ACCEPTABLE USE OF DISTRICT TECHNOLOGY RESOURCES

Purpose

Tacoma Public Schools provides a wide range of technology resources to its students and staff for the purpose of advancing the educational mission of the District. These resources are provided and maintained at the District’s expense and therefore, the public’s expense and are to be used by members of the school community with respect for the public trust through which they have been provided.

This Regulation outlines the appropriate and inappropriate use of District Technology Resources and personal electronic devices connected to the TPS Guest Wireless Network. This Regulation does not attempt to articulate all required or proscribed behavior by users. Employees are reminded that they are at all times subject to the District’s Employee Conduct Rules, Policy 2010, and students are reminded that they are at all times subject to the District’s Student Code of Conduct. Successful operation of the District computer network and the use of District Technology Resources requires that all users conduct themselves in a manner consistent with the Policies, Regulations, and rules that otherwise apply to them. You, the user, are ultimately responsible for your actions in accessing and using District Technology Resources and the District computer network. As a user of District Technology Resources, you are expected to review and understand the guidelines and procedures in this document. Employees are reminded that under the District’s Policy No. 5230, Job Responsibilities, “It shall be the duty of all employees to know the rules, policies, and regulations of the school and the school district.”

Scope

The following apply to all District staff and students, and covers all District Technology Resources, which include all District computer equipment (including any desktop or laptop computers provided to staff, all tablets or smart devices provided to staff), the District’s computer network, the District’s wireless network, and any software licensed to the District.

Appropriate Use

The District expects everyone to exercise good judgment and use the District’s Technology Resources in a professional manner. Employee use of District Technology Resources is expected to be related to the District’s goals of educating students and/or conducting District business. Student use of District Technology Resources is expected to be related to legitimate educational activities. The District recognizes, however, that some de minimis personal use is inevitable, and that incidental and occasional personal use of District Technology Resources that is infrequent or brief in duration is permitted so long as it occurs on personal time for staff and non-class time for students, does not interfere with District business, does not result in a material or substantial disruption of the educational environment, and is not otherwise prohibited by District policy or procedures. However, this does not create any expectation of privacy in staff or student use of District Technology Resources, as outlined in greater detail below.
Use of District Software:

District software is licensed to the District by a large number of vendors and may have specific license restrictions regarding copying or using a particular program. Users of District software must obtain permission from the District prior to copying or loading District software onto any computer, whether the computer is privately owned or is a District Computer.

Use of Non-District Software:

Prior to loading non-District software onto District Computers (including laptops, desktops, and District network drives), a user must receive permission from the District. The District will create a list of "authorized software" programs that may be loaded onto District laptops without specific permission. For example, a user will be able to load software onto a laptop that is necessary for a user to access a personal Internet service for the purpose of remotely accessing the District’s email network. All software must be legally licensed by the user prior to loading onto District Equipment. The unauthorized use of and/or copying of software is illegal.

It is against TPS practice for staff or students to copy or reproduce any licensed software on TPS computing equipment, except as expressly permitted by the specific software license. Unauthorized use of software is regarded as a serious matter and any such use is without the consent of TPS.

Remote Access:

The District provides remote access to its internal email network for the convenience of its staff. Users may access the District’s email network over a standard Internet connection by using either a District laptop or a privately-owned computer. Staff should keep in mind the importance of maintaining the security of confidential student information that may be on the staff member’s email or laptop, and should not use unsecured networks to access the District’s email network if doing so could compromise the security of the information related to District students or staff.

TPS Guest Wireless Network:

The District will maintain and provide a guest network to allow internet access for personal digital devices when possible. The district will not support or troubleshoot technical or software issues on personal digital devices.

Personal digital devices such as laptops, notebook computers, tablets, smart phones, and other personal electronic devices are permitted to connect to the District network’s via the TPS Guest Wireless Network for appropriate use in the same manner as district owned equipment.
Prohibited Use

District Technology Resources may not be used for the following purposes:

- **Commercial Use:** Using District Technology Resources for personal or private gain, personal business, or commercial advantage is prohibited.

- **Political Use:** Using District Technology Resources for political purposes in violation of federal, state or local laws is prohibited. This prohibition includes using District Technology Resources to assist or to advocate, directly or indirectly, for or against a ballot proposition and/or the election of any person to any office. The use of District Technology Resources for the expression of personal political opinions to elected officials is prohibited. Only those staff authorized by the Superintendent may express the District’s position on pending legislation or other policy matters.

- **Illegal or Indecent Use:** Using District Technology Resources for illegal, harassing, vandalizing, inappropriate, or indecent purposes (including accessing, storing, or viewing pornographic, indecent, or otherwise inappropriate material), or in support of such activities is prohibited. Illegal activities are any violations of federal, state, or local laws (for example, copyright infringement, publishing defamatory information or committing fraud). Harassment includes slurs, comments, jokes, innuendoes, unwelcome compliments, cartoons, pranks, or verbal conduct relating to an individual that (1) have the purpose or effect or creating and intimidating, a hostile or offensive environment; (2) have the purpose or effect of unreasonably interfering with an individual’s work or school performance, or (3) interfere with school operations. Vandalism is any attempt to harm or destroy the operating system, application software or data. Inappropriate use includes any violation of the purpose and goal of the network. Indecent activities include violations of generally accepted social standards for use of publicly-owned and operated equipment.

- **Non-District Employee Use:** District Technology Resources may only be used by District staff and students, and others expressly authorized by the District to use the equipment.

- **Disruptive Use:** District Technology Resources may not be used to interfere or disrupt other users, services or equipment. For example, disruptions include distribution of unsolicited advertising (“Spam”), propagation of computer viruses, distribution of large quantities of information that may overwhelm the system (chain letters, network games, or broadcasting messages), and any unauthorized access to or destruction of District Technology Resources or other resources accessible through the District’s computer network ("Cracking" or "Hacking").

- **Student use of the District’s Technology Resources** must comply with the District’s Student Code of Conduct, Policies, Regulations, and school rules that apply to students, including but not limited to prohibitions concerning harassment, intimidation and bullying as provided in Policy No. 3207 and its associated Regulation, 3207R.

- **Shall not encrypt communications and digital data so as to avoid security review unless otherwise required for business related purposes and approved in advance by the superintendent or designee. If any data needs to be encrypted, users shall consult with the**
Technology Services Department, from which encryption protocol and keys shall be provided. All encryption keys shall be provided to the Office of the General Counsel or authorized staff for the purpose of security.

- Do not engage in any "spamming" or other activities that could clog or congest Internet networks

**No Expectation of Privacy/Potential for Disciplinary Action**

District Technology Resources, the Internet and use of email are not inherently secure or private. For example, the content of an email message, including attachments, is most analogous to a letter or official memo rather than a telephone call, since a record of the contents of the email may be preserved by the sender, recipient, any parties to whom the email may be forwarded, or by the email system itself. It is important to remember that once an email message is sent, the sender has no control over where it may be forwarded and deleting a message from the user’s computer system does not necessarily delete it from the District computer system. In some cases, emails have also been treated as public records in response to a public records disclosure request or student records in response to request by parents to review student educational records. Likewise, files, such as Internet “cookies” (explained more fully below) may be created and stored on a computer without the user’s knowledge. Users are urged to be caretakers of your own privacy and to not store sensitive or personal information on District Technology Resources. The District may need to access, monitor or review electronic data stored on District Technology Resources, including email and Internet usage records.

While the District respects the privacy of its staff and students, the District reserves the right to monitor the use of District Technology Resources for any legitimate business or educational reason. Employees and students should have no expectation of privacy in emails sent to or from a District email account. Employees should always remember that any email may be subject to disclosure as either a public or student record. The District may monitor and review the information in order to analyze the use of systems or compliance with policies, conduct audits, review performance or conduct, obtain information, or for other reasons. The District reserves the right to disclose any electronic message to law enforcement officials, and under some circumstances, may be required to disclose information to law enforcement officials, the public, or other third parties, for example, in response to a document production request made in a lawsuit involving the District or by a third party against the user or pursuant to a public records disclosure request.

The Appropriate Use Procedures are applicable to all users of District Technology Resources and refers to all information resources whether individually controlled, shared, stand alone or networked. Disciplinary action, if any, for students, staff, and other users shall be consistent with the District’s standard policies and practices. Violations may constitute cause for revocation of access privileges, suspension of access to District Technology Resources, other disciplinary action, and/or appropriate legal action. Specific disciplinary measures will be determined on a case-by-case basis.
Care for District Technology Resources

Users of District Technology Resources are expected to respect the District’s property and be responsible in using the equipment. Users are to follow any District instructions regarding maintenance or care of the equipment. Users may be held responsible for any damage caused by your intentional or negligent acts in caring for District Technology Resources under your control. The District is responsible for any routine maintenance or standard repairs to District Technology Resources. Users are expected to timely notify the District of any need for service. Users are not to delete or add software to District Technology Resources without District permission. Due to different licensing terms for different software programs, it is not valid to assume that if it is permissible to copy one program, then it is permissible to copy others.

If a District laptop is lost, damaged or stolen while under the control of a user, the user is expected to file a claim under his/her insurance coverage, where coverage is available. Except in cases of negligent or intentional loss or damage, the District will cover out-of-pocket expenses.

Other Users Access to Technology Resources

Individuals from outside the district (i.e., parents, PTA members, community members, contractors, consultants, interns, vendors, volunteers) requesting access to Technology Resources must sign the “Digital Resources” form for Non-District Employee.” The school/department administrator shall review the acceptable use policy for Technology Resources and associated regulations with all outside individuals prior to any use of District Technology Resources. Copies of the form shall be filed with the Technology Services Department.

Using Email and the Internet Wisely

Using Email Wisely

• Email encourages informal communication because it is easy to use. However, unlike a telephone call however, email creates a permanent record that is archived and often transmitted to others. Remember that even when you delete an email from your mailbox; it still may exist in the system for some period of time.

• Be circumspect about what you send and to whom. Do not say anything in an email that you would not want to see republished throughout the District, in Internet email, or on the front page of the Eastside Journal. Remember that email invites sharing; a push of the button will re-send your message worldwide, if any recipient (or hacker) decides to do so. What you say can be republished and stored by others.

• Beware of the "Reply All" button. Often your message only needs to be returned to one individual -- is the message really appropriate for (and should it really take the time of) everyone on the address list.

• You can create liability for yourself and the District. For example, within or outside the District, if you "publish" (type or re-send) words that defame another individual or disparage another individual or institution, if you upload or download or re-send copyrighted or pornographic material, if you use email to harass or discriminate against
Regulation 6973R

someone, or if you send private information or data about someone, you may violate applicable laws and District policy. Make sure none of your activities violate any law or policy.

• Please keep in mind that because of intermediary server problems and other potential delays, Internet email can sometimes take anywhere from five minutes to several days to arrive. It may not be the best means to send time-sensitive information.

• Finally, beware of sending attachments. They may arrive garbled if the recipient is using a different email system.

• Email attachments can introduce viruses into the District system, and you can introduce a virus into a recipient’s system by forwarding an infected attachment. This is especially likely if the attachment arrives from an unknown source via the Internet. If you do not know the sender of Internet email, consider routing the message to the MIS staff who can open the attachment for you on a computer isolated from the District network. While that should prevent activating a virus, it will not stop certain other infections (e.g., a logic bomb). Please do not open attached files ending in "EXE," "BAT," or "COM," as these files may be viruses or programs designed to delete data from the computer.

Using Internet Access Wisely

• Be circumspect about where you go and what you do. Do not visit any site or download or share any material that might cause anyone to question your professionalism, or the District’s.

• Read the "License" or "Legal" contract terms on every site. Do not purport to bind the District to any license or other contract. If you make an agreement on your own behalf, do not violate that agreement using the District equipment or Internet account.

• Do not assume that just because something is on the Internet, you may copy it. As a general rule, assume that everything is copyrighted and do not copy it unless there is a notice on the site stating that you may do so. For example, if you see a clever cartoon assume that you may NOT copy it. Governmental documents are an exception (you may copy them), but you must confirm that it is the "government" and not a government related entity such as the post office.

• Be aware of the "Do you want a cookie?" messages (if you have configured your browser to get such messages). If you answer yes, whatever activity in which you are engaged will be logged by the site owner to help it or its advertisers develop a profile about you or the District. It is possible that your browser is set to accept cookies without asking you each time.

• You can create liability for yourself and the District. For example, if you "publish" (type or re-send) words that defame or disparage another individual or institution, if you upload or download or re-send copyrighted or pornographic material, if you use the Internet to harass or discriminate against someone, or if you provide private information or data about someone, you may violate applicable laws or District policy. Make sure none of your activities violate any law or policy.
References

Cross References:
- Policy 2025: Copyright Compliance
- Regulation 2025R: Copyright Compliance
- Policy 3200: Student Rights and Responsibilities
- Policy 5230: Job Responsibilities
- Policy 5251: Conflict of Interest
- Policy 6210: Purchasing
- Regulation 6250.1: Use of District-Owned Material and Equipment
- Regulation 6250.2: Use of District Telephones
- Regulation 6250.3: Wireless Communications

Legal References:
- RCW 28A.600.010: Government of schools, pupils, employees, rules and regulations for--Due process guarantees-Enforcement

Adopted: 1/3/2012, Revised, 5/15/2015