

WESTMORLAND UNION ELEMENTARY SCHOOL DISTRICT

BOARD POLICY NO. 4022: TECHNOLOGY USE POLICY

1. Overview

- 1.1. This Technology Use Policy (“Policy”) applies to all users of the technology resources of the Westmorland Union Elementary School District (“District”).
- 1.2. As used herein, the term “technology resources” includes, but is not limited to, the District’s website, computers, hardware, software, data files, computer files, operating systems, security systems, networks, intranets, Internet access, e-mail systems, telephone systems, voice mail systems, facsimile systems, data transmission equipment, cables, fixtures, electronic storage media and drives, and all user communications and files.
- 1.3. As used herein, the term “user” includes District employees, students, and other individuals authorized by the District Superintendent or Technology Director to use the District’s technology resources. “Technology Director” means the District employee charged with primary oversight and maintenance of the District’s technology resources.

2. Purpose and Permissible Uses

- 2.1. The District provides its employees and students with the privilege of using its technology resources for the performance of employee work duties, student educational uses, and certain limited uses as set forth below. All District technology resources, as defined above, shall remain the sole and exclusive property of the District. Prior to using such resources, users must receive adequate District instruction regarding usage. District employees shall also review, sign, and return the attached form entitled Employee Acceptance of Technology Use Policy prior to use. Students will be provided instruction regarding the policy and execute an appropriate form provided by the Superintendent prior to being provided access to District technology resources. The District may restrict or revoke user access at any time and at its sole discretion.
- 2.2. District employees shall use District technology resources almost exclusively to fulfill their work duties but may in certain circumstances make limited personal use of such resources. Any employee’s personal use of such resources must: 1) be incidental or minimal, 2) not be on work time, 3) not interfere with employee work duties, 4) not adversely affect the performance of District technology resources, 5) not involve political activities or activities for personal financial gain, and 6) not violate other sections of this Policy or applicable local, state, or federal law. Students may not use the District’s technology resources for personal use.
- 2.3. Employees affiliated with official District employee organizations may use District technology resources for the limited purpose of communicating with other District employees regarding matters within the organization’s purpose. Such use must: 1) be incidental or minimal, 2) not be on work time, 3) not interfere with employee work duties, 4) not adversely affect the performance of District technology resources, 5) not involve political activities such as elections, campaigns, or voting, and 6) not violate other sections of this Policy or applicable local, state, or federal law.

- 2.4. If any personal or union-related use of District technology resources becomes excessive, unreasonable, impracticable, or unaffordable, the District may revoke such use at anytime and at its sole discretion.
- 2.5. Equipment or other technology resources covered by this Policy may be taken off-site (i.e., off District grounds) by employees only for work purposes and with the authorization of the Superintendent or Technology Director. No equipment may be taken off-site for personal, commercial, or union-related use. Whether on-site or off-site, employees shall care for District technology resources in a reasonable manner. An employee may be subject to discipline and potential financial liability for loss or damage to District property resulting from reckless or intentional misuse.
- 2.6. Pursuant to the Family Educational Rights and Privacy Act (“FERPA”), District employees shall not disclose personal student information unless authorized in writing by the student or parent/guardian or unless otherwise authorized by FERPA or other applicable law.
- 2.7. The District shall use its best efforts to block or filter obscene, pornographic, or patently offensive materials from its technology resources. Parents or guardians who desire that their children not be granted internet access should inform the District in writing and state the reasons therefore. The District will use its best efforts to respect such requests.

3. Prohibited Uses

- 3.1. The District recognizes that the use of its technology resources may at times result in unauthorized access, improper use, or other ill effects. This Policy thus sets forth appropriate usage limits by prohibiting reckless or intentional misuse or attempted misuse of District technology resources. Such misuse or attempted misuse may result in discipline up to and including termination of employment for employees or suspension or expulsion for students. Specific examples of prohibited reckless or intentional misuse by users include, but are not limited to, the following:
 - 3.1.1. Causing or engaging in unauthorized alteration, duplication, deletion, removal, dissemination, malfunction, damage, or theft of District technology resources;
 - 3.1.2. Placing unlawful or harmful materials or programs on District technology resources, including but not limited to computer viruses, Trojan horses, or worms;
 - 3.1.3. Accessing or using restricted files, networks, and systems without authorization, or bypassing District firewalls used for security or blocking certain internet sites;
 - 3.1.4. Making unauthorized changes to passwords, access codes, or security information, or placing physical locking devices on District technology resources;
 - 3.1.5. Violating or permitting the violation of the legal privacy rights of individuals whose information is routinely stored on District technology resources;
 - 3.1.6. Using another user’s account or password to send or receive communications or masking the identity of a user account or system;
 - 3.1.7. Reproducing or using any copyrighted or licensed material in violation of applicable copyright or trademark law or licensing agreements;
 - 3.1.8. Installing or loading a user’s personal programs or software on District

technology resources for personal use or non-District activities;

- 3.1.9. Using District technology resources for: 1) political activities, elections, personal financial gain, or gambling, 2) unlawful discrimination, harassment, libel, or slander, or 3) any other use in violation of District policy or applicable law;
- 3.1.10. Preparing, transmitting, downloading, displaying, accessing, or connecting to obscene, pornographic, or patently offensive materials, including but not limited to images, writings, or recordings, or materials descriptive of destructive devices or harmful matter as defined by Penal Code section 313(a);
- 3.1.11. Sending a mass e-mail or communication to all District users unless authorized by the Superintendent or Technology Director;
- 3.1.12. Participating in or engaging in chain letters, chat rooms, spamming, hacking, or similar activities. "Spamming" means sending indiscriminate, non-District related e-mail or junk e-mail to multiple mailing lists, individuals, users, or newsgroups. "Hacking" means accessing District technology resources or other third party networks, computer systems, or files illegally or without permission.

4. Monitoring and Maintenance

- 4.1. Users should be aware that records relating to usage of District technology resources may remain on District systems despite efforts to delete such information. Although messages, files, website usage, or other data may appear deleted, they are typically stored on backup systems and may be accessed by the District or law enforcement authorities requesting such information.
- 4.2. The District may monitor, remove, or maintain at anytime and for any reason any and all information recorded or stored on its technology resources, whether personal or related to District business. Such monitoring, removal, or maintenance may occur in a variety of circumstances including, but not limited to, the following: routine business activities; need for information in a user's absence; searches for District documents or other information; maintenance, repair, or troubleshooting of District technology resources; suspected misuse or illegal activities; criminal investigations; in response to subpoenas or court orders; or other potential circumstances.
- 4.3. Monitoring and maintenance may involve inspection and review of a user's activities, usage, files, hardware, communications, and any other tangible or intangible District technology resource. The District may disclose any such records or materials to appropriate law enforcement authorities or other third parties as required by local, state, or federal law. By using the District's technology resources, users consent to the monitoring and review of such resources by the District or authorized third parties.
- 4.4. Users should not expect or assume that personal information which they store or record on District technology resources will be private. As used herein, the terms "personal" or "personal information" refer to any information, which a user records, saves, or otherwise introduces into District technology resources, whose introduction the District did not require or which is unrelated to District business and to District needs.
- 4.5. The Superintendent or Technology Director may occasionally establish or modify user account storage limits depending on available technology resource capacity.

Information in a user's account that exceeds applicable storage limits may be deleted, modified, or removed with or without notice.

5. Security

- 5.1. The District will use its best efforts to block or filter unauthorized access, viruses and other harmful programs, obscene, pornographic, or patently offensive materials, and other security risks. Users shall not disable or make unauthorized changes to any security system on District technology resources, including but not limited to virus detection software, filtering software, password protection, or similar systems.
- 5.2. Users should be aware that communications via the internet are sometimes susceptible to eavesdropping by third parties. When possible, users should refrain from sending information of a confidential and personal nature via the internet.
- 5.3. A user account and password must be established before a user can access District technology resources. The use of passwords does not mean that user personal information is completely private. The District may monitor and review user activity.
- 5.4. Users shall not disclose their passwords or remote access numbers or use another user's account or password unless authorized by the Superintendent or Technology Director. Users shall shut down their workstations when not in use, log out, or use a password protected screen saver. The Superintendent or Technology Director may periodically require users to establish new user account names or passwords.

6. Reporting Abnormalities or Misuse

- 6.1. Users shall immediately report observed or known misuses, abnormalities, or security breaches of District technology resources to the Superintendent or Technology Director. Users shall not allow anyone aside from the Superintendent, Technology Director, or their designees to observe potentially offensive, obscene, or like materials.
- 6.2. Upon learning of any abnormalities or misuse, the Superintendent, Technology Director, or their designees shall review the applicable technology resources or materials. The Superintendent may report any suspected illegal activities to appropriate law enforcement authorities.

7. Licenses and Copyrights

- 7.1. The District purchases software licenses and does not own the copyright thereto or related documentation. The Technology Director or his or her designee shall be responsible for loading licensed software and removing any known unlicensed software. The Technology Director will centrally store all software programs and licenses.
- 7.2. Users shall use software in accordance with their licensing agreements and refrain from making unauthorized reproductions of software or related documentation.
- 7.3. The District retains the copyright to any material deemed to be District proprietary materials or information. Use of District propriety materials and information shall be in accordance with applicable copyright law and District policy.

8. Discipline

- 8.1. The consequences for violating any provision of this Policy include, but are not limited to, one or more of the following:
 - 8.1.1. For employees, disciplinary action up to and including termination of employment;
 - 8.1.2. For students, disciplinary action up to and including suspension or expulsion;
 - 8.1.3. And where applicable, referral to appropriate law enforcement authorities for suspected illegal activities.

9. District Immunity

- 9.1. At times, the District’s technology resources may fail or may require repair or maintenance. The District shall not be liable for loss or damage to user data, materials, or information caused by, among other things, system failures, server crashes, or monitoring, maintenance, removal, or repair of District technology resources.
- 9.2. The District shall not be liable for a third party’s unauthorized access to personal information as defined in Section 4 above.
- 9.3. The District shall not be liable for a user’s unauthorized or illegal duplication of software or copyrighted materials in violation of copyright or software agreements.

10. Rules Specific to Students

10.1 Teachers will review with students annually the rules set forth below regarding student use of technology resources emphasizing that these rules will be enforced for their safety:

10.1.1 Students shall use computers and technology resources for educational purposes only and not for personal use.

10.1.2 Students shall only use computers designated for student use, and not gain access to or attempt to gain access to computers utilized by District employees.

10.1.3 Students shall only use computers while under the supervision of a certificated employee unless an education program permits students to take laptop computers home.

10.1.4 Students shall not have access to or be provided access to electronic mail.

10.1.5 Students shall not have access to or be provided access to passwords.

10.1.6 Students shall not access or attempt to access illegal websites including, but not limited to, unlicensed software websites, illegal music download

or

adult content websites.

10.1.7 Students shall not place in computers or on the internet personal disks or personal information by which persons outside of the school could

identify

them, such as their home or school addresses or telephone numbers.

10.1.8 Students shall not gain or attempt to gain access to the network or to

modify the network.

10.1.9 Students are expressly prohibited from visiting “chat rooms.”

10.1.10 Students are not to use computers in such a manner as is likely to result in damage to them.

Legal Reference:

Education Code §§ 220 (prohibition of discrimination), 230 (prohibition of sexual harassment), 7050-7058 (political activities of school officers and employees), 49069, 49076, 49077 (access to student records and disclosure by court order or subpoena)

Government Code §§ 1126 (incompatible employment activities by local agency employees), 3201-3209 (political activities of public employees), 12940 (prohibited discrimination)

Penal Code §§ 313-313.5 (prohibition of harmful matter), 422.6 (prohibition of hate crimes and hate speech), 502 (prohibition of unauthorized access/use of computer systems and data)

Code of Civil Procedure § 1985.6 (subpoenas of employee records)

Business & Professions Code §§ 17529-17529.9, 17538.45 (anti-spam act)

Federal Law: U.S.A. Patriot Act, Public Law 107-56 §§ 210, 212, 215, 216, 507; Children’s Internet Protection Act, 47 U.S.C. §§ 254(h), 254(l); Computer Fraud and Abuse Act, 18 U.S.C. § 1030 et seq.; Federal Anti-Spam Act, 15 U.S.C. §§ 7701-7713; Family Education Rights and Privacy Act, 20 U.S.C. § 1232g

Date Policy Adopted By The Board:

WESTMORLAND UNION ELEMENTARY SCHOOL DISTRICT

EMPLOYEE ACCEPTANCE OF TECHNOLOGY USE POLICY

I have thoroughly read and understand each and every provision of the District's Technology Use Policy, Board Policy 4022 (the "Policy"). I knowingly and voluntarily agree to comply with each and every provision of the Policy and to abide by local, state, and federal law applicable to the District's technology resources. I understand that I may be subject to appropriate discipline, up to and including termination of employment, if found in violation of this Policy. I also understand that any suspected illegal activities via the District's technology resources may be reported to appropriate law enforcement authorities. I further understand that my use of such resources is subject to monitoring at any time and that I retain no rights of privacy or ownership in any materials or information on such resources. I further understand and agree that this acceptance and acknowledgement agreement shall be placed in my personnel file and shall be a prerequisite to my use of District technology resources.

Signature of Employee

Date

Printed Name of Employee