Employee Use of Technology

Staff Technology Acceptable Use Agreement 2025-26

revised 7/1/2025

This Staff Technology Acceptable Use Agreement ("AUA") protects Oak Park Unified School District ("OPUSD") and its employees by providing guidelines and regulations for the appropriate use of District technology, information, and communication. 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, the Staff Social Media Guidelines and Best Practices as outlined in the District's communication plan, 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 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. However, the district shall not prevent or restrict access to an employee's mobile or other communications device(s) if there is a need to seek emergency assistance, assess the safety of a situation, or communicate with a person to confirm the person's safety.

District technology includes all District-owned or managed computing devices (such as Chromebooks, laptops, and tablets), communication tools (such as email, phones, and ParentSquare), network infrastructure (including Wi-Fi, servers, and security systems), and online information systems and services (such as Google Workspace, Q-SIS, and educational software platforms).

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, or misuse, of the system.

Each employee who is authorized to use district technology shall sign this Agreement, which indicates that the employee has read and understands this Agreement and Board Policy 4040 - Employee Use of Technology.

This AUA serves to:

- Ensure District resources are used to promote the District's educational goals;
- Ensure District communication and information resources are accessible to all;
- Ensure employees adhere to the highest standards of professionalism, integrity, and civility.
- Protect the welfare and rights of students, families, and staff;
- Protect the privacy and the security of student and staff information;
- Protect the District's network infrastructure, information systems, and equipment;
- Protect intellectual property rights;

OAK PARK UNIFIED SCHOOL DISTRICT
BOARD POLICY

EMPLOYEE OBLIGATIONS AND RESPONSIBILITIES

Employees are expected to use district technology safely, responsibly, and primarily for work-related purposes and in accordance with the accompanying board policy and applicable copyright laws. 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 responsible for any loss or damage incurred by an employee as a result of the employee's personal use of district technology.

Particular care should be exercised when transmitting confidential information about students, employees, and/or any other business of the District. Federal and state laws which apply include:

1. The federal **Americans with Disabilities Act** (1990) and the **Rehabilitation Act of 1973** (**sections** 504 and **508**), which establish regulations to ensure accessibility to information technology and appropriate accommodations for those with disabilities.

2. The federal **Children's Internet Protection Act (CIPA)**, which protects the safety and privacy of minors. The District uses requisite filtering technology to monitor and screen access to the Internet in an attempt to prevent online access to materials that are obscene, contain child pornography or are harmful to minors.

3. The federal **Children's Online Privacy Protection Act (COPPA)**, protects against the online collection of personal information from children under 13.

4. The federal **Digital Millennium Copyright Act (DMCA)** addresses copyright infringement in digital media.

5. The federal **Family Educational Rights and Privacy Act (FERPA)** protects the rights of students regarding access to, amendment, and disclosure of information contained in education records.

6. The federal **Health Insurance Portability and Accounting Act (HIPAA)** protects the rights of students and employees regarding confidential health information.

7. The federal **Protection of Pupil Rights Amendment (PPRA)** concerns the administration of surveys to students that cover eight protected areas and ensures student privacy, parental access to information, and prior parental consent.

8. The California **Child Abuse and Neglect Reporting Act,** AB 1775 (2014), which expands the definition of sexual abuse/exploitation to include a person who knowingly downloads, streams, or accesses digital media in which a child is engaged in an act of obscene sexual conduct.

9. The **California Electronic Communications Privacy Act (CalECPA)**, also known as Senate Bill 178 (2015), which strengthens electronic privacy against access to data on electronic devices.

10. The California **Student Online Personal Information Protection Act (SOPIPA),** Assembly Bill 1584 (2014), and Senate Bill 1177 (2014), which protect student information and records with regard to operators of websites, online services, and applications that are marketed and used for K-12 school purposes.

11. The **California Consumer Privacy Act of 2018 (CCPA)**, AB 375 extends protections for student Personally Identifiable Information (PII) up through age 16 (beyond the COPPA protections, which cover children up through age 13).

12. The **California Public Records Act (PRA)** was enacted to safeguard the accountability of government to the public, promote maximum disclosure of the conduct of governmental operations, and explicitly acknowledge the principle that secrecy is antithetical to a democratic system.

13. **California Penal Code section 502**, which prohibits unauthorized computer access.

14. **California Education Code section 49073, *et seq***., which governs student data privacy laws and gathering information from student's social media accounts.

PROHIBITED USES

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

a. Access, post, display, create, or otherwise use material that is discriminatory, defamatory, obscene, sexually explicit, harassing, intimidating, threatening, or disruptive
b. Infringe on copyright, license, trademark, patent, or other intellectual property rights
c. Engage in personal commercial or other for-profit activities without permission of the Superintendent or designee
d. Engage in unlawful use of district technology for political lobbying.
e. Intentionally disrupt or harm district technology or other district operations (such as destroying district equipment, placing a virus on district computers, adding or removing a computer program without permission, changing settings on shared computers).
f. Install unauthorized software
g. Causing congestion or disruption to the District network through inappropriate downloads of large files, streaming audio/video not directly related to providing instruction or district business, or other such non-work-related activities;
h. Accessing, changing, or using another person's account, files, output, records, or username for which one does not have explicit authorization to do so.
i. Engage in or promote unethical practices or violate any law or board policy, administrative regulation, or district practice

j. Disclose or in any way cause to be disclosed confidential or sensitive district, employee, or student information without prior authorization from a supervisor, including sharing confidential information or personally identifiable information with an open artificial intelligence system

EQUIPMENT CARE AND LOSS

Employees are expected to treat District property including technology such as laptops or mobile computing devices with care. Reoccurring or willful damage to District-owned device(s) may result in the employee being held responsible for the cost of repair or replacement. Staff are to avoid using their district devices while eating food or with open beverage containers nearby.

If a District device is lost or stolen from an employee, the staff member shall obtain a police report and provide it to the district so the district can seek reimbursement from insurance.

PRIVACY

Employees have no specific ownership or possessory right in District-owned devices used or in the information stored or created therein.

a. The employee in whose name district technology is issued is responsible for its proper use at all times.
b. 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.
c. 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.
d. Employees shall not attempt to access any data, documents, emails, or programs in the district's system for which they do not have authorization.
e. The District may confiscate any District-owned device at any time and without cause. If the District confiscates a District-owned device, an employee is no longer the authorized possessor of the device.

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.

a. 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, Internet searches, browsing history, use of artificial intelligence, 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. Employees should be aware that, in most

instances, their use of district technology (such as web searches or emails) cannot be erased or deleted.

b. The data that employees create, store, and/or transmit using District technology is not private and is considered the property of the District. 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.
c. If an employee uses a personally owned device to access district technology or conduct district business, the employee shall abide by all applicable board policies, administrative regulations, and this 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.

Employees are to conduct official business and correspondence *only* through District-provided or District-managed accounts and not through their personal accounts. Official accounts include district email, Parent Square, Google Classroom, District webpages including Googlesites.

a. District/school business communications are subject to discovery pursuant to a subpoena, public records act request, or other lawful request.
b. District and/or school records maintained on any personally owned device or official communications sent or received on a personally owned device may be subject to discovery and disclosure, pursuant to a subpoena, public records act request, or other lawful request.
c. District-provided email accounts are strictly for educational business use and shall not be used for personal purposes.
d. Staff will adhere to the OPUSD Staff Social Media Guidelines when using social media with students.
e. 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 Board Policy/Administrative Regulation 3580 - District Records, Board Policy/Administrative Regulation 5125 - Student Records, or other applicable policies and regulations addressing the retention of district or student records.
f. If an employee becomes aware of any security problem (including, but not limited to, a cyberattack, phishing, or any compromise of the confidentiality of any login or account information), or misuse of district technology, the employee shall immediately report such information to the Superintendent or designee and Technology@opusd.org.

Accounts used to access District technology services and data systems must be kept secure (e.g., device logins, email, file storage, student information systems, electronic grade books, attendance and grade reporting functions, staff data systems, etc.)

a. Employees shall keep their passwords secure and shall not write down their passwords anywhere near the computer or where a student or other unauthorized user might discover them.

b. Employees shall not give their login credentials (such as passwords) to students, teacher assistants, aides, or other users nor allow them to access or input grades or attendance information into the district's student information systems.
c. Staff are required to follow all district established cybersecurity protocols (including multi-factor authentication (MFA) to access district technology tools and services including computers, email systems, student information systems, and/or other electronic or online resources. Secure authentication methods may include the use of a smartphone authenticator app (on employee's own personal smartphone), physical security key (provided by the district), and/or other district-approved method.)

Staff shall promote information security and uphold staff and student data privacy when working with third-party vendors and online resources.

k. In order to ensure student data remains private and protected from unauthorized use or sale, staff shall not use third-party websites or digital resources that use student email accounts for login that don't have a current and valid California-National Student Data Privacy Agreement CSDPA/NDPA agreement in place with Oak Park USD or other data privacy agreement that has been approved by the district technology department.
l. Staff may use third-party websites and digital resources with students when those tools/resources do not require students to authenticate with their district email account nor provide any Personally Identifiable Information (PII) including email addresses. (Students may use a teacher-generated join code without providing any personally identifiable information.)

STAFF COMMUNICATIONS

Accountability, Discretion, and Professionalism:

a. Employees are expected to exercise discretion and maintain professionalism in all online communications—both personal and job-related. They are accountable for their posts, messages, and shared content across all platforms, including social media, email, messaging apps, and media-sharing sites.
b. Online interactions with students, parents, colleagues, and alumni should reflect the same respect and conduct as in-person communication. At no time should digital platforms be used to harass, intimidate, disparage, or violate the privacy of others.
c. Use of websites, blogs, learning platforms, and social media must align with the professional standards and conduct outlined in this Acceptable Use Agreement (AUA). If an employee's online activity violates this agreement, the District may require the activity to cease and may pursue disciplinary action, up to and including termination.

Employee Maintained Webpages:

Employees shall ensure that the publicly accessible webpages/websites they maintain shall be accessible to individuals with disabilities in compliance with Americans with Disabilities Act and Section 508 of the Rehabilitation Act of 1973. This may be done by adherence to Web Content

Accessibility Guidelines (WCAG 2.0) (or updated equivalents of these guidelines) which helps to ensure that webpages can be correctly interpreted by automatic screen reading devices. Required accessibility criteria includes, but is not limited to, the following:

- **Images**: All images must contain an "alt tag" or long description
- **Text Equivalents**: Provide text descriptions to logos, pictures, icons, and audio
- **Videos closed captioned**: All videos on a school/district webpage must have closed captioning embedded within the video
- **PDF Documents**:
    - PDF's must have Accessibility Tags embedded (such as those edited with Acrobat Pro with Accessibility Tools enabled)
    - Forms must be fillable fields in PDFs
    - PDF documents should not contain scanned images
    - Scanned documents must be converted to text using OCR (Optical Character Recognition)
- **HTML Headings:** must use Headings ,<h1>, <h2>, <h3> in formatting webpage (not pasted from MS Word)
- **Tables**: Column and Row headings must be meaningful and descriptive
- **Animations** (Flash): Avoid flashing or blinking, no more than 1 flash/sec, presentation transitions no less than 5 seconds
- **Links**: must not be broken, and those pointing outside of district/school should have a written warning that clicking on that link will cause the user to leave the district/school website

Employees needing assistance implementing the above-stated criteria on employee-maintained webpages should contact the District's Director of Technology dthompson@opusd.org for support.

Use of Student Images and Work:

In order to safeguard student privacy, staff shall not post photos and/or student work along with the names of students on school or district websites unless they have received explicit written permission from both student and parents to do so. Staff may post student photos and student work without names, or post student names without photos (unless a parent has submitted a Media Release OPT OUT Form to the school office indicating that they do not wish their child's photo to be published at all). Prior to publishing student images, staff shall consult the District's directory information list to determine whether students shown in the image have not submitted an OPT OUT Form.

Use of Electronic Communication with Students:

a. Employees should communicate with students primarily through district-provided e-mail, Google Classroom, or the Parent Square communications platform. Employees shall refrain from messaging (e.g., iMessage, Snapchat, etc.) or any other texting, photo or video communication with students on a personal basis not directly tied to an educational activity. This is especially true with regard to services whose messages disappear after receipt.

b. Employees may use social networking tools for appropriate educational purposes but should only use accounts created specifically for class communication and not a personal account. Such purposes may include clubs, athletic teams, and co-curricular activities. Employees must adhere to COPPA in relation to student privacy and identity.
c. According to Board Policy 4119.24, Maintaining Appropriate Adult-Student Interactions, district staff are prohibited from "[5.] Creating or participating in social networking sites for communication with students, other than those created by the district, without the prior written approval of the principal or designee" and "[6.] Inviting or accepting requests from students, or former students who are minors, to connect on personal social networking sites (e.g., "friending" or "following" on social media), unless the site is dedicated to school business." To maintain compliance with the board policy requirements, teachers and staff must annually obtain prior written permission from their site administration.
d. Please see the District's **Social Media Guidelines and Best Practices outlined in the OPUSD Communication plan** for more information.

MOBILE COMMUNICATION DEVICES

Mobile communication devices are defined as cell phones, smartphones, earphones/earbuds, tablets, gaming devices, smartwatches, smartglasses or any other device that connects to the internet or a cellular network. When on campus or when under the supervision of district employees, students may only use mobile communication devices as permitted under Board Policy 5131.8 (1).

Devices may only be used during approved times:

- **TK-5:** Devices off and stored during school hours.
- **6-8:** Devices off and away unless permitted by a teacher.
- **9-12:** Devices off during class unless instructed by the teacher. Use allowed during breaks and lunch.

FREE SPEECH

A District employee acting in an individual capacity and outside the scope of employment may, during non-working time, express views and opinions that do not necessarily state or reflect those of the District. Any such expression shall neither state nor imply that it is made on behalf of the District. A District employee shall not communicate information otherwise prohibited by District policy and procedures using District technology.

INTELLECTUAL PROPERTY

a. The District recognizes that employees may create instructional materials or online resources in the course of their employment in carrying out their duties as educators. The District shall retain a non-exclusive perpetual license to use, modify, and adapt the materials and resources created while under employment by the District for the purpose of carrying out the staff member's duties. The

materials and resources otherwise remain the property of the author, who is free to take the material (aside from private or confidential student records) with them when they leave the District.

b. Misuse of technology may result in discipline, penalties under applicable laws, and/or the loss of use of technology. Users may be held accountable for their conduct under any applicable District policy or collective bargaining agreement. Illegal reproduction or distribution of software and other intellectual property protected by U.S. copyright law is subject to civil damages and criminal punishment, including fines and imprisonment.

STREAMING VIDEO

District staff are prohibited from using retail consumer streaming video services (such as Netflix, Hulu, Disney+, Amazon Prime, Apple TV, etc.) to show movies during class or for school events. Although teachers have some latitude for using copyrighted materials for instructional purposes under Fair Use guidelines of federal Copyright law, those fair use exceptions do not apply to consumer-oriented streaming video services (such as Netflix, Hulu, Amazon Prime, Disney+, etc.), which are only licensed to individual consumers (not schools) and whose licensing agreements specifically prohibit the showing of those videos in a public setting. Teachers wishing to show movies or other copyrighted videos in the course of "face-to-face" instruction must do so from legally purchased physical media (such as DVD or Blue-Ray disc) or through a District K-12 licensed video streaming company (such as Swank Motion Pictures/Movie Licensing USA) with a license purchased for each specific performance.

ARTIFICIAL INTELLIGENCE USE IN THE CLASSROOM

In accordance with BP 4040, only AI systems and platforms that have been vetted and approved by the district (to ensure compliance with state and federal student data privacy regulations) may be used with students. At the start of each academic year or semester (for semester-only classes), teachers shall provide students and parents with written instructions about the teacher's AI use policy, stating whether or under which circumstances students will be allowed to use AI in the course or class. Students and parents shall be asked to acknowledge and agree to the teacher's AI policy in writing (or through Parent Square post/form):

> *If students will be prohibited altogether from using AI for such class, that will be made clear and explicit in the AI use policy. If the teacher allows the use of AI on a case-by-case or assignment-by-assignment basis, then the AI use policy shall state that the use of AI is prohibited unless the teacher explicitly authorizes the use of AI on a particular assignment or project. For each assignment or project where students will be allowed to use AI, the teacher shall clarify both orally and in writing the scope and purposes for which AI may be used, and the consequences for violation (e.g., 50% credit). Teachers shall use good faith efforts to have consistent, fair, and equitable policies and consequences within their course/class regarding the use of AI and shall use good faith efforts to coordinate with other teachers teaching the same class to develop consistent policies and consequences for the use of AI. Teachers shall guide*

and monitor student use of AI in their classes, ensuring that it aligns with the District's Student Acceptable Use guidelines and policies.

Employees shall not share any personally identifiable information or confidential information with any AI platform.

Personally identifiable information includes but is not limited to, a person's name, address, email address, telephone number, Social Security number, or other personally identifiable information. Confidential information includes, but is not limited to, information in a student's education record such as their grades and information pertaining to an Individualized Education Plan.

CONSEQUENCES FOR VIOLATION

Violations of the law, board policy, or this 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.

EMPLOYEE ACKNOWLEDGMENT

I have received, read, understand, and agree to abide by this Agreement, Board Policy 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, its personnel, and the Governing Board 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.

To be completed and signed online electronically via Google Forms

OAK PARK UNIFIED SCHOOL DISTRICT
BOARD POLICY

Series 4000 *Personnel* *E4040(11)*

Copy of Annual Acknowledgement and Signature Page

To be completed and signed online electronically via Google Forms

Staff Technology Acceptable Use Agreement (AUA) Overview

All Oak Park Unified School District ("District") employees are responsible for reviewing, understanding, and following the Staff Technology Acceptable Use Agreement (AUA) and related procedures issued by the Technology Department. These policies are legally binding, regardless of whether the employee has signed the AUA.

Supervisors must enforce these policies consistently. No supervisor may modify or waive the AUA without written approval from the Superintendent.

Employees are required to electronically sign the AUA Acknowledgement Form annually. Violations of the AUA will be considered actions taken outside the scope of employment and may result in disciplinary action, up to and including termination or legal prosecution. The following statements align with Board Policy 4040.

☐ **Student Data Privacy and Security**:

I will not allow students to access my Q account, record attendance, input grades, or handle any student data. I will not post student work online showing both face and full name (first name or initials only, unless public record).I will check the Media Opt-Out list before publishing student images. I will only use tools with a CSDPD/NDPA agreement or written approval from the Superintendent or designee.*

☐ **Website Compliance:**

My public class/school web page(s) will follow WCAG 2.0+ accessibility standards. I will not post copyrighted materials publicly, only within secure platforms like Google Classroom or OPUSD-only Google resources.

☐ **No Expectation of Privacy**: I understand I have no expectation of privacy when using District technology.

☐ **No Possessory Interest**:

- I understand that District devices are District property and may be reassigned or collected.
- I will treat devices with care and mya be held financially responsible for intentional or repeated damage.

☐ **District Access to Devices and Accounts**: I understand the District may access, maintain, or retrieve data from my assigned devices or accounts for:

(1) Repair or maintenance of the device;
(2) Public or student record requests.
(3) Administrative searches or compliance
(4) Fulfill the District's statutory duties and Board policies to maintain public records; and

(5) Any other District or school-related purpose.

☐ **Personal Devices:** I understand that District-related communications or files on my personal devices may be subject to legal discovery.

☐ **Personal Files:** I will regularly remove personal files from District devices and accounts to protect privacy and ensure available storage.

☐ **Exclusive Use of District Technology**: I will not allow non-employees (e.g., students, family, volunteers) to use District-owned devices or access District systems.

☐ **Video Streaming:** I will not stream videos from personal accounts or consumer services (e.g. Netflix, Disney+) unless my site has obtained a proper performance license.

☐ **Social Media Accounts:** I will annually request and receive written approval from the principal/Director of Technology before using any social media accounts for officially post associated with the school or district.

☐ **Cybersecurity protection: I** will follow district cybersecurity protocols including multi-factor authentication and other District-mandated protections.

☐ **Artificial Intelligence use in the classroom:**

- I will communicate my Classroom AI Use Policy to students and parents in writing at the beginning of the class term.
- I will obtain written acknowledgment of receipt and agreement to this policy each year.

I have read and understand the Staff Technology Acceptable Use Agreement, the latest version of which is posted on the District's website. A copy of the District's **Social Media Guidelines and Best Practices** document can also be found on the district website.

OPUSD Staff, this is a copy of the online acknowledgment form distributed to all staff via district email. Do NOT sign and submit this form on paper; instead, submit the electronic form with e-signatures entitled "**Staff Technology Acceptable Use Agreement Acknowledgement Form**."

Updated: 7/1/2025