

Acceptable Use Policy for Digital Resources

Digital resources are maintained for the purpose of supporting the education of students and the goals of the district. All students, staff and other users must adhere to federal and state laws and district policies and regulations applying to the use of all digital resources. District access to the Internet shall be allowed via TEDNET only. The district reserves the right at all times to make the sole and final decision as to what is deemed inappropriate, unethical, obscene and/or unacceptable use of any digital resources. This determination shall be made by the superintendent or designee.

It is the responsibility of all district administrators to annually review the acceptable use policy for digital resources with all staff assigned to their school/department. During the course of the year, the school/department administrator shall review the policy with all new staff during the school/department orientation.

Staff, students and other users are cautioned to carefully evaluate information carried, stored or manipulated on district resources (i.e., the Internet). Since there is no regulation of material or assurance of accuracy of information placed on these sources, care must be exercised in the use of these materials.

Student Access to Digital Resources

All students shall have the ability to access the Internet and other digital resources via district computers and/or other district equipment. Staff shall review the Acceptable Use Policy for Digital Resources with all students using district computers. After completing the proper review procedures, students shall be allowed Internet access via TEDNET only.

If a parent/guardian does not wish their student to participate in the use of Internet access, the parent must sign a "Student Internet Restriction" form. Copies of the "Student Internet Restriction" form shall be retained in appropriate locations as well as in the student's cumulative folder. This form is only valid for the student's stay at a particular school. A new "Student Internet Restriction" form must be signed when moving from one school to another or upon reentry to a school previously attended.

Staff Access to Digital Resources

All district staff members requiring access to district digital resources shall complete a "Digital Resources Form." The digital resources form must have the staff member's signature and approval of the school/department administrator.

No person shall access digital resources without receiving appropriate training. Each staff member shall be given a 45-day grace period to obtain the necessary training. If staff is familiar with the use of E-mail and Internet, they may complete the “E-mail and Internet Training Waiver” form. It is the responsibility of each staff member to become familiar with the acceptable use policy for digital resources and associated regulations. After completing the proper form(s) and procedures, staff members shall be allowed to access digital resources. Internet access is allowed via TEDNET only. Copies of the approved “Digital Resources” form and “E-mail and Internet Training Waiver” form shall be filed in Computer Services, the employee’s personnel folder, and in other appropriate locations.

Computer services shall be notified by the human resources department of any staff member leaving the employment of the district (e.g., resignation, termination, retirement, short- or long-term leave of absence). Once notified of the effective date, computer services shall terminate all access to digital resources. Staff members who transfer from one location to another location shall also have their digital resources terminated until a new “District Resource” form has been completed with proper signatures.

Other Users Access to Digital Resources

Individuals from outside the district (i.e., parents, PTA members, volunteers) requesting access to digital resources must sign the “Digital Resources” form specifying the category of “Other.” The school/department administrator shall review the acceptable use policy for digital resources and associated regulations with all outside individuals before the individual is allowed use of any district digital resources. Copies of the form shall be filed in Computer Services Department and in other appropriate locations.

Penalties for Violation of the Acceptable Use Policy for Digital Resources

Use of district digital resources that does not directly support classroom learning and/or administrative function may be considered to be inappropriate use. Inappropriate use of digital resources may be cause for disciplinary action(s) consistent with the district’s policies and regulations, and may also result in revoking access privileges to digital resources, initiating legal action(s), and/or taking any action(s) deemed necessary for the inappropriate activity.

Acceptable Use Guidelines

A. Network

1. All district digital resources are maintained for the purpose of supporting the education of students and the goals of the district.
2. The digital resources must be used in conformity with all state and federal laws, licenses and district policies.
3. Use of the digital resources for commercial solicitation is prohibited. Use of the digital resources for charitable purposes must be approved in advance by the superintendent or designee.
4. No use of the digital resources shall serve to disrupt the district operations; digital resources components including hardware and software shall not be destroyed, modified or abused in any way.
5. Communications and digital data may not be encrypted so as to avoid security review. Attempts to bypass district web blocking or filtering software by using external proxy servers or client software (i.e. America Online) or the encryption of stored data or programs shall be considered a direct attempt to violate the district acceptable use policy for digital resources.
6. Malicious use of digital resources to harass others or gain unauthorized access to any computer or the network or its components, thereof, is prohibited. Users are responsible for the appropriateness and content of data they store, transmit and/or publish on the network. Hate mail, harassment, discriminatory remarks or other antisocial behaviors are expressly prohibited. No person shall use the digital resources to discriminate on the basis of gender, race, ethnic origin, age, disability, sexual orientation or marital status.
7. Subscriptions to mailing lists, bulletin boards, chat groups and commercial on-line services and other information services must be pre-approved by the superintendent or designee.

8. No person shall use digital resources for political action activities, which include support or opposition of political candidates or ballot measures.
9. Use of digital resources to access, store or distribute obscene, pornographic or other inappropriate material is prohibited.

B. Digital Resources Security

1. Security authorization accounts are to be used only by the authorized owner of the account. Users may not share their user identification (ID) or password(s) with another person or leave an open file or session unattended or unsupervised. Account owners are responsible for all activity under their account.
2. Users shall not seek information on, obtain copies of, or modify files, user IDs, passwords or data belonging to other users; misrepresent other users on the network; and/or attempt to gain unauthorized access to other digital resources. No person shall transmit deliberately falsified information.
3. Students shall not be given security or permission to use computers to access the student information system, financial system or human resources system of the district.
4. All users shall notify the technology hotline immediately if they identify a security problem of any type. Security of district digital resources is of the highest priority, since they contain critical data that is vital to the operation of the district.
5. Users must change their network password every 120 days to ensure the integrity and security of the district's digital resources. Users shall be notified upon login when their network password has expired. Each user shall be given two additional 'grace login' opportunities to change their password. Once the grace period has expired, the user must contact computer services to reapply for a new password.

C. Personal Security

1. Users shall avoid easily guessed passwords (i.e., birth dates, child's name, phone numbers).

2. Users shall not use passwords assigned to others or access systems where authorization has not been given.
3. Personal information such as addresses and telephone numbers must remain confidential when communicating via the Internet or stored on any district digital resource. Students must never reveal such information without permission from their teacher or other supervising adult.
4. Students must never make appointments to meet people in person that they have contacted on the Internet without district and parent permission.
5. Students must notify their teacher or other supervising adult whenever they come across inappropriate or questionable information or messages that are dangerous or contain information that makes them feel uncomfortable.

D. Copyright

1. The unauthorized installation, use, storage or distribution of copyrighted software or materials on district computers is prohibited, pursuant to Policy No. 2025, "Copyright Compliance."

E. General Use

1. Diligent effort must be made to conserve district digital resources. Users shall frequently delete electronic mail, voice mail and unused files.
2. Nothing in this regulation is intended to preclude the supervised use of the digital resources while under the direction of a teacher or other approved user acting in conformity with district policies, regulations and procedures.
3. No person shall steal data, information, equipment or intellectual properties (software or other copyrighted material) through or from district digital resources.

F. District Liability

1. The district shall not be held liable for the following:

- a. Any information that may be lost, damaged or unavailable due to technical or other difficulties.
- b. Information retrieved through any network.
- c. Contracts or legally binding agreements or financial obligations without following purchasing procedures, pursuant to Policy No. 6210, "Purchasing."

G. Confidentiality/Monitoring of Information

- 1. All district digital resources are the property of Tacoma School District. Since many users share the digital resources, information within the district shall not be considered confidential unless specifically identified as such by state or federal laws. The Tacoma School District reserves the right to prioritize use and access to the network and other digital resources.
- 2. All digital resources are subject to monitoring, editing, discarding and/or disclosure solely at the discretion of the district and without notice.
- 3. Web page development shall follow the district guidelines and shall be hosted on the district web servers.

H. Remote Access

- 1. Remote access to digital resources shall be considered the same as on-site district facility use and shall fall under the same policies and regulations.
- 2. Remote access to digital resources from personal home computers is prohibited unless granted by the superintendent or designee.
- 3. Use of modems within the district is prohibited unless approval is granted by the superintendent or designee.

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

Approved 3/19/02