

Acceptable Use Regulation for Digital Resources

1.0. Overview

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..

Student access to the Internet shall be allowed via the District network 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 shall be cautioned to carefully evaluate information carried, stored or manipulated on district digital resources. 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.

2.0. Student Access to Digital Resources

All students should 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 and Regulation for Digital Resources with all students using district computers. After completing the proper review procedures, students shall be allowed Internet access via District network. Students shall be aware that use of the District digital resources for accessing, storing and distributing inappropriate websites, graphics, materials, messages; and for harassment and cyber bullying is strictly prohibited.

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.

3.0. Staff Access to Digital Resources

All district staff members requiring access to district digital resources for their work related purposes shall complete a “Digital Resources Form” *for District Employee*. The form must have the staff member’s signature and approval of the school/department administrator.

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.. Copies of the approved “Digital Resources” form shall be filed in Human Resources Department. .

Technology Services shall be notified by the human resources department at least one day prior to the effective date of any staff member change of status. Once notified of the effective date, Technology Services shall take appropriate action associated with access privileges.

4.0. Other Users Access to Digital Resources

Individuals from outside the district (i.e., parents, PTA members, contractors, consultants, volunteers) requesting access to digital resources must sign the “Digital Resources” form *for Non-District Employee*.” 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 Technology Services Department.

5.0. Personal Digital Devices

1. All personal digital devices such as laptop, desktop computers and other devices shall not be allowed to physically connect to the District network or plug in to the computers or other digital equipment unless otherwise necessary and approved by the superintendent or designee. If approval is given to allow personal devices access to the District network, Technology Services team should be notified in advance in an appropriate amount of time, so that necessary services could be arranged and provided smoothly.
2. The primary means for connecting the personal digital devices to the District network, if approval is granted, will be via the District “*Guest*” network or any network segment assigned by Technology Services.
3. Any personal digital device connected to the District network shall have most updated Operating System (OS) patches and ant-virus software with the most updated virus signature files properly installed and configured.

6.0. Security

6.1. Network Security

1. All district digital resources are maintained for the purpose of supporting the education of students and the goals of the district. Use of the District digital resources for personal business or other inappropriate purposes is prohibited.
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. Users shall not encrypt communications and digital data so as to avoid security review unless otherwise required for business related purposes and approved by superintendent or designee. If any data needs to be encrypted, users shall consult with Technology Services Department, from which encryption protocol and keys shall be provided. All encryption keys shall be provided to the District legal department or authorized staff for the purpose of security and legal review.
6. Attempts to bypass district web blocking or filtering software by using external proxy servers or client software or the encryption of stored data or programs shall be considered a direct attempt to violate the district acceptable use policy for digital resources.
7. Malicious use of the District digital resources to harass others or gain unauthorized access to any computer or the network or its components, thereof, is prohibited. Users shall be responsible for the appropriateness and content of data they store, transmit and/or publish on the network. Hate mail, harassment, cyber bullying, discriminatory remarks or other antisocial behaviors shall be expressly prohibited. No person shall use the digital resources to discriminate on the basis of gender, race, ethnic origin, age, disability, religion, political belief, sexual orientation or marital status.
8. Using the district digital identification (username and password) to subscribe 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.

9. No person shall use digital resources for political action activities, which include support or opposition of political candidates or ballot measures.
10. Use of digital resources to access, store or distribute obscene, pornographic or other inappropriate material is prohibited.
11. Devices with dual network adapters (LAN and Wireless LAN cards) or equipped with other connectivity devices must have Wi-Fi card turned off or disabled while connecting to the District network.

6.2. Digital Resources Security

1. Users shall 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 activities under their accounts.
 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 District mission-critical applications or confidential data.
 4. Staff members shall pay attention and take good care of portable devices assigned to them when taking those devices out of the office. Staff members shall not keep those devices unattended in the public places or in the unlocked vehicles.
 5. No mission-critical application and/or confidential data shall be stored on mobile devices unless otherwise securely encrypted with an acceptable encryption standard approved and supported by Technology Services Department.
1. All users shall notify the Technology Services 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. In case of any loss of the District digital devices occurs, staff members shall notify Technology Services immediately, so that appropriate preventative actions will be taken.

6.3. Personal Security

1. New users shall change their password upon the first login and existing users shall change their 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.
2. Users should avoid blank and easily guessed passwords such as birth dates, child's name, phone numbers, address, other personal information, and dictionary words. The strong password shall be applied in minimum of eight characters long and shall contain digits (0-9), characters (lower and upper case), and special characters (!@#%*&). The password shall not be left unattended or shared with other people.
3. Users shall not use ID and passwords assigned to others or access data, information, and systems where authorization has not been given. Users shall keep ID and password assigned to them secure and safe and shall not transfer this information to other users.

4. Student 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.
5. Students must never make appointments to meet people in person that they have contacted on the Internet without district and parent permission. Using the District digital resources to make such appointments shall be strictly prohibited.
6. 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.

6.4. Copyright

The unauthorized installation, use, storage or distribution of copyrighted software or materials on district computers is prohibited, pursuant to Policy No. 2025, "Copyright Compliance." Users shall not install any unauthorized software or change configuration settings on the District computers.

7.0. General Use

1. Diligent effort must be made to conserve district digital resources. Users should appropriately maintain and manage digital resources assigned to them, 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.

8.0. 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 monitor, prioritize use and access to the network and other digital resources.
2. All digital resources are subject to reviewing, 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.
4. Staff members shall not use public email accounts for communication related to the District business purposes and exchanging any information confidential to the District.

9.0. Remote Access

Remote access to digital resources shall be considered the same as on-site District facility use and shall fall under the same policy, regulation, and Remote Access Procedure.

10.0. Enforcement

Any user who violates this regulation shall be subject to appropriate disciplinary action.

11.0. 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