EMPLOYEE USE OF TECHNOLOGY

The Governing Board recognizes that technological resources enhance employee performance by offering effective tools to assist in providing a quality instructional program; facilitating communications with parents/guardians, students, and the community; supporting district and school operations; and improving access to and exchange of information. The Board expects all employees to learn to use the available technological resources that will assist them in the performance of their job responsibilities. As needed, employees shall receive professional development in the appropriate use of these resources.

(cf. 0440 - District Technology Plan)
(cf. 1100 - Communication with the Public)
(cf. 1113 - District and School Web Sites)
(cf. 1114 - District-Sponsored Social Media)
(cf. 4032 - Reasonable Accommodation)
(cf. 4131 - Staff Development)
(cf. 4231 - Staff Development)
(cf. 4331 - Staff Development)

Employees shall be responsible for the appropriate use of technology and shall use district technology primarily for purposes related to their employment.

(cf. 0410 - Nondiscrimination in District Programs and Activities)
(cf. 4119.11/4219.11/4319.11 - Sexual Harassment)
(cf. 4119.21/4219.21/4319.21 - Professional Standards)
(cf. 4119.23/4219.23/4319.23 - Unauthorized Release of Confidential/Privileged Information)
(cf. 4119.25/4219.25/4319.25 - Political Activities of Employees)
(cf. 5125 - Student Records)
(cf. 5125.1 - Release of Directory Information)
(cf. 6162.6 - Use of Copyrighted Materials)
(cf. 6163.4 - Student Use of Technology)

District technology includes, but is not limited to, computers, the district's computer network including servers and wireless computer networking technology (wi-fi), the Internet, email, USB drives, wireless access points (routers), tablet computers, smartphones and smart devices, telephones, cellular telephones, personal digital assistants, pagers, MP3 players, wearable technology, any wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off site or through district-owned or personally owned equipment or devices.

The Superintendent or designee shall establish an Acceptable Use Agreement which outlines employee obligations and responsibilities related to the use of district technology. Upon employment and whenever significant changes are made to the district's Acceptable Use Agreement, employees shall be required to acknowledge in writing that they have read and agreed to the Acceptable Use Agreement.

Employees shall not use district technology to access, post, submit, publish, or display harmful or inappropriate matter that is threatening, obscene, disruptive, sexually explicit, or unethical or that promotes any activity prohibited by law, Board policy, or administrative regulations.

EMPLOYEE USE OF TECHNOLOGY (continued)

Harmful matter includes matter, taken as a whole, which to the average person, applying contemporary statewide standards, appeals to the prurient interest and is matter which depicts or describes, in a patently offensive way, sexual conduct and which lacks serious literary, artistic, political, or scientific value for minors. (Penal Code 313)

The Superintendent or designee shall ensure that all district computers with Internet access have a technology protection measure that protects against access to visual depictions that are obscene, child pornography, or harmful to minors and that the operation of such measures is enforced. The Superintendent or designee may disable the technology protection measure during use by an adult to enable access for bona fide research or other lawful purpose. (20 USC 7131; 47 USC 254)

The Superintendent or designee shall annually notify employees in writing that they have no reasonable expectation of privacy in the use of any equipment or other technological resources provided by or maintained by the district, including, but not limited to, computer files, email, text messages, instant messaging, and other electronic communications, even when provided their own password. To ensure proper use, the Superintendent or designee may monitor employee usage of district technology at any time without advance notice or consent and for any reason allowed by law.

In addition, employees shall be notified that records maintained on any personal device or messages sent or received on a personal device that is being used to conduct district business may be subject to disclosure, pursuant to a subpoena or other lawful request.

Employees shall report any security problem or misuse of district technology to the Superintendent or designee.

Inappropriate use of district technology may result in a cancellation of the employee's user privileges, disciplinary action, and/or legal action in accordance with law, Board policy, and administrative regulation.

(cf. 4118 - Dismissal/Suspension/Disciplinary Action)
(cf. 4218 - Dismissal/Suspension/Disciplinary Action)

Legal Reference: (see next page)

EMPLOYEE USE OF TECHNOLOGY (continued)

Legal Reference:

GOVERNMENT CODE
3543.1 Rights of employee organizations
6250-6270 California Public Records Act
PENAL CODE
502 Computer crimes, remedies
632 Eavesdropping on or recording confidential communications
VEHICLE CODE
23123 Wireless telephones in vehicles
23123.5 Mobile communication devices; text messaging while driving
23125 Wireless telephones in school buses
UNITED STATES CODE, TITLE 20
7101-7122 Student Support and Academic Enrichment Grants
7131 Internet safety
UNITED STATES CODE, TITLE 47
254 Universal service discounts (E-rate)
CODE OF FEDERAL REGULATIONS, TITLE 47
54.520 Internet safety policy and technology protection measures, E-rate discounts
COURT DECISIONS
City of San Jose v. Superior Court (2017) 2 Cal.5th 608
City of Ontario v. Quon et al. (2010) 000 U.S. 08-1332

Management Resources:

WEB SITES
CSBA: http://www.csba.org
American Library Association: http://www.ala.org
California Department of Education: http://www.cde.ca.gov
Federal Communications Commission: http://www.fcc.gov
U.S. Department of Education: http://www.ed.gov

EMPLOYEE USE OF TECHNOLOGY

Internet Safety Policy

The Wheatland School District strongly believes in the educational value of electronic services and recognizes their potential to support the curriculum and student learning by facilitating resource sharing, ciii) innovation, and communication.

The district expects all employees to use technology responsibly in order to avoid potential problems and liability. The district may place reasonable restrictions on the sites, material, and/or information that employees may access through the system.

The district makes no guarantee that the functions or services provided by or through the district will be without defect. In addition, the district is not responsible for financial obligations arising from unauthorized use of the system.

Definitions

District technology includes, but is not limited to, computers, the district's computer network including servers and wireless computer networking technology (wi-fi), the Internet, email, USB drives, wireless access points (routers), tablet computers, smartphones and smart devices, telephones, cellular telephones, personal digital assistants, pagers, MP3 players, wearable technology, any wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off site or through district-owned or personally owned equipment or devices.

1. Access to Inappropriate Material

a. The District employs an Internet filtering system designed to prevent students and adults from accessing obscene, pornographic, and other materials harmful to minors, as those terms are defined in the Children's Internet Protection Act ("CIPA").

b. These safeguards may be disabled for adults only for bona fide research or other lawful purpose.

2. District Monitoring and Education

a. The District will monitor the online activities of minors to prevent minors' access to obscene, pornographic, and other materials harmful to minors, as those terms are defined in CIPA.

b. To the extent possible, it is the duty of all District teachers and staff to educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

EMPLOYEE USE OF TECHNOLOGY (continued)

Acceptable Use Agreement

All users of the District's networking services must sign this Agreement acknowledging and agreeing to the following standards and requirements.

Parents must closely review this Agreement. Both parents and their children are ultimately responsible for complying with its terms. Please refer to the Internet section of the District's Student Discipline Handbook for additional information. (References are not an exhaustive list).

1. Personal Safety

a. Students may not disseminate or distribute personal contact information about themselves or other people without the permission of their parents, teacher, and any affected third party. Personal contact information includes but is not limited to photos, addresses or telephone numbers. (Safety violation)

b. Students may not meet in person with someone they have met online without their parent's approval. (Safety violation)

c. Students will promptly disclose to their teacher or other school employee any message they receive that is inappropriate. Inappropriate messages are those that are obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful. (Safety violation)

2. Illegal Activities

a. Students and staff may not attempt to gain unauthorized access ("hacking") to the District's network resources or to any other computer system to go beyond their authorized access.

This includes attempting to log-in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing." (Theft)

b. Students and staff may not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal. (Vandalism)

c. Students and staff may not use the District network to engage in any other illegal act, such as arranging for a drug sale, engaging in criminal gang activity, or threatening the safety of a person. (Drug and safety violation)

EMPLOYEE USE OF TECHNOLOGY (continued)

d. Students and staff may not read, move, rename, edit, delete, or in any way alter the files that have been created or organized by others without express permission. (Vandalism)

e. Students and staff may not install or remove software on any District computers or on the District network without the direct approval and supervision of District staff. (Vandalism)

f. Students and staff may not alter hardware or software setups or settings on any District computer resources. (Vandalism)

g. Employees and staff may not engage in or promote unethical practices or violate any law or Board policy, administrative regulation, or district practice

3. Security

a. Students and staff are responsible for their individual accounts and should take all reasonable precautions to prevent others from gaining access. (Safety violation)

b. Students and staff must immediately notify a teacher, campus administrator, or other appropriate authority if they identify a possible security problem with the network or peripheral computers. Students and staff may not go looking for these security problems, because this may be construed as an attempt to gain improper or illegal access in violation of this Agreement. (Safety violation/theft)

c. Students and staff must take all precautions to avoid the spread of computer viruses. (Vandalism)

d. Students and staff may not attach any computer equipment, mobile devices (including smartphones and/or tablets) or other peripherals to the District network or its infrastructure without District approval. "Computer equipment or peripherals" does not include data storage devices such as USB drives, flash drives, floppy disks, CDs, or DVDs. (Safety)

4. Inappropriate Language

a. Students and staff may not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language. (Derogatory statements/sexual harassment/)

EMPLOYEE USE OF TECHNOLOGY (continued)

b. Restrictions against inappropriate language apply to public messages, private messages, emails, and material created for assignments or to be disseminated or distributed on web pages. (Derogatory statements/disruption of education/defamatory/sexually explicit/harassing/intimidating/threatening/disruptive)

c. Students and staff may not engage in personal attacks, including prejudicial or discriminatory attacks through their use of District network services or technology. (Derogatory statements/disruption of education/defamatory/sexually explicit/harassing/intimidating/threatening/disruptive)

d. Students and staff may not harass other people through their use of the District's network systems or technology. Harassment is persistently acting in a manner that distresses or annoys another person. If students or staff are told by a person to stop sending them such messages, I will stop. (Disrespecting others' rights/disruption of education)

e. Students and staff may not knowingly or recklessly disseminate or distribute false or defamatory information about a person or organization through their use of the District's network or technology resources. (Derogatory statements/disruption of education)

5. Respect for Privacy

a. Students and staff may not redistribute messages that were sent to them privately without permission of the person who sent them the message. (Disrespecting others' rights)

b. Students and staff may not disseminate or distribute private information about another person through the use of the District's network or technology resources. (Disrespecting others' rights)

c. Since the use of district technology is intended for use in conducting district business, no employee should have any expectation of privacy in any use of district technology.

The district reserves the right to monitor and record all use of district technology, including, but not limited to, access to the Internet or social media, communications sent or received from district technology, or other uses within the jurisdiction of the district. Such monitoring/recording may occur at any time without prior notice for any legal purposes including, but

EMPLOYEE USE OF TECHNOLOGY (continued)

not limited to, record retention and distribution and/or investigation of improper, illegal, or prohibited activity. Employees should be aware that, in most instances, their use of district technology (such as web searches or emails) cannot be erased or deleted.

All passwords created for or used on any district technology are the sole property of the district. The creation or use of a password by an employee on district technology does not create a reasonable expectation of privacy.

6. Respecting Resource Limits

a. Students must use the technology and network only for educational purposes. (Disruption of education)

b. Staff must use the District's network and technology primarily for work-related purposes. Staff may engage in minimal personal use of the technology and network, provided that such use does not interfere with their employment obligations to the District and/or otherwise breach this Agreement or any applicable collective bargaining agreement.

Personal use of district technology shall not interfere with district business and operations, the work and productivity of any district employee, or the safety and security of district technology. The district is not responsible for any loss or damage incurred by an employee as a result of his/her personal use of district technology.

c. Students and staff may not disseminate or distribute chain letters or engage in "spamming." Spamming is sending an annoying or unnecessary message to a large number of people. (Disruption of education)

d. Students and staff may not download or use games, pictures, video, music, instant messaging, e-mail, or file sharing applications, programs, executables, or similar materials unless authorization is first obtained from the District, it is legal for to possess such files, and it is in support of a classroom assignment or employment duties to the District. (Disruption of education)

e. Students and staff understand that District personnel may monitor and access any equipment connected to the District's network resources and my computer activity. The District personnel may delete any files, program and/or media that are not for a classroom assignment. (Security)

EMPLOYEE USE OF TECHNOLOGY (continued)

7. Plagiarism and Copyright Infringement

a. Students may not plagiarize works found on the Internet or on the computers at my school. Plagiarism is taking the ideas or writings of others and presenting them as if they were my own. (Theft)

b. Students and staff may not engage in copyright infringement. Copyright infringement occurs when students or staff inappropriately reproduce a work that is protected by a copyright. If a work contains language that specifies or limits the way(s) in which a work may be used, students and staff may use the work only as specified by the copyright holder. If students or staff are unsure whether a particular work may be used, permission must first be requested from the copyright holder. (Theft)

c. Infringe on copyright license, trademark, patent, or other intellectual property rights

8. Inappropriate Access to Material

a. Students and staff may not use District network resources to access or store material that is profane, obscene (pornography), that advocates illegal acts, or that advocates violence and/or discrimination toward other people. (Disruption of education/safety violation)

b. Should students and/or staff mistakenly access inappropriate material, they must immediately tell their teacher, appropriate administrator, or supervisor, and will not attempt to access the inappropriate information again. (Failure to comply with directives)

c. Parents will instruct their student(s) as to additional material that they believe is inappropriate for their student to access. Students agree not to access any material that their parents have informed them is inappropriate. (Respect for others violation)

d. Students and staff understand that Internet access is provided for support of classroom assignments and/or employment duties to the District, and agree that they will not attempt to surf anonymously or modify the computer in any way that would allow access to inappropriate websites, programs or files that are not authorized for use. (Disruption of education).

EMPLOYEE USE OF TECHNOLOGY (continued)

9. Network Use and Access While Off-Campus and/or During Non-Working Hours

a. The provisions of this Agreement govern access to, and the use of, District networking and technology resources for all students and staff while off campus or during non-working hours. Students and staff agree to abide by the terms of this Agreement whenever they use or access District networking and technology resources, regardless of time or location.

10. Use of District-issued hardware

a. From time to time the District may issue hardware to District students and staff for educational or employment-related purposes. Students and staff agree that their use of District-issued hardware will be limited to that necessary to the educational or employment-related purpose(s) for which it was issued.

b. Students and staff agree not to download, install, or access any program, website, file, document, and/or other electronic media except that which is used in furtherance of that educational or employment-related purpose. Students and staff also agree not to delete, modify, or otherwise tamper with any programs, files, documents, and/or other electronic media existing on District-issued hardware at the time it is provided to the student or staff member.

c. Students and staff agree not to disseminate, disclose, or otherwise make use of any confidential, private, or sensitive information they gain access to through or as a result of their use of any District-issued hardware.

d. Students and staff agree to return any District-issued hardware on demand from the District, or immediate at the conclusion of the purpose(s) for which it was issued. Students and staff agree to return any District-issued hardware in the same physical condition, and with the same, programs, files, documents, and/or electronic media with which the hardware was provided.

e. Engage in unlawful use of district technology for political lobbying

11. Discipline

Failure by students or staff to abide by the terms of this Agreement is grounds for disciplinary action, up to and including expulsion (students) and termination of employment (staff).

EMPLOYEE USE OF TECHNOLOGY (continued)

Consequences for Violation

Violations of the law, Board policy, or this Acceptable Use Agreement may result in revocation of an employee's access to district technology and/or discipline, up to and including termination. In addition, violations of the law, Board policy, or this agreement may be reported to law enforcement agencies as appropriate.

12. Personally Owned Devices

If an employee uses a personally owned device to access district technology or conduct district business, he/she shall abide by all applicable Board policies, administrative regulations, and this Acceptable Use Agreement. Any such use of a personally owned device may subject the contents of the device and any communications sent or received on the device to disclosure pursuant to a lawful subpoena or public records request.

Employee Acknowledgment

I have received, read, understand, and agree to abide by this Acceptable Use Agreement, BP 4040 - Employee Use of Technology, and other applicable laws and district policies and regulations governing the use of district technology. I understand that there is no expectation of privacy when using district technology or when my personal electronic devices use district technology. I further understand that any violation may result in revocation of user privileges, disciplinary action, and/or appropriate legal action.

I hereby release the district and its personnel from any and all claims and damages arising from my use of district technology or from the failure of any technology protection measures employed by the district.

My name and signature below represents that I have received, read, and fully understand the Internet Safety Policy and my responsibilities, as defined in the Acceptable Use Agreement above, when using District technological resources

Parents and guardians of children under the age of 18, must also sign below, indicating that they have received, read, and fully understand the Internet Safety Policy and the responsibilities of their student when using District technological resources. The signature of a parent or guardian below acknowledges and accepts full responsibility for their student's compliance with the terms herein, and hereby give their permission for their student to use the District network and Internet services.

_____ _____

Parent or Guardian Printed Name (if student under 18) Date

EMPLOYEE USE OF TECHNOLOGY (continued)

Parent or Guardian Signature (if student under 18)	Date
Student Printed Name	Date
Student Signature	Date
Student Permanent ID#	
Staff Member Printed Name	Date
Staff Member Signature	Date