OAK PARK UNIFIED SCHOOL DISTRICT
Staff Technology Acceptable Use Policy (a.k.a. Acceptable Use Agreement)

Substantive changes highlighted in yellow

This Staff Technology Acceptable Use Agreement ("AUP") 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. By using District technology, employees agree to abide by all of the terms described in this AUP. This AUP applies when District technology is accessed on or off site, both through District-owned or personally owned equipment or devices. This AUP complements and supports District Board Policy 4040, as well as any other relevant Board Policy or applicable law.

District technology includes, but is not limited to, **District owned and/or District managed computing devices and peripherals** (e.g., computers, laptops, tablets, projection systems, printers, storage devices, wearable technology, etc.), **District network and communication devices/services** (telephones, wired and wireless networks including WiFi access points, emergency radios, email systems, file servers, etc.), and **District managed on-line services** (such as G-Suite/Google Apps For Education, Apple Classroom/iCloud, Aequitas Q Student Information System, etc.), access to online information sources, and future technological innovations.

The purpose and considerations reflected in this AUP include, but are not limited to:

- Protecting the welfare of children;
- Protecting individuals' right to privacy;
- Protecting intellectual and property rights;
- Respecting the rights of students, parents/guardians, and staff;
- Protecting District technology and electronic information;
- Assuring District resources are used to promote the District's educational goals;
- Assuring District technology and other information resources are accessible to all, well designed, and easy to navigate; and
- Assuring all employees adhere to the highest standards of professionalism, integrity and civility.

The District provides a wide range of technology to its employees for the purpose of advancing the District's educational mission, which includes classroom instruction, information processing for school business, and enhancing communication between District employees, parents, students, and community members. The District's goal for using technology is to promote educational excellence in schools by providing appropriate access to all students; fully integrating technology into the daily curriculum; modeling and promoting digital citizenship; facilitating critical thinking, creativity, communication, and collaboration; and preparing students and educators to meet the challenge of participating in a dynamic global society.

All District employees are expected to learn and use the available technological resources that will assist them in the performance of their job responsibilities. Resources are provided at the public's expense and maintained by the District and are to be used by employees with respect for the public trust through which they have been provided. The District intends to maintain a nonpublic forum, and the forums created by use of District technology are reserved for the District's intended purposes.

Successful operation of District technology requires that all users conduct themselves in a responsible, confidential, ethical, professional, and polite manner, consistent with the District's mission and goals, as well as all applicable laws and regulations. This AUP does not attempt to articulate every single required or prohibited behavior by employees. The District Technology Department can provide additional guidance, support, or clarification when needed.

GENERAL TERMS AND CONDITIONS

1. Employees have no specific ownership or possessory right in District-owned device used or in the information stored or created therein.
    a. Upon receipt of a District-owned device, employees may be the authorized possessor as defined in the California Electronic Communications Privacy Act (CalECPA). As an authorized possessor of a District-owned device, employees are responsible for using the device appropriately and for employment related purposes.
    b. Only the employee assigned by the District to the device may use the device.
    c. 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.
    d. District-owned devices are the property of the District. District-owned devices and the information contained therein may be assigned or used by other employees, on as-needed basis, in furtherance of the District's operational and administrative objectives.

2. Employees have no reasonable expectation of privacy in using District managed technology and services.
    a. An employee's use of District technology is a waiver of the protections of CalECPA. By using District technology, whether from personal or District-owned devices, employees grant specific consent, as defined by CalECPA, to the District to review and monitor all electronic communication information and electronic device information created, stored, or transmitted via District technology.
    b. The data that employees create, store, and/or transmit using District technology is not private and is considered the property of the District, even when employees use a password to secure the device or service.
    c. The District retains the right to inspect, delete, and report any apps, information, and files on District technology. Employees uncomfortable with this stipulation should refrain from loading personal information, files, apps, and email accounts onto District-owned devices.
    d. Employees are prohibited from bringing illegal content onto District technology. The District will comply with all legal requirements for notification and reporting of any illegal activity or suspected illegal activity to law enforcement officials.
    e. Employees who choose to access District technology services (e.g., the District's network) on their personal devices acknowledge and agree to turn over their personally owned devices and/or equipment when requested by law enforcement officials as a condition of accessing District technology services from those devices. Employees who do not agree to these stipulations must refrain from using their personally owned devices and equipment to access and communicate via District technology.
    f. Employees shall periodically examine their district electronic devices and purge them of any personal files, photos, and videos unrelated to the District's educational mission.

3. All District employees are to conduct official business and correspondence ***only*** through District provided or District managed accounts and not through their personal accounts.
    a. District/school business communications are subject to discovery pursuant to a subpoena, public records act request, or other lawful request.
    b. District employees who conduct official District/school communications from their own personal, non-district issued devices acknowledge and agree that, in doing so, those personal devices may be subject to discovery and disclosure pursuant to a subpoena, public records act request, or other lawful request

c. 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.
d. District provided email accounts are strictly for educational business use and shall not be used for personal purposes.

4. Accounts used to access District technology services must be kept secure (e.g., device logins, email, file storage, student information systems, electronic grade books, attendance and grade reporting functions, etc.)
    a. Employees are required to 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. Under no circumstances are employees to give their password(s) to students or let students or other unauthorized user input grades or attendance information into grade book/attendance programs.

PROHIBITED USES

The following non-exhaustive list is intended to provide employees with examples of prohibited conduct, but is not intended to serve as a comprehensive list of potential employee misconduct related to the impermissible use of District technology:

1. Creation and transmission of material that a recipient might consider disparaging, harassing, and/or abusive based on race, ethnicity, national origin, immigration status, sex, gender, sexual orientation, age, disability, religion, and/or political beliefs.
2. Accessing, creating, publishing, or transmitting harmful or inappropriate matter that is sexually explicit, obscene, or threatening or that promotes any activity prohibited by law, Board policy, or administrative regulation;
3. Creating, transmitting, or publishing defamatory material;
4. Engaging in plagiarism;
5. Infringing upon copyright, including software, published texts, and student work, or storing and/or public showing of audio and video media for which proper license or ownership is not maintained;
6. Transmission of commercial and/or advertising material;
7. Political and/or religious proselytizing;
8. Intentionally interfering with the normal operation of District technology, including the willful propagation of computer viruses, use of spyware, or other malware;
9. Causing congestion or disruption to District technology 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;
10. Accessing, changing, or using another person’s account, files, output, records, or username for which one does not have explicit authorization to do so.

LEGAL COMPLIANCE

District employees must obey all applicable laws and follow rules of professional conduct when using technology during the performance of their duties. Particular care should be exercised when transmitting confidential information about students, employees, and/or any other business of the District. Employees must ensure that their activities while using District technology are in compliance with the following federal and state laws:

1. The **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)**, which protects against the online collection of personal information from children under 13.

4. The federal **Digital Millennium Copyright Act (DMCA)**, which addresses copyright infringement with regards to digital media.

5. The federal **Family Educational Rights and Privacy Act (FERPA)**, which 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)**, which protects the rights of students and employees regarding confidential health information.

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

8. The California **Chavez Bill AB 307 Educational Technology** (2006), which address student and staff education in ethical use of technology, internet safety, plagiarism, copyright, and file sharing.

9. 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.

10. 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.

11. 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 regards to operators of websites, online services, and applications that are marketed and used for K-12 school purposes.

12. 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).

STREAMING VIDEO * new section for 2020-21

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, 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 K-12 licensed video streaming company (such as Swank Motion Pictures/Movie Licensing USA, or Motion Picture Licensing Corporation) with a license for that specific performance. Teachers may not show copyrighted videos via Distance Learning without a specific license from Movie Licensing USA or the studio that produced the video to cover that specific "performance."

EQUIPMENT LOSS

In the event of damage or loss of District technology equipment, employees shall complete the District "Tech Equipment Loss Report Form" as soon as possible and submit it to the District Technology Department. If a District device is stolen from an employee, he/she must obtain a police report and attach it to the Loss Report Form. This may allow the District to seek reimbursement from its own insurance carrier in certain cases, among other reasons.

STAFF COMMUNICATIONS

Accountability, Discretion, and Professionalism: As in all social situations, employees should remember that they represent the District and recognize that they model good judgment for students and others. Social media activities may be visible to current, past, or prospective students, parents, colleagues, and community members. Employees should therefore exercise discretion and professionalism with *all* online communications and postings, both personal and job-related. Employees must understand that they are always accountable for their postings, social media content, and other electronic communications. This is especially true for online activities conducted with a District e-mail address; while using District Technology; while on District property; and while discussing District-related activities or information.

Interacting online with colleagues, students, parents, and alumni should be considered the same as interacting with those individuals or groups face-to-face. Accordingly, the use of technology and electronic communication should be used to enhance effective communication and collaboration, creativity, and critical thinking skills. Social networking sites (e.g., Facebook, Instagram, Tumblr, Twitter, Pinterest, etc.), school-based content and learning management systems, e-mail, texting, picture and video-based share sites (e.g., Vine and YouTube) should never be used to disparage, harass, intimidate, or violate privacy. The use of websites, blogs, wikis, and media share tools should always be used in accordance with standards of professionalism and employee conduct as outlined in this AUP.

Discretion and prudent judgment in social networking activities are essential for protecting the District, its students, and employees. If an Employee's activity on a social networking site, blog or personal website violates this AUP, the District reserves the right to request that the employee cease such activity, and it may take disciplinary action up to and including termination.

Employee Maintained Webpages: Employees shall ensure that the publically 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 for support.

Use of Student Images and Work: The District considers photographs (including digital photos) to be directory information and thus may be used without explicit permission by the District for non-commercial purposes within digital, online, and traditional publications in accordance with California Education Code section 49076 and Title 34 of the Code of Federal Regulations. 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: Employees should only communicate with students through District provided or sanctioned e-mail and other online platforms (e.g., GSuite/Google Apps for Education, Google Classroom, etc.). 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 that are believed to disappear after receipt. Please see the District's **Social Media Guidelines and Best Practices** document for more information.

SOCIAL NETWORKING

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.

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 will obtain prior written permission to use social media accounts with students by completing the OPUSD Social Media Registry application form (http://bit.ly/OPsocialmediaRegistry) and waiting for that written permission (such as an email reply) from their site principal/administrator before using that platform with students. (* new section for 2020-21)

Use of Social Networks for Development, Alumni, and Admissions Purposes: The District has determined that it is in its best interest to establish a social networking presence (e.g., Facebook, Twitter, or other social media sites) for development, alumni relations, marketing, and other school-related purposes. All official contacts or postings to these sites will be under the direction of the District Office and Administration.

Employment-Related Friends (co-workers, supervisors, and subordinates): Employees in supervisor/subordinate relationships are strongly encouraged to use caution due to the potential for both parties to feel awkward or pressured to accept a "Friend" request for business purposes. Such awkwardness or pressure potentially impacts the work and social relationship, and may raise allegations and concerns about conflicts of interest, unequal treatment, discrimination, or harassment.

Public Information: Given the open nature of the internet and social networks in particular, it is prudent for employees using social networks to assume that *none* of their personal content is private, including photos and videos.

Privacy Settings: Employees should carefully review their privacy settings and exercise care when posting content and information in their online profiles. The District strongly encourage employees to have the highest level of privacy settings on both their personal and professional accounts. Employees should review their personal pages regularly, especially when content is posted by others.

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

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 in perpetuity 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 remains the property of the author who is free to take the material with them when they leave the District.

Misuse of technology may result in discipline, penalties under applicable laws, and/or the loss of technology. Users may be held accountable for their conduct under any applicable District policy or collective bargaining agreement. Illegal production 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.

LIMITATIONS ON DISTRICT RESPONSIBILITY

The District makes no guarantee that the functions or services provided by or through District Technology will be without defect or uninterrupted. The District is not responsible for any damages suffered while utilizing 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. The District is not responsible for any financial obligations arising from unauthorized use of District Technology.

OAK PARK UNIFIED SCHOOL DISTRICT
Staff Technology Acceptable Use Policy (a.k.a. Acceptable Use Agreement)

Copy of Annual Acknowledgement and Signature Page

To be completed and signed online electronically via annual Parent Square Form

Oak Park Unified School District ("District") employees are expected to review, understand, and abide by the policies described in the Staff Technology Acceptable Use Policy ("AUP") and the accompanying procedures provided by the District's Technology Department. This document is legally binding on employees, whether or not they have signed the AUP. District supervisors are required to enforce these policies consistently and uniformly. No supervisor has the authority to override the policies unless he or she obtains the express written permission of the Superintendent. Staff shall electronically sign the Staff Technology AUP Acknowledgement Form each year. Any employee who violates any provision of this AUP shall be considered as having acted in an individual capacity and outside the scope of employment and may be subject to disciplinary action up to and including termination or criminal prosecution by government authorities. The following statements are provided in accordance with Board Policy 4040.

☐ 1. **Student Data Privacy and Security**: In order to safeguard student data protected by state and federal regulations and to ensure privacy, I

- Will NOT allow students to access my Q Teacher Connect account, record attendance, input grades, or otherwise access student information in Q.
- Will NOT post student work (student made videos, presentations, artwork, etc.) online using BOTH their faces and full names. This includes publicly accessible websites, social media outlets, and YouTube. (First names only, or initials are okay)*.
- Will be cognizant of any students in my class who have signed the Media Opt-Out form (housed at the school office) which prohibits the use of images of their faces anywhere on publicly facing communications.

*Announcements of student achievements that are in the public record (such as sports results, or winners of awards) which include the student's name may be shared on social media along with photos commemorating those awards/achievements as long as the parents have not filled out a Media Opt-Out form.

☐ 2. **Website Compliance:**

- **ADA** I understand and acknowledge that all of my publicly accessible school and class webpages need to be fully accessible to individuals with disabilities. In order to do so, I understand that my web pages should maintain compliance with Web Content Accessibility Guidelines (WCAG 2.0+).
- **Proprietary Materials** I understand that publisher's curricular materials may NOT be uploaded and shared on a publicly facing teacher/class/school webpage (republishing copyrighted work is prohibited), but may be distributed to students from within a closed classroom forum which requires a password at login, such as Google Classroom, or a shared Google Doc/Site with sharing permissions set to share with OPUSD users only. (Ensuring copyrighted materials stay within the "four walls of a classroom" adheres to Fair Use Guidelines for educational use of copyrighted materials).

☐ 3. **No Expectation of Privacy**: I understand and acknowledge that I have no expectation of privacy when using District technology, as defined in the Staff Technology AUP.

☐ 4. **No Possessory Interest**: I understand and acknowledge that I have no specific ownership or possessory right in the District-owned devices I use or in the information stored or created therein. I understand and acknowledge that District-owned devices are the property of the District. District-owned devices and the information contained therein may be assigned or used by other employees.

☐ 5. **District Access to Devices and Accounts**: I understand and acknowledge that the District has the right to and does periodically upload information from the District-owned device(s) assigned to me. I understand that the data I create, store, and/or transmit using District technology is not private and is considered the property of the District, even when I am provided my own password. I understand that the District will periodically access my District-owned device(s) (e.g., cellular telephone, computer (laptop and/or desktop), and/or other personal computing and communicating devices) and district managed online accounts to perform the following functions:

(a) Repair or maintenance of the device;
(b) Upgrade or update of the device;
(c) Retrieval of information in response to Public Records Act;
(d) Retrieval of records in compliance with the Pupil Record Act, Education Code section 49062, et seq., FERPA and AB 1584;
(e) Conduct administrative searches of the device;
(f) Fulfill the District's statutory duties and Board policies to maintain public records; and
(g) Any other District or school related purpose.

☐ 6. **Personal Devices:** I understand and acknowledge that any District or school records maintained on any of my personally owned devices, or messages sent or received on a personally owned device that is being used to conduct District business, may be subject to discovery and disclosure, pursuant to a subpoena or other lawful request.

☐ 7. **Personal Files:** I understand and acknowledge that I have hereby been reminded to purge my District issued devices and accounts of personal files, photos, and videos on a regular basis in order to protect my personal privacy and to ensure that there are sufficient resources remaining on the device/service to conduct District business.

☐ 8. **Exclusive Use of District Technology**: I understand and acknowledge that in order to comply with state and federal student privacy laws, I will **not** allow people who are not District employees (such as **parents, volunteers, students, children, spouses, or significant others**) to use or access my District-owned devices or any other District technology since confidential or protected student information or sensitive District information may be stored or accessed from there.

☐ 9. **Video Streaming:** I understand and agree not to use consumer/retail streaming video services in the course of face-to-face instruction or distance learning. I recognize that my school will need to obtain a specific performance license from a movie licensing agency if I wished to show an internet streamed copyrighted video. Otherwise, I will only show videos played from legally purchased physical media (such as DVD or Blu-Ray).

☐ 10. **Social Media Accounts:** I understand and agree to obtain prior written authorization from my site administrator before using social media accounts with students using the Social Media Registry located at http://bit.ly/OPsocialmediaRegistry.

I have read and understand the Staff Technology Acceptable Use Policy, the latest version of which is

posted on the District's website at www.opusd.org/staffaup. A copy of the District's **Social Media Guidelines and Best Practices** document can also be found there.

OPUSD Staff, this is a copy of the online acknowledgement form that is distributed to all staff via Parent Square post. Do NOT sign and submit this form via paper, but do activate your staff Parent Square account and find the relevant post which contains the electronic form with e-signatures entitled "**Staff Technology Acceptable Use Policy Acknowledgement Form**."

00536-00005/4269103.3