OAK PARK UNIFIED SCHOOL DISTRICT
Staff Technology Acceptable Use Policy

This Acceptable Use Policy ("AUP") outlines the acceptable use of "District technology" for Oak Park Unified School District ("District") personnel.

"District technology" includes, but is not limited to, District-owned or managed electronic devices and use of or accessing district owned or managed systems or services related to electronic data and/or communications. These include but are not limited to computers, wireless communication device (smartphones, mobile computers and tablets, emergency radios, etc.) telephones, external storage devices (flash drives, mobile hard drives, etc.), and wearable technology; use of District messaging systems (such as email, voicemail, text messaging, etc); accessing the district's wired and wireless data networks; accessing network information sources; use of local and online collaboration and file storage systems and services; use of any data systems or software programs owned, managed or licensed by the District (such as Google Apps for Education, Aequitas Q, etc.); use of electronic peripherals including printing, imaging, recording or projection devices or systems; and future technological innovations.

This AUP is in place to protect both the District and its employees. This AUP provides direction regarding the appropriate and inappropriate use of District technology and information/communication services and applies to all District employees, whether or not they come into direct contact with students, and use of all District technology and services.

All aspects of this AUP apply equal whether District technology devices or services are accessed on or off site, and through District-owned or personally owned equipment or devices.

By using District technology, employees agree to abide by all regulations in this AUP. This AUP supports and complements Board Policy 4040.

Considerations reflected in this AUP are:

- Protecting the welfare of children;
- Protecting every individual's right to privacy;
- Protecting intellectual and property rights;
- Respecting the rights of students, parents/guardians, and staff;
- Assuring technology resources are used to promote the District's educational goals; and
- Assuring District technology is of the highest quality and is organized, well designed, and easy to navigate.

The District provides quality services and support for life-long learning opportunities. The District has a strong commitment to providing a quality education for its students, including access to and experience with technology. The District's goals for technology

in education include promoting educational excellence in schools by facilitating collaboration, innovation, and communication; providing appropriate access to all students; supporting critical and creative thinking; fully integrating technology into the daily curriculum; promoting entrepreneurship; modeling and promoting digital citizenship; and preparing students and educators to meet the challenge of participating in a dynamic global society.

The District recognizes that technology can enhance employee performance by improving access to and facilitating the exchange of information, offering effective tools to assist in providing a quality instructional program, and facilitating operations. The District provides a wide range of District technology to students and employees for the purpose of advancing the District's educational mission, which includes teaching, information processing for school business, and enhancing communication between District employees, parents, students, and community members.

All employees are expected to learn and use the available technological resources that will assist them in the performance of their job responsibilities. These resources are provided at the public's expense and maintained by the District, and therefore, 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, decent, and polite manner, consistent with the District's Mission and Goals, as well as existing and applicable laws and regulations. This AUP does not attempt to articulate all required or prohibited behaviors by users. The District Technology Department can provide additional guidance, support, or clarification when needed.

1. Employees have no reasonable expectation of privacy in use of District technology.

2. The District reserves the right to monitor all employee use of District technology within the jurisdiction of the District without specific advance notice.

3. 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 are provided their own password.

4. Upon receipt of a District-owned device, the employee may be the authorized possessor as defined in the California Electronic Communications Privacy Act ("CalECPA"), also known as Senate Bill 178. As an authorized possessor of a District-owned device, employees are responsible for using the device appropriately for employment related purposes. Only the employee assigned by the District to the device, may use the device.

5. Employees have no specific ownership or possessory right in the District-owned device used or in the information stored or created therein. The District may confiscate any District-owned device at any time and without cause. If the District confiscates a District-owned device, the employee is no longer the authorized possessor of the device. 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.

6. The District has the right and does periodically upload information from District-owned devices to District maintained servers and databases.

7. 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.

8. Employees using personal accounts to load applications ("apps") and resources onto a District-owned device must exercise prudent judgment to ensure that only appropriate apps and resources for the school setting are loaded onto the District-owned devices. Employees have no reasonable expectation of privacy in personal apps, files, or email accounts residing on a District-owned device or District managed service. The District retains the right to inspect, delete, and report any apps, information, and files that find their way onto District-owned technology. Employees uncomfortable with this stipulation should refrain from loading personal information, files, apps, and email accounts onto District-owned devices.

9. Records maintained on any personally owned device or messages sent or received on a personally owned device that is being used to conduct District business may be subject to disclosure, pursuant to a subpoena or other lawful request.

10. Employees who choose to use District technology with their own personally owned computing devices do so at their own risk and forfeit any expectation of privacy in information stored on or accessed using District technology. This includes any communications that travels through the District's network.

11. 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.

12. Employees who choose to use District technology (e.g., the District's network) on their personal devices agree to turn over their personally owned devices and/or equipment when requested by law enforcement officials as a condition of access to District technology. Employees who do not agree to these stipulations must refrain from using their personally owned devices and equipment to access and communicate with District technology.

13. District staff member accounts for access to District technology (e.g., network access, internet access, and access to employee resources such as email, student information systems, electronic grade books or attendance and grade reporting functions) must be kept secure. Under no circumstances are employees to give their password(s) to students or let students input grades or attendance information into grade book/attendance programs. Employees are to keep their passwords secure and should not write down their passwords anywhere near the computer or where a student might discover them.

14. District technology is intended to further the District's mission of educating the students of the District. All communications using District Technology and all communications related to an employee's professional duties should be aligned to the District's educational mission and goals.

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. Accessing, creating, posting, submitting, publishing, displaying or transmitting harmful or inappropriate matter that is threatening, offensive, obscene, disruptive, sexually explicit or unethical, or that promotes any activity prohibited by law, Board policy, or administrative regulation;

2. Creating, publishing, or transmitting defamatory material;

3. Engaging in plagiarism;

4. 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;

5. Political and/or religious proselytizing;

6. Intentionally interfering with the normal operation of District technology, including the propagation of computer viruses and unsanctioned high-volume network traffic that substantially hinders others in their use of the network;

7. Causing congestion or disruption District technology through inappropriate downloads of large files, streaming audio/video, or other such activities;

8. Examining, changing, or using another person's files, output, records, or user name for which they do not have explicit authorization;

9. Transmission of commercial and/or advertising material; and

10. Creation and transmission of material that a recipient might consider disparaging, harassing, and/or abusive based on race, ethnicity, national origin, sex, gender, sexual orientation, age, disability, religion, and/or political beliefs.

The District allows limited access to web based personal email accounts for personal correspondence provided personal emails are brief, limited in number, and generated during off duty time. In order to preserve District technology bandwidth and resources, District employees are encouraged to use their personal email accounts from home for non-work related communications. District provided email accounts are strictly for educational business use and should not be used for personal purposes.

When District technology is used to transmit confidential information about students, employees, and/or the business of the District, all appropriate safeguards must be used. District employees, during the performance of duties, must obey all applicable laws and must follow rules of professional conduct. The District is committed to compliance with the following:

1. The federal Family Educational Rights and Privacy Act (FERPA), which protects the rights of students regarding education records.

2. The federal Health Insurance Portability and Accounting Act (HIPAA), which protects the rights of students and employees regarding protected health information.

3. The federal Children's Internet Protection Act (CIPA), which protects the safety and privacy of minors. Consequently, the District uses appropriate 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.

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

5. The federal Protection of Pupil Rights Amendment (PPRA), which concerns the administration of surveys to students that cover 8 protected areas and ensuring student privacy, parental access to information, and prior parental consent.

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

7. The federal ERATE regulations, which address the appropriate and ethical use of information technology in the classroom so that students and teachers can distinguish lawful from unlawful uses of copyrighted works, including the

following topics: the concept and purpose of both copyright and fair use; distinguishing lawful from unlawful downloading and peer- to-peer file sharing; and avoiding plagiarism.

8. The California Chavez Bill AB 307, which addresses the education of students and employees on ethical use of information technology, Internet safety, plagiarism, copyright, and file sharing.

9. The California Assembly Bill 1584 (2014) and Student Online Personal Information Protection Act (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.

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.

All users of District technology must exercise individual vigilance and responsibility to avoid inappropriate and/or illegal activities. Employees are ultimately responsible for their actions in accessing and using District technology. The District accepts no liability relative to information stored and/or retrieved on District technology. The District accepts no liability for employee-owned technology resources used on District property or in connection with District technology.

Employees must complete the District "Tech Equipment Loss Report Form" in the event of damage or loss of District technology 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.

AUP: Staff Communication

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 (yours or others). The use of personal 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.

When engaging in online communications, employees must adhere to the following, which are consistent with the District's workplace standards on harassment, student relationships, conduct, professional communication, and confidentiality:

- Employees may not make statements that would violate any of the District's policies.
- Employees may not disclose any confidential information pertaining to the District, its schools, employees, students and their families, or visitors, including prospective families.
- Employees must comply with federal, state, and local laws, including the California Child Abuse and Neglect Reporting Act, when engaging in online communications.

Use of Student Images and Work: Employees must verify media release permissions have been obtained from students/parents before uploading any content containing named student work or image of said student.

Class Use of Social Networking: Employees may use appropriate social networking tools for educational purposes only. Such purposes may include clubs, athletic teams, and co-curricular activities. Employees must adhere to COPPA in relation to student privacy and identity. Please see "Social Media Guideline and Best Practices" for more information.

Use of Electronic Communication with Students: It is recommended that employees only communicate with students through District provided or sanctioned e-mail and other online platforms (e.g., Google Apps for Education, Class Dojo, etc.). Employees should limit use of Short Message Service (SMS), Multimedia Messaging Service (MMS), or peer-to-peer messaging, (e.g., iMessaging through iPhone) or any other texting, picture 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 "Social Media Guideline and Best Practices" for more information.

Friending/Following: It is recommended that employees do not have **personal** social networking relationships (e.g., "friend" or "following" relationships) from employee personal accounts with current students of any age or former students under the age of 18. Employees may use their school-related social networking page to communicate, share and connect ("friend") with students for educational purposes.

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. We strongly encourage employees to have the highest level of privacy settings on both their personal and professional accounts. Employees may wish to review their personal pages regularly, especially when content is posted by others.

Accountability, Discretion, and Professionalism: As in all social situations, employees should remember that they represent the District and recognize that they model adult behavior for our students. 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 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.

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 may take disciplinary action up to and including termination.

OAK PARK UNIFIED SCHOOL DISTRICT
Staff Technology Acceptable Use Policy

Annual Acknowledgement and Signature Page

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 and the accompanying procedures provided by the District Technology Department. This document is legally binding on employees, whether or not they have signed the Acceptable Use Policy. 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 written permission of the Superintendent. Signed Acceptable Use Policies are kept on file at the District. Any employee who violates any provision of this Acceptable Use Policy shall be considered as having acted in an individual capacity and outside the scope of employment and, as such, 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.

I have read and understand the Staff Technology Acceptable Use Policy, the latest version of which is posted on the district website at www.opusd.org/staffaup. A copy of the Social Media Guidelines and Best Practices informational document can also be found there.

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 Acceptable Use Policy.

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.

District Access to Device: I understand and acknowledge that the District has the right 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) 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; and,
(f) Fulfill the District's statutory duties and Board policies to maintain public records.

I also understand 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 disclosure, pursuant to a subpoena or other lawful request.

I also understand 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 since confidential or protected student information or sensitive District information may be stored or accessed from there.

Employee Name: _____(Printed)

Employee Signature: _____

Date: _____

Effective School Year: _____

00536-00004/3280993.2EK