Staff Acceptable Use Policy

Educational Purpose

The Tigard-Tualatin network and the Internet offer a wealth of educational material to District employees. Original source materials, information, data, images, and computer software may be brought into the classroom. Access to the Internet is an important part of the District's plan to create lifelong learners who have the skills to find information in a rapidly changing world. Internet access makes contact with people all over the world possible, bringing into the classroom experts in every content area.

Use of technology is a necessary element of the School District educational mission, but is furnished as a privilege, not a right. The District seeks to protect legitimate users of technology by establishing limits on such use and sanctions for those who abuse the privilege. Eliminating computer abuse provides more computing resources for users with legitimate needs.

District Acceptable Use Policy

1. Personal Safety and Respect for Privacy

a. Users will not post any personal information about other staff, students or other constituents on non-secured web resources
b. Users will promptly forward to postmaster@ttsd.k12.or.us any email message received that is inappropriate, harassing or threatening.
c. Users will respect and protect the privacy of senders and the content of messages. Messages will be re-posted only to those who have a legitimate educational or professional interest in their contents.
d. If electronic communication regarding a student is necessary (ie there is a legitimate educational interest, as defined by FERPA), users will send ONLY the student's ID number and initials for identification.

2. Illegal or Destructive Activities

a. Users will not attempt to gain unauthorized access to the District network, or to any other computer system through the District network, or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files. On occasion & with permission, IT staff members (district and school level) may need to access another staff member's account information to resolve technical issues.
b. Users will not make deliberate attempts to disrupt any computer system performance or destroy data.
c. Users will not use the District network to engage in unauthorized commercial gain and/or any illegal acts. Illegal activities shall be defined as a violation of local, state, and/or federal laws.

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, including locking of computer screen when not present/in use. Under no conditions should a user

provide his or her password to any person. (Except IT Staff)

b. Users will immediately notify their school administrator or the Director of IT if they have identified a possible security problem. Users will not search for security problems, because this may be construed as an illegal attempt to gain access. Under no conditions should a user provide *system* passwords to any unauthorized person.
c. Users will avoid the inadvertent spread of computer viruses by following the District virus protection procedures.. All computers running Windows operating system on the TTSD network MUST have district anti-virus software installed and configured by IT Staff.
d. No machine will be set up as a server until it has been registered with the District Information Technology Department.
e. Users will not purchase and/or install unauthorized computer and/or network equipment (refer to District Technology Equipment Purchasing Guidelines)

4. Inappropriate Conduct

Restrictions against inappropriate language apply to public messages, private messages, and material posted on Web pages (including social networking sites).

a. Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
b. Users will not post information that, if acted upon, could cause damage to an individual or property or has the potential to interfere with or disrupt other network users, services or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer viruses or worms, distributing quantities of information that overwhelm the system (chain letters, network games, etc.) and/or using the network to make unauthorized entry into any other resource.
c. Users will not engage in personal attacks, including prejudicial or discriminatory attacks. (Users will not submit, publish or display any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or messages either public or private.)
d. Users will not harass another person. (Users will not use the District network to engage in harassment. Harassment is defined as slurs, comments, jokes, innuendos, unwelcome compliments, cartoons, pranks, and/or other verbal conduct relating to an individual which:
    a. Has the purpose or effect of creating an intimidating, hostile or offensive environment;
    b. Has the purpose or effect of unreasonably interfering with an individual's work or school performance; or
    c. Interferes with school operations.)

    If a user is told by a person to stop sending messages, the user must stop.
e. Users will not intentionally post false or defamatory information about a person or organization.
f. Users will not utilize the District network for commercial or political activity or for personal or private gain.
g. Only District approved, secured social networking & “cloud” computing sites will be used by staff and students for classroom or curriculum enhancement. Staff members will protect student data and confidential student information by utilizing only District

approved, secured social networking & "cloud" computing sites. (refer to Board Policy JOB and FERPA regulations)

h. Staff members will utilize non-secured Internet websites (including, but not limited to, social networking & "cloud" computing sites) judiciously by not posting confidential or other personally identifiable information about students, staff or district business. (refer to Board Policy JOB and FERPA regulations)
i. Personal cellular telephones, pagers, and other digital and video devices shall be silenced during instructional [or class] time, while on duty or at any other time where such use of the device would cause a disruption of school activities or interfere with work assignments.

5. Respecting Resource Limits

a. Users will use the network only for educational and professional and/or career development activities. The network is not to be used for personal gain.
b. Users will respect disk space quotas on network file servers. Files stored on district equipment are limited to educational and curricular development.
c. Users will not post chain letters or engage in "spamming." Spamming is defined as sending an annoying or unnecessary message to a large number of people.
d. Users will check their e-mail daily, delete unwanted messages promptly, and must abide by any e-mail quota that may be established. Districts record retention policies are the responsibility of individual staff members. (board policy JO)
Users will subscribe only to educational and professional and/or career development discussion group mail-lists

6. Staff Responsibility for Supervising Students

a. Student use of computing equipment and network resources must abide by the "educational purpose" of the District infrastructure. This includes classroom activities, research, professional and/or career development.
b. Access to Internet resources is filtered, as required by CIPA. Every effort will be made to block inappropriate materials from entering the District network. Students should not try to access material that is not appropriate or attempt to circumvent access controls. If a student inadvertently accesses such information, they should immediately report it to the staff member in charge who should email the address of the inappropriate site to filter@ttsd.k12.or.us.
c. All student access to the Internet must be approved by a responsible staff member., and appropriate adult supervision must be provided.
d. All students will follow the guidelines for student safety and appropriate use that are established in the Students Rights & Responsibilities Handbook. These should be reviewed with students annually.
e. In the event that a student violates the appropriate use of technology as outlined in the Students Rights & Responsibilities Handbook, the student may be disciplined pursuant to the procedures described in State and Federal law and/or in the Students Rights & Responsibilities Handbook.
f. District policies on copyright govern the use of materials accessed through the District network. These policies will be reviewed annually with students.
g. District policies on plagiarism will govern the use of material accessed through the District network. Teachers will instruct students in appropriate research and citation

practices.

h. When using the Internet with students, teachers will select material that is relevant to the course objectives. Teachers will provide guidelines to assist their students in channeling their research activities effectively and properly.
i. Staff will not install any software on District equipment without the permission of IT staff. All installations approved by staff must comply with all District guidelines for licensure, appropriateness and the educational focus of District technology.
j. Staff use of personal equipment will follow all guidelines outlined in the Staff Acceptable Use Policy.

7. Plagiarism and Copyright Infringement

a. Users will not plagiarize works that they find on the Internet. Plagiarism is defined as taking the ideas, writings, images or materials 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 (including images, music, text, etc..) 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
c. Users will only install software to which the District has a legitimate license.
d. Staff members are responsible for licensing compliance on equipment assigned to them. This includes following all District and building procedures for tracking software licenses.

8. Inappropriate Access to Material

a. Users will not use the District network to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature). Exceptions may be made for staff engaged in bona fide research or other lawful purposes. If a project of this nature requires special access through the Internet filter, notification of the request will be sent to the building administrator
b. If a user inadvertently accesses such information, they should immediately disclose the inadvertent access by sending the email with the complete address of the offending material to filter@ttsd.k12.or.us.

9. Web Sites

a. Teachers may post student web pages that include student pictures and first name only unless the student's legal guardian requests in writing that this information not be posted. Web pages may include pictures, district telephone extension, email address and the full name of staff members unless it is requested in writing that this information not be posted.
b. Any teacher created web page must acknowledge the authorship of the page.

10. Staff use of personal equipment/software in the District:

a. Staff will not be allowed to use personal equipment on the District network. This includes peripherals used either in conjunction with District or personal equipment. A Guest wireless network will be provided for this purpose. All activities on the TTSD

Guest wireless network are subject to the Staff AUP guidelines for use.

b. Technical support for personal equipment will not be provided.
c. Staff is responsible for providing a copy of licensure for any personal software installed on District equipment.
d. Staff is responsible for ensuring that all material on personal equipment used in the District meets all District guidelines for appropriateness.
e. Staff bringing personal technology equipment for use on district property, accepts all responsibility for the equipment. The district and/or its employees will not be responsible for equipment that is lost, stolen or damaged on district property.

11. Due Process

a. In the event there is an allegation that a user has violated the District Acceptable Use Policy and Agreement, the user will be provided with a written notice of the alleged violation and an opportunity to present an explanation before an administrator.
b. Disciplinary actions will be tailored to meet specific concerns related to the specific violation and will follow procedures outlined by the collective bargaining agreements, district policy, and state and federal law.