

## EMPLOYEE USE OF TECHNOLOGY

The Superintendent or designee shall oversee the maintenance of the district technology as defined in Board Policy and may establish guidelines and limits on its use. All employees shall receive a copy of this administrative regulation, the accompanying Board policy, and the district's Acceptable Use Agreement describing expectations for appropriate use of district technology and shall also be provided with information about the role of district employees in supervising student use of technological resources.

Employees shall prescreen technological resources and online sites that will be used for instructional purposes to ensure that they are appropriate for the intended purpose and the age of the students.

### I. Online/Internet Services: User Obligations and Responsibilities

Employees are authorized to use district technology to access the Internet or other online services in accordance with Board policy, the user obligations and responsibilities specified below, and the district's Acceptable Use Agreement.

1. The employee in whose name district technology, or to whom an online services account is issued, is responsible for its proper use at all times. Employees shall not share their assigned online services account information, passwords, or other information used for identification and authorization purposes, and shall use the district system only under the account to which they have been assigned. This includes, but is not limited to, other teachers, students, para-professionals, parent volunteers, and other district employees except Technology Department technical support personnel required to have access to said information to perform their duties.
2. Employees shall not gain unauthorized access to the files or equipment of others, access electronic resources by using another person's name or electronic identification, or send anonymous electronic communications. Furthermore, employees shall not attempt to access any data, documents, emails, or programs in the district's system for which they do not have authorization.
3. Employees shall use district technology safely, responsibly, and primarily for work-related purposes.
4. Employees shall not access, post, submit, publish, or display harmful or inappropriate matter that is threatening, intimidating, obscene, disruptive, or sexually explicit, harassing, or that could be construed as harassment or disparagement of others based on their race or ethnicity, nationality, national origin, sex, gender, gender identity, gender expression, sexual orientation, age, disability, religion, or political beliefs.

Employees shall not disclose, or in any way cause to be disclosed, or disseminate confidential or personal identification information about themselves or other employees or

**EMPLOYEE USE OF TECHNOLOGY**

students when using email, social media, chat rooms, or any other form of electronic communication without prior authorization from a supervisor.

5. Employee and student records may only be shared with authorized personnel, or with proper consent, or where permitted by state and federal law. Student records may only be shared where permitted by the Family Educational Records and Privacy Act (FERPA) and district policy. Non-employee district consultants, vendors, or individuals working on behalf of the district must incorporate a written confidentiality provision in their agreement before receiving any employee or student records.
6. Employees shall not use district technology to encourage the use of drugs, alcohol, or tobacco, nor shall they promote unethical practices or any activity prohibited by law, Board policy, or administrative regulations.
7. Employees shall not use district technology to engage in personal commercial or other for-profit activities without permission from the Superintendent or designee.
8. Employees shall not engage in unlawful use of district technology for political lobbying.
9. Employees shall not use district technology to threaten, intimidate, harass, bully/cyberbully or ridicule other employees or students. Bullying/ cyberbullying, includes the transmission of communications, posting of harassing messages, direct threats, or other harmful texts, sounds, or images on the Internet, social media sites, or other digital technologies using a cellular telephone, computer, or any wireless communication device.
10. Employees shall not infringe on copyright, license, trademark, patent, or other intellectual property rights. Copyrighted material shall not be placed on the district's computer systems without the author's permission. Employees may download copyrighted material only in accordance with applicable copyright laws.
11. Employees shall not intentionally upload, download, or create computer viruses and/or maliciously attempt to harm or destroy district equipment or materials or manipulate the data of any other user, including so-called "hacking."
12. As required under Board Policy 4040, employees shall use district technology primarily for purposes related to their employment. Personal and/or non-district email addresses or services shall not be used for electronic communication as a district employee. Employees shall not attempt to interfere with other users' ability to send or receive email, nor shall they attempt to read, delete, copy, modify or forge other users' email.
13. Employees shall not develop any classroom or work-related web sites, blogs, forums, social media accounts, or similar online communications representing the district or district school or using district equipment or resources without permission of the Superintendent or designee. Such sites shall be subject to rules and guidelines established for district online

## EMPLOYEE USE OF TECHNOLOGY

publishing activities including, but not limited to, copyright laws, privacy rights, and prohibitions against obscene, libelous, and slanderous content. Because of the unfiltered nature of blogs, any such site shall include a disclaimer that the district is not responsible for the content of the messages. The district retains the right to delete material on any such online communications.

14. Employees shall report any security problem or misuse of district technology to a principal, the Director of Technology, or the Superintendent or Superintendent's designee.

### II. District Equipment and Devices: User Obligations and Responsibilities

1. When an employee is issued any district owned equipment or device from the district or a district school, it must be used in accordance with the Acceptable Use Agreement, and Employee Use of Technology board policy and administrative regulation.
2. Employees shall be responsible for the appropriate use of technological resources and shall use district technology for purposes primarily related to his/her employment. Such use is a privilege which may be revoked at any time.

### III. Social Media and Electronic Messaging: User Obligations and Responsibilities

1. Employees are responsible for their own behavior when communicating through the use of social media. Employees will be held accountable for the content of the communications that they post or state on social media platforms.
2. The district is not responsible for the content of external online platforms. Any views expressed on an external site or social media platform are those of the employee and do not reflect the views of the district.
3. Employees are expected to communicate in a respectful, courteous, and professional manner.
4. When accessing social media platforms or websites through the use of district technology, employees shall not post any material or content that is inconsistent with District Board policy and administrative regulation 4040.
5. When employees place their communication in "privacy" marked social media using district technology, they cannot expect that their information will not be disclosed by a person within their "private marked" group. Such information may be disclosed by others within the "private group", or the information may be disclosed by other means. The district may be provided this information and may be required to investigate it further. Information the district obtains may be disclosed without limitation for purposes of investigation, litigation, internal dispute resolution, and discipline regardless of whether the particular user employee is involved.

## EMPLOYEE USE OF TECHNOLOGY

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 employee use of the 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 not limited to, record retention and distribution and/or investigation of improper, illegal, or prohibited activity.

Whenever an employee is found to have violated Board policy, administrative regulation, or the district's Acceptable Use Agreement, the Superintendent or designee may revoke or limit an employee's user privileges. Inappropriate use may also result in disciplinary action, up to, and including dismissal, and/or appropriate legal action.

### Technology Acceptable Use Policy

The following pages include the Acceptable Use Agreement

Revised: 05/30/2012

Board Adopted: 06/29/2012

Revised: 05/15/2013

Board Adopted: 05/28/2013

Revised: 06/13/2017

Board Adopted: 06/27/2017

**TRACY UNIFIED SCHOOL DISTRICT  
ACCEPTABLE USE AGREEMENT  
EMPLOYEE USE OF DISTRICT TECHNOLOGY  
(BP/AR 4040)**

The Tracy Unified School District (“district”), authorizes district employees to use technology owned or otherwise provided by the district as necessary to fulfill the requirements of their position. The use of district technology is a privilege permitted at the district’s discretion and is subject to the conditions and restrictions set forth in applicable Board policies, administrative regulations, and this Acceptable Use Agreement. The district reserves the right to suspend access at any time, without notice, for any reason.

The district expects all employees to use district technology responsibly 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 district’s system.

The district makes no guarantee that the functions or services provided by or through the district will be without defect or technical issues. In addition, the district is not responsible for financial obligations arising from the unauthorized use of the system. Furthermore, the district shall not be held responsible for any damages suffered by the user, including those arising from non-deliveries, mis-deliveries, service interruptions, unauthorized use, loss of data and exposure to potentially harmful or inappropriate material sustained or incurred in connection with the use, operation, or inability to use the district’s system.

Each employee who is authorized to use district technology shall sign this Acceptable Use Agreement as an indication that he/she has read and understands the agreement. Please read this document carefully. It is a legally binding agreement when signed.

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.

Employee Obligations and Responsibilities

Employees are expected to use district technology safely, responsibly, and primarily for work-related purposes in support of the enhancement of employee performance by improving access to and exchange of information; offering effective tools to assist in providing a quality instructional program; facilitating communications with parents/guardians, students, and the community; and supporting and facilitating district and school operations. Any incidental 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

**TRACY UNIFIED SCHOOL DISTRICT  
ACCEPTABLE USE AGREEMENT  
EMPLOYEE USE OF DISTRICT TECHNOLOGY  
(BP/AR 4040)**

responsible for any loss or damage incurred by an employee as a result of his/her personal use of district technology.

The district's network/computer system ("district system") is shared and available to all registered employee users. The employee in whose name district technology is issued is responsible for its proper use at all times. Employees shall not share their assigned online services account information, passwords, or other information used for identification and authorization purposes, and shall use the system only under the account to which they have been assigned. Employees shall not gain unauthorized access to the files or equipment of others, access electronic resources by using another person's name or electronic identification, or send anonymous electronic communications. Furthermore, employees shall not attempt to access any data, documents, emails, or programs in the district's system for which they do not have authorization.

Employees are prohibited from using district technology for improper purposes, including, but not limited to, use of technology to:

- Access, post, submit, publish, or display harmful or inappropriate matter that is threatening, intimidating, obscene, disruptive, or sexually explicit, harassing, or that could be construed as harassment or disparagement of others based on their race/ or ethnicity, nationality, national origin, sex, gender, gender identity, gender expression, sexual orientation, age, disability, religion, or political beliefs.
- Intentionally disrupt or harm district technology or other district operations, such as altering software; uploading, downloading, or creating computer viruses on district computers; and/or maliciously attempt to harm or destroy district equipment or materials or manipulate the data of any other user, including so-called "hacking."
- Install non-approved software/programs, or download and install software/programs on district computers or district system.
- Communicate unlawful information or to transmit computer viruses.
- Disclose or in any way cause to be disclosed confidential or sensitive district, employee, or student information without prior authorization from the Superintendent or designee.
- Encourage the use of drugs, alcohol, or tobacco, nor shall they promote unethical practices or any activity prohibited by law, Board policy, or administrative regulations.
- Engage in personal commercial or other for-profit activities without permission from the Superintendent or designee.
- Engage in unlawful use of district technology for political lobbying.
- Threaten, intimidate, harass, bully or ridicule other employees or students.

**TRACY UNIFIED SCHOOL DISTRICT  
ACCEPTABLE USE AGREEMENT  
EMPLOYEE USE OF DISTRICT TECHNOLOGY  
(BP/AR 4040)**

- Infringe on copyright, license, trademark, patent, or other intellectual property rights.
- To send “junk”, “mass”, or “spam” email.
- Engage in or promote unethical practices or violate any law or Board policy, administration regulation, or district practice.
- Other conduct deemed objectionable by the district.

When accessing social media platforms or websites through the use of district technology, employees shall not post any material or content that is inconsistent with district board policy and administrative regulation 4040.

When employees place their communication in “privacy” marked social media using district technology, they cannot expect that their information will not be disclosed by a person within their “private marked” group. Such information may be disclosed by others within the “private group”, or the information may be disclosed by other means. The district may be provided this information and may be required to investigate it further. Information the district obtains may be disclosed without limitation for purposes of investigation, litigation, internal dispute resolution, and discipline regardless of whether the particular employee is involved.

Privacy

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 platforms, communications sent or received from district technology, online digital storage, or other uses within the jurisdiction of the district. Such monitoring/recording may occur at any time without prior notice for any legal purpose including, but 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.

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.

**TRACY UNIFIED SCHOOL DISTRICT  
ACCEPTABLE USE AGREEMENT  
EMPLOYEE USE OF DISTRICT TECHNOLOGY  
(BP/AR 4040)**

Records

Any electronically stored information generated or received by an employee which constitutes a district or student record shall be classified, retained, and destroyed in accordance with applicable District Board policies and regulations addressing the retention of district or student records.

Reporting

If an employee becomes aware of any security problem (such as any compromise of the confidentiality of any login or account information) or misuse of district technology, he/she shall immediately report such information to the Superintendent or designee.

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.



**TRACY UNIFIED SCHOOL DISTRICT  
ACCEPTABLE USE AGREEMENT  
EMPLOYEE USE OF DISTRICT TECHNOLOGY  
(BP/AR 4040)**



TRACY UNIFIED SCHOOL DISTRICT ACCEPTABLE USE POLICY (AUP)  
NETWORK AND COMPUTER RELATED RESOURCES  
(Based on BP/AR 4040 and BP/AR 6163.4)

**TUSD EMPLOYEE ACKNOWLEDGEMENT**

I have received, read, understand, and agree to abide by this Acceptable Use Agreement, Board Policy and Administrative Regulation 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 access to district technology, disciplinary action, up to and including termination, 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.

Employee (PRINT NAME)	School Site/ Department	Staff ID #	Job/Title	Signature	Date
-----------------------	----------------------------	------------	-----------	-----------	------