Oregon City Schools

Network Privacy and Acceptable Use Policy –Staff

Statement of Purpose

Oregon City Schools (hereafter referred to as District) is pleased to offer our staff access to the Internet and other electronic networks. Staff are encouraged to use the technology available in the District. The District's technology is an important educational resource, which provides opportunities for collaboration and exchange of information; facilitates personal growth in the use 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 *Network Privacy & Acceptable Use Policy* (here after referred to as the Policy) is an agreement between the staff member and the District. The intent of this document is to ensure that staff are knowledgeable about and will comply with the Policy approved by the District.

It is the intention of the Oregon City School District Board of Education to protect the privacy of staff members who use the school computers, computer network, and electronic messaging systems to the maximum extent possible given the operational and security needs of the District. The purpose of this policy is to identify the limitations on this privacy and the general restrictions applying to the use of computers and electronic messaging systems of the District.

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), staff should understand and agree to the following items (as signified by physically or digitally signing the agreement). Staff who use or otherwise access the Network via wireless or hardwired connection (hereafter referred to as Users) are responsible for their behavior on the Network. The User consents to the terms of this Policy whenever he or she accesses the Network. The District reserves the right to remove files, limit or deny access, and/or refer staff for other 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 completed, signed, and returned to the Network Administrator.

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 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.

D. 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.

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

F. 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.**

G. 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. Users will not use their District-approved account/access to obtain, view, download, or otherwise gain access to such materials.

H. 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.

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

J. 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.

K. 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 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.

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 Users 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

Student Acceptable Use and Internet Safety Policy – It is the responsibility of each staff member to be aware of and enforce the Student Acceptable Use and Internet Safety Policy. Contents of the Staff Network Privacy and Acceptable Use Policy are also in the Student Acceptable Use and Internet Safety Policy. There are additional elements, however, in the Student Policy (such as "Use of Web 2.0 Tools" and "Internet Safety"), which are not a part of the Staff Policy. The complete Student Policy can be found on our District Webpage.

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.

Right of Access - Although the Board of Education respects the natural desire of all persons for privacy in their personal communications, and will attempt to preserve this privacy whenever possible, the operational and security needs of the District's Network and messaging systems require that full access be available at all times. The District therefore reserves the right to access and inspect any computer, device, or electronic media within its systems and any data, information, or messages that may be contained therein. All such data, information, and messages are the property of the District and staff members should have no expectation that any messages sent or received on or through the School District's systems will always remain private. **Staff members shall not be held accountable for messages unintentionally received.**

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 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. The District and its personnel are not responsible for User 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, and teachers shall notify the technology department.

Web Sites - Web sites created through the Network and/or linked with the District's official web site must relate specifically to District-sanctioned activities, programs or events. Web sites created using the Network or the District's equipment, or web sites 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 guarantee that Web sites created using means other than the District's Network will be open and reserves the right to filter them based on System Security and Integrity. 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 District functions and mission as determined by the Board.

Oregon City Schools

Network Privacy and Acceptable Use Policy
STAFF AGREEMENT – SIGNATURE PAGE

Staff Agreement

This agreement is entered into between (first and last name, please print)_____ (User) and the **OREGON CITY SCHOOLS.** I have read and I understand the Network Privacy and Acceptable Use Policy and agree to abide by all of the rules and standards for acceptable use stated within. If Users have any doubt about their obligations under this Policy, including whether a certain activity is permitted, they must consult with the Director of Technology or Network Administrator to be informed whether or not a use is appropriate.

Signature of User: _____ Date: _____

Submit this signature page to your immediate supervisor so they may request access to needed systems and sign-off. ***The remainder of this signature page should be completed by the building principal or department administrator.***

Administrator Designations *(to be completed by building principal or department administrator)*

Building(s):
❑ Administration ❑ Clay High School ❑ Fassett Junior High School ❑ Eisenhower Intermediate School
❑ Coy Elementary ❑ Jerusalem Elementary ❑ Starr Elementary ❑ District (Sub / Classified)
❑ Blackmon Center ❑ Other (specify):_____

Position:
(Choose one)
❑ Teacher ❑ Sub Teacher (Daily) ❑ Sub Teacher (Long-Term) : List cooperating teacher here
❑ Classified Staff ❑ Classified Sub ❑ Student Teacher : List cooperating teacher her .
❑ Administration ❑ Secretarial Staff ❑ NPESC Staff ❑ Adult Ed
❑ Other (specify): _____

Signature of Administrator: _____ Date: _____

Send this <u>original</u> completed form to Network Administrator, Drew Predmore, for account creation.

Technology Office Use:

Network Admin _____ Account Created Date _____ Account Expiration: _____ User Name: _____