will not use their District-approved account/access to obtain, view, download, or otherwise gain access to such materials.

I. All information services and features contained on District and/or network resources are intended for the *private* use of its registered users. Any use of these resources for commercial-for-profit uses, intrusion on other users' privacy, or other unauthorized purposes (i.e., advertisements, political lobbying), in any form, is expressly forbidden.

J. The District reserves the right to impose time limits, access limits, and disk and printer quotas. Academic pursuits take priority over all other activities.

K. The District reserves the right to log device use and to monitor utilization by users. The District reserves the right to remove a user account from the network to prevent further unauthorized activity.

L. The District and/or Director of Technology will periodically make determinations on whether specific uses of District technology (such as new advancements in technology) are consistent with the acceptable-use practice.

Acceptable and Unacceptable Uses of the network - The District devices, user accounts and network are intended for educational uses and school-related communications. Incidental use of these systems by users for personal reasons is permitted as long as such use does not interfere with the users educational responsibilities and performance and does not interfere with system operations or other system users.

The District has implemented technology-blocking measures that protect against access by both adults and minors to visual depictions that are obscene, child pornography or, with respect to the use of computers by minors, harmful to minors.

"Harmful to minors" is define as any picture, image, graphic image file or other visual depiction that:

1. Taken as a whole and with respect to minors appeals to a prurient interest in nudity, sex or excretion;
2. Depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated, normal or perverted sexual acts of a lewd exhibition genitals and
3. Taken as a whole, lacks serious literary, artistic, political or scientific value to minors.

Unacceptable use of District devices, user accounts, or network resources shall include, but not be limited to:

1. the connection of any non-district owned wireless/or hard-wired device to the computer network unless on the public wireless environment or specifically authorized by the District's Director of Technology
2. intentionally seeking information on, obtaining copies of, or modifying files, other data, or passwords belonging to other users; logging on to other users' accounts (for any reason)
3. sharing your password with anyone, logging other users onto your account, or letting others users use your account.
4. impersonating other users on the network through any electronic communication.
5. interfering with others' use of the network; disrespecting other users' rights to privacy
6. accessing or attempting to access information in areas students do not have access to
7. vandalizing District owned hardware, software, or network resources
8. attempting to defeat network security features including, but not limited to account and device restrictions
9. use of anonymous proxies or any other attempts to circumvent Internet content filtering is strictly prohibited
10. disrupting the operation of the network through abuse or alteration of any District owned hardware, software, or resources
11. attempting to hack into any District owned hardware, software, or network resources
12. engaging in activity that could be considered forgery, fraud, or plagiarism
13. engaging in or promoting any other activity deemed illegal by local, state or federal law
14. downloading, installing, or using any software or other tools that are not District owned or approved to be used on the device or network. No third party software will be installed or used without the consent of the Technology Department.
15. using the intellectual property of others without permission and/or without citing the author
16. violating copyright law, which includes but is not limited to the storage or illegal use of copyrighted software, text, audio and video files as well as video games
17. malicious use of the network through hate mail, harassment, profanity, vulgar or threatening statements, cyber bullying, or discriminatory remarks
18. uses that constitute defamation (libel or slander)
19. trasmitting materials which are obscene, lewd, vulgar, or disparaging of persons based on their race, color, sex, age, religion, national origin, or sexual orientation or are disruptive or sexually explicit
20. extensive use for noncurriculum-related communication
21. using District provided electronic communications for expression of opinions, as a public forum of any kind, or to support private or public causes or external organizations.
22. non-educational uses including, but not limited to commercial, fundraising or profit making activities, religious or political uses,

unless specifically authorized by an administrator
23. engaging in commercial transactions. users may not use the school network to sell or buy anything over the Internet unless specifically authorized by an administrator.
24. neglecting to follow guidelines of Web 2.0 tools (outlined in separate section below.)
25. using technology and Web 2.0 tools to facilitate academic dishonesty

Use of Outside Services - Email, document storage, social media, online classroom environments, or any and all other online services must be provided and/or approved by the District through its network. Because the list is vast, and because technologies change so rapidly, individual services are not listed in this Policy. However, some examples of this are Google, e-mail, Schoology, and STAR accounts that are provided to certain grade levels, as well as many other online accounts through the District. users are responsible for individually managing sharing permissions in order to protect secure information. The use of providers of such functionality or storage through the District's network, outside of those approved, is prohibited. users shall inquire about the use of a service if its approval is not known. Permission to access these services may be granted on a limited basis by the Director of Technology. A user must obtain permission prior to access. Outside e-mail systems may be used for personal e-mail, however, use of such systems for District business is prohibited.

Personal Equipment - The only equipment that is permitted to be hard-wired to the network is that equipment expressly approved by the Director of Technology and the network Administrator after thorough testing. This includes, but is not limited to, personally owned equipment such as gaming consoles, personal devices, handhelds, phones, etc. In no case shall equipment be connected to the Oregon City School's network that is expressly prohibited by the Northwest Ohio Computer Association (NWOCA), including routers, modems, and managed switches. The use of personal equipment, such as tablets, laptops and mobile phones is encouraged on the Oregon Public wireless network, if approved in your grade level/building. If syncing a mobile device to district provided services or information, including e-mail and Google Accounts, end-user is required to password-protect the device in case it is lost or stolen.

Waiver of Privacy - The District reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the network, Internet access, and any use of District provided equipment and services. No user shall have any expectation of privacy regarding such materials.

Confidentiality and Student Information - users are responsible for maintaining security of student information and other personally identifiable data that they access, even if they access such data accidentally or without permission, and for upholding FERPA (20 U.S.C. § 1232g), the student confidentiality law (Ohio Revised Code Section 3319.321), the Ohio Privacy Act (Chapter 1347 of the Ohio Revised Code), and any other applicable privacy policies and regulations. users are responsible whether such data is downloaded from the network to their device screen, transmitted by e-mail, stored on a flash drive, portable device or laptop, copied by handwriting or by any or all other devices, forms of storage or methods.

System Security and Integrity - The District has defined these guidelines to help students and to insure an understanding of appropriate use and expectations. The District reserves the right to suspend operations of the network, in whole or in part, at any time for reasons of maintaining data security and integrity or any other lawful reason. The District reserves the right to block or filter any web sites, email addresses, servers or Internet domains which it, in its sole judgment, has determined to present a risk of exposing students or employees to sexually explicit or otherwise inappropriate content, or which exposes the system to undue risk of compromise from the standpoint of security or functionality. Staff members will exercise reasonable care in supervising student use; however, the District and its personnel are not responsible for student exposure to objectionable or inaccurate content or for the unauthorized activities of a user.

No Warranties Created - The District and/or technology department do(es) not warrant that the functions of the system will meet any specific requirements the user may have or that it will be error free or uninterrupted; nor shall it be liable for any direct or indirect, incidental, or consequential damages (including lost data, information, or time) sustained or incurred in the connection with the use, operation, or inability to use the system. Students are to report any problems to the teacher, who shall notify the technology department.

Websites - Websites created through the network and/or linked with the District's official website must relate specifically to District-sanctioned activities, programs or events. Websites created using the network or the District's equipment, or websites created as part of a classroom or club assignment or activity are the sole and exclusive property of the District in perpetuity without any ownership rights existing in the page creator(s). The District reserves the right to require that all material and/or links with other sites found to be objectionable be altered or removed for any reason or for no reason, in the sole judgment of the Superintendent. The District does not intend to open web pages for the expression of opinion, and specifically does not intend for its web pages to be a public forum or limited public forum for students, staff, or citizens. Web pages exist solely in support of the School District functions and mission as determined by the Board.

Use of Web 2.0 Tools - Online communication is critical to our students learning 21st Century Skills and tools such as online classroom environments, digital collaboration, forums, email, and online/cloud computing offer an authentic, real-world vehicle for student expression. The primary responsibility to students is their safety. Hence, expectations for classroom projects or other Web interactive activities, such as online classroom activities, digital collaboration, forums, email, and online/cloud documents, must follow all established Internet safety guidelines.

A. The use of online classroom environments, digital collaboration, forums, email, online/cloud computing, or other Web 2.0 tools is considered an extension of the classroom. Therefore, any speech that is considered inappropriate in the classroom is also inappropriate in all uses of online classroom environments, digital collaboration, forums, email, online/cloud documents, or other Web 2.0 tools. This includes, but is not limited to, cyber bullying, profanity, racist, sexist or discriminatory remarks.
B. Students using online classroom environments, digital collaboration, forums, email, online/cloud computing, or other Web 2.0 tools are expected to act safely by keeping ALL personal information out of their posts.
C. A student should NEVER post personal information on the web (including, but not limited to, last names, personal details including address or phone numbers, or photographs). Do not, under any circumstances, agree to meet someone you have met over the Internet.
D. Comments made in online classroom activities, digital collaboration, forums, email, and online/cloud documents will be monitored and - if they are inappropriate – will be deleted and disciplinary action may be taken.
E. Never include links to web sites from online classroom activities, digital collaboration, forums, email, and online/cloud documents without reading the entire article to make sure it is appropriate for a school setting.
F. Students using such tools agree to not share their user name or password with anyone besides their teachers and parents and treat these environments and activities as though they were in a traditional classroom. Speech that is inappropriate for class is also inappropriate for a these environments.
G. Students who do not abide by these terms and conditions may lose their opportunity to take part in the project and/or be subject to consequences appropriate to misuse.

Internet Safety

A. Parents and users - Despite every effort for supervision and filtering, all users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged students. Every user must take responsibility for his or her use of the network and Internet and avoid these sites.
B. Personal Safety - In using the network and Internet, users should not reveal personal information such as home address or telephone number. users are responsible for maintaining the security of their data and other personally identifiable information. users should never give out private or confidential information about themselves or others on the Internet. users should never arrange a face-to-face meeting with someone “met” on the Internet without a parent’s permission.
C. Active Restriction Measure - The District will utilize filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) pornographic, or (3) harmful to minors. The use of anonymous proxies or any other attempts to circumvent the content filter is strictly prohibited and will be considered a violation of this Policy. The school will also monitor the online activities of students, through direct observation and/or technological means.
D. The District will educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. The Superintendent/designee will develop a program to educate students on these issues.
E. The District will provide age-appropriate training for users who access the Internet through the District network. Following receipt of this training, the user will acknowledge that he/she received the training, understood it, and will follow the provisions of the Policy herein. The training provided will be designed to promote the District commitment to:
   - The standards and acceptable use of Internet services as set forth herein;
   - users safety with regard to:
     - safety on the Internet;
     - appropriate behavior while on online, on social networking websites, in collaborative environments, and in forum type environments; and
     - cyber bullying awareness and response.
   - Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

Student's Name (please print) _____ ***Grade*** _____
Last First

Student ID# _____

Building (check one):

□ Clay HS □ Fassett Junior High □ Eisenhower Intermediate □ Other (please specify):
□ Coy Elementary □ Jerusalem Elementary □ Starr Elementary _____

Oregon City Schools

Acceptable Use and Internet Safety Policy Agreement

Student Agreement

This agreement is entered into between _____ and the **OREGON CITY SCHOOLS.**
(student first & last name, **please print**)

I have read and I understand the ***Oregon City Schools Acceptable Use and Internet Safety Policy*** and am willing to abide by said rules and regulations of system usage as well as any changes deemed necessary by the Director of Technology. These rules and changes will be available in the technology, from the Director of Technology, from the building principals, and on our district website.

_____ _____
Signature of Student (for grades 3 – 12 only) Date

Parental Release

I, _____ the parent/guardian of _____
(parent/guardian name, **please print**) (student name, **please print**)

have read and understand the ***Oregon City Schools Acceptable Use and Internet Safety Policy***, and I agree to its terms and conditions as well as any changes deemed necessary by the Director of Technology. These rules and changes will be available in the technology, from the Director of Technology, from the building principals, and on our district website. I confirm my child's intention to abide by the terms and conditions therein.

_____ _____
Signature of Parent/Guardian (for grades K – 12) Date

This agreement must be signed every school year and upon enrollment to the Oregon City School District.