OPUSD Student Technology Acceptable Use Agreement

Overview of Responsible Digital Citizenship for Students

1. **Be aware of what you post online.** Social media venues including wikis, blogs, photo and video sharing sites are very public. What you contribute leaves a digital footprint for all to see. Do not post anything you wouldn't want friends, enemies, parents, teachers, or a future employer to see.

2. **Follow the school's code of conduct** when writing online. It is acceptable to disagree with someone else's opinions, however, do it in a respectful way. Make sure that criticism is constructive and not hurtful. What is inappropriate in the classroom is inappropriate online.

3. **Be safe online**. Never give out personal information, including, but not limited to, last names, phone numbers, addresses, exact birthdates, and pictures. Do not share your password with anyone besides your teachers and parents.

4. **Linking to other websites to support your thoughts and ideas** is recommended. However, be sure to read the entire article prior to linking to ensure that all information is appropriate for a school setting.

5. **Do your own work**! Do not use other people's intellectual property without their permission. It is a violation of copyright law to copy and paste other's thoughts. When paraphrasing another's idea(s) be sure to cite your source with the URL. It is good practice to hyperlink to your sources.

6. **Be aware that pictures may also be protected under copyright laws.** Verify you have permission to use the image or it is under Creative Commons attribution.

7. **How you represent yourself online is an extension of yourself**. Do not misrepresent yourself by using someone else's identity.

8. **Blog and wiki posts should be well written**. Follow writing conventions including proper grammar, capitalization, and punctuation. If you edit someone else's work be sure it is in the spirit of improving the writing.

9. If you run across **inappropriate material** that makes you feel uncomfortable, or is not respectful, **tell your teacher right away**.

10. **Abide by the full Student Technology Acceptable Use Agreement** - www.opusd.org/aua

Adapted from http://goo.gl/IVqvPD

OPUSD Student Technology Acceptable Use Agreement

Oak Park Unified School District ("OPUSD" or "District") offers its educational community a wide range of technologies to support teaching and learning. The District is committed to promoting a respectful, secure, and responsible learning environment in all areas of the educational setting, including the digital context. This Technology Acceptable Use Agreement ("AUA") provides students and parents (all further references to "parents" in this AUA include parents or legal guardians) with the rules, expectations, and guidance for a student's appropriate use of District technology.

Use of District technology shall comply with all OPUSD Board policies and procedures, including, but not limited to, Board Policy 6163.4, as well as all applicable federal and state laws. California Education Code 48900 also applies to this AUA. Education Code 48900 describes a school's jurisdiction over student activity and discipline to include:

(1) While on school grounds.
(2) While going to or coming from school.
(3) During the lunch period whether on or off the campus.
(4) During, or while going to or coming from, a school-sponsored activity.

District "technology" includes all tools and resources including but not limited to, **District-owned computing devices and peripherals** (e.g., computers, laptops, tablets, removable storage devices, wearable technology, interactive classroom projection systems, etc.); **District network and communication devices/services** (telephones, wired and wireless networks including WiFi access points, emergency radios, email systems, file servers, etc.); **District-managed on-line services** (such as G-Suite/Google Apps For Education, EADMS, Aequitas Q Student Information System, etc.); access to all on-line collaboration and information sources; and any and all future technological innovations.

The advent of on-line learning spaces, particularly those managed by the District (including Google's G-Suite/Google Apps for Education), expands the concept of class time beyond the school campus. Students should consider their use of District provided on-line accounts a school-sponsored activity so that their actions and behaviors while on-line using school accounts and interacting with others falls under the purview of this AUA. This is particularly true in District 1-to-1 take-home mobile device programs.

OPUSD supports and encourages students' First Amendment right to free speech, but a student's communication that adversely impacts a school's instructional environment (e.g., making others feel unsafe while on campus or in a district managed on-line collaboration tool) may not be speech protected by the Constitution-- even if it occurs off campus (See, U.S. Supreme Court ruling in *Tinker v. Des Moines Independent Community School District*). Students are cautioned to communicate responsibly while on-line at all times to ensure the school environment remains safe and welcoming to all.

Before a student is authorized to use District technology, a student and his/her parent must acknowledge that they have read, understood and signed this AUA. By using District technology students and parents agree to the following:

1. By using District technology, whether from personal or District-owned devices, students and parents grant specific consent, as defined by the California Electronic Communications Privacy Act (also known as "CalECPA" or Senate Bill 178), for the District to review and monitor all electronic communication information and electronic device information created with, stored on, or transmitted via District technology.
2. The District may monitor or access any and all student use of District technology without any further advanced notice. Students have no reasonable expectation of any right to privacy while using District technology, which, as stated above, includes any and all files and communications traveling over or stored on its network, or while using District provisioned accounts and on-line resources including email and on-line collaboration tools at any time.
3. Students must abide by all school policy and procedures as outlined in their school's Student Handbook when using District technology. The inappropriate use of technology while on campus or through district managed accounts off campus may result in school discipline.
4. Electronic devices are only permitted for educational uses while on campus. Students who play games, text message, or attempt to access social networking websites or applications during class time without the consent, direction, and supervision of a teacher may have the privilege to use District technology suspended or revoked. Repeated violations may result in more severe discipline.
5. The District may act as an authorized agent for the creation of on-line student accounts solely for educational purposes in accordance with state and federal student information privacy laws (COPPA, FERPA, SOPIPIA, etc.). District managed student accounts may include but are not limited to, on-line accounts created to access Google G-Suit (Google Apps for Education), Apple iCloud/Classroom, Microsoft Office365, and access to other apps, programs, or on-line services and digital curriculum resources.
6. Cellular phones and personal electronic devices may be brought to campus and used only under the following specific circumstances.

    a. **Elementary & Middle School Policy Specifics**: Cellular phones and personal electronic devices must be turned off and stowed during school hours, including non-class time (e.g., recess, nutrition, lunch).

    b. **High School Policy Specifics**: Cellular phones and personal electronic devices may be used during non-class time (e.g., nutrition, lunch), in a manner that abides by this AUA.

    Students who bring cell phones or other personal electronic devices to school do so at their own risk. Students and parents release the District from liability due to loss, damage, or theft, or loss of use of the device, even if confiscated. All personal devices brought to school by students must be kept in the **OFF position** and out of view during class time unless allowed by the classroom teacher or administrator and under their direct supervision. Students may use cell phones or other personal electronic during class time **only if** under the direct supervision and instruction of a teacher or administrator. Failure to comply may result in the immediate confiscation of the device, and the District will only return the device to a student's parent.
7. **S**chool issued and personal cell phones or other electronic devices (especially any device with a camera or recording capability) may not be turned on or taken out of its covered carrying case/bag in a bathroom or locker room. If a student is found with a device turned on or out in the open in either of these locations the device will be confiscated immediately and may result in more severe discipline/consequences.

8. The data that students create, store and transmit using District technology is not private and is considered the property of the District. Personally owned cell phones and other electronic devices will **not** be searched unless there is a reasonable suspicion, under the circumstances, that the student is violating school rules, District policy, or the law. (*New Jersey v. T.L.O.)*

9. Any content created by students (including text, posts, comments, images or video) may be shared appropriately on-line by the District, the school, or the student's teacher. The District holds the safety of its students in the highest regard. However, the ability to share information and teach responsible digital citizenship is also vital to the educational process. This includes the use of e-mail, school learning management systems, on-line collaboration tools, classroom photo sharing services, and other social media avenues when applicable under the guidelines of the District's Best Practices of Social Media in Education document.

10. The District may use images and videos of students for marketing and community outreach including on the school and district's website and print materials. Parents may decline to allow this by completing a **Student Media Release Opt Out Form** obtained from the school office and obtaining a signature of receipt on that Form from their child's school office manager or designee. This Opt out Form must be completed annually.

11. The following activities or uses of technology are prohibited to ensure a **respectful** digital learning environment:
    - Using technology to threaten, bully, or harass others by sending, accessing, uploading, downloading, or distributing text, images, or other materials or means that are offensive, threatening, profane, obscene, or sexually suggestive or that could be construed as harassment or disparagement of others based on their race/ethnicity, national origin, sex, gender, sexual orientation, age, disability, religion or political beliefs.
    - Recording video or audio of other students or staff without their permission.
    - Searching for, accessing, or possessing lewd, sexually suggestive, graphically violent, or derogatory/demeaning images and/or media files.
    - Posing on-line as someone other than themselves.
    - Using District issued devices or network to search for and/or access repositories of illegal content, content that may cause harm to the District's network, or content that promotes, encourages, or teaches students how to commit an illegal act (e.g., bomb-making, pirating electronic media, intentionally causing harm, etc.).
    - Bypassing (or attempting to) the District's internet content filter through a web proxy, anonymizers, or other means from a District or personal computing device.

12. The following activities or uses of technology are strictly prohibited to ensure a **secure** digital learning environment:
    - Circumventing network security measures or attempting to access confidential, private, or restricted information on the District's network or district managed on-line services.
    - Sharing one's passwords or access to on-line accounts with anyone other than the student's parent or trusted adult.
    - Logging into a device or service with the account of another student or a staff member or otherwise gaining access to their files and accounts without their permission.
    - Sharing or publishing personal information on-line such as a phone number, home address, financial information, social security numbers, family issues, login credentials and passwords.

- Destroying, damaging, defacing, or rendering unusable any property (both physical property like a computer, or virtual, such as a webpage) belonging to the District or another person.
- Altering a District device's settings in a manner to cause confusion, frustration, or loss of use to other users (changing backgrounds, homepages, dock, network configurations, account logins, etc.).
- Using or installing viruses, malware, keyloggers, spyware, or other software/hardware that can be used to damage the District's network, harvest other users' login information and other data, or propagate unwanted messages or files.

13. The following activities or uses of technology are strictly prohibited to ensure a **responsible** digital learning environment:
    - Plagiarism or other forms of academic dishonesty
    - Illegally downloading, storing, installing, or transmitting copyrighted materials without the proper license or permissions. The District explicitly forbids student use of torrenting software or services on the District network.
    - Stealing others' intellectual property including text, music, movies, and software, or using them without the appropriate citation or expressed permission in accordance with Copyright Laws and Fair Use guidelines or any other applicable laws.
    - Using or visiting social networking sites (e.g., Facebook, Instagram, Twitter, Vine, etc.) during class time for non-educational purposes during class time.
    - Use of instant messaging or chat rooms not directly related to instruction (including texting, picture messaging, audio and video messaging) during class time.
    - Publishing personal information including private events and images (e.g., weekend plans or a party/event that not everyone in the class is invited to) or using social media to share images to brag about events to purposefully make others feel left out or uncomfortable.

14. Everything students put on-line can create a permanent digital footprint that remains out of their control. Students should be mindful of the digital trail they create for themselves – it is like a tattoo which is almost impossible to erase. Apps, websites, and software that claim to delete information may still leave a permanent record accessible to others. Students should not assume their on-line presence will remain private and should conduct themselves on-line expecting that any and all data they furnish could be accessible to a wider audience such as admissions officers and potential employers in the future.

15. All OPUSD academic and behavioral policies and expectations apply to all technology use on campus while using District technology or personal devices, or any off-campus use of technology that may cause serious disruption at school. The District reserves the right to intervene when off-campus (including on-line) issues are brought to its attention that have the potential to impact school climate and safety.

16. Students whose behavior or device repair record indicates careless use or abuse of school issued devices or other District technology will be referred for appropriate disciplinary action consistent with this AUA.

17. The District can impose disciplinary action as a result of any violation of Board policy or this AUA including one or more of the following:
    - An increase in the supervision of a student's use of District technology.
    - The confiscation of a device.
    - Limitation or cancellation of a student's user privileges.

- Discipline, including, but not limited to, detention, suspension and expulsion in accordance with the student behavior and discipline policies outlined in a Student's school Student Handbook or applicable law.
- Legal action in accordance with Board policy or law.
- Reimbursement of expenses.

As the District works to fulfill its mission of preparing students for higher education and an evolving workforce, it will increasingly utilize tools and resources that are housed on-line and accessed through the internet. On-line accounts are necessary for web based file storage and collaboration tools such as Google Drive, Google Classroom, Google Docs, and District administered Google email, as well as other educational web-based resources. Web and cloud-based services permit on-line distribution and hand-in of student assignments, on-line based class discussions and collaboration activities, web-based curriculum or learning resources, and in some grade levels, student email.

District provisioned student accounts will comply with state and federal student privacy requirements. In California, the Student On-line Personal Information Protection Act SOPIPA (AB1584, SB1777, and AB1442) creates privacy standards for all on-line services catering to K-12 education in California and prevents them from advertising to students, building digital profiles about them, or selling harvested student information to other parties. The District believes these restrictions provide a safe environment for students to utilize accounts that are created by the District for accessing on-line educational resources and services.

The federal Child On-line Privacy and Protection Act (COPPA) allows school districts to provide consent on a parent's behalf to create on-line accounts which may collect student information **limited to the educational context and for no other commercial purpose.** OPUSD operates under these guidelines to create and manage on-line student accounts. By law, parents may choose to opt out of this implied parental consent by obtaining the **Student On-line Account Opt-Out Form** from their child's school office, completing the form, scheduling a conference with the school principal, and signing the Opt-Out form in the presence of the principal who will sign receipt of the form after discussing reasons for and the consequences of opting out.

Parents and students should be aware that opting out of District managed on-line accounts for students can significantly impact a student's ability to participate in some class lessons and activities and may also impair students from learning state-mandated digital citizenship principals and practicing responsible digital behaviors taught in class. It might also make it more difficult for them to receive assignments, participate in on-line collaborative class projects, submit work to their teacher, or access on-line lessons, digital textbooks, and on-line tutorials. Because the District's progressive use of technology to enhance learning is part of its core values, parents recognize the importance of allowing the District to carry out its mission to promote responsible digital citizenship and safe on-line practices and behaviors for all students through creating and maintaining on-line student accounts.

As part of the District's multi-tiered digital citizenship training strategy, **students will not be allowed access to email services in grades k-2** even though the District will assign each student a Google log-in. **Students in grades 3-8 will have limited email** functionality which allows them to send and receive emails with their teacher and other students within the District, but not the "outside world" unless it is to a specific pre-approved site/destination for a particular assignment. The District will grant **students in grades 9-12 more access to send and receive e-mails with individuals and organizations outside of the District**, but all email communications must be for educational purposes and the District may monitor them.

Student Technology Acceptable Use Agreement
Acknowledgement Page

Parents and Students to acknowledge receipt, reading, and understanding the contents of this AUA on an annual basis. These policies are in effect whenever a student uses or accesses District technology, including but not limited to, the District network or District managed on-line accounts. Parents and Students agree to abide by the AUA as a condition for using District technology.

Notice of Student On-Line Account Opt-Out Form

According to the Federal Children On-line Privacy Protection Act (COPPA), the District must allow parents to Opt Out of the District's plans to create and manage on-line student accounts used for educational purposes. Parents may obtain the **Student On-line Account Opt-Out Form** from the school office, schedule a conference with the school principal, and then complete and sign the Opt-Out form in the presence of the principal who will counter sign receipt of the form after a discussion about the reasons for and the consequences of opting out. If parents do not submit a Student On-Line Account Creation Opt-Out Form, the District shall assume implied consent to the District creating and managing on-line accounts for their child(ren) in order to provide access to educational materials, services, and on-line storage of student information.

Notice of Student Photo and Media Release Opt-Out Form

In accordance with California Education Code section 49076 and Title 34 of the Code of Federal Regulations, the District considers photographs (including digital photos) to be directory information and thus may be used by the District for non-commercial purposes including digital, on-line, and traditional publications. Parents may opt-out of the use of student photos by the District by completing the **Media Release Opt-Out Form** which may be obtained from the school office and submitting the completed form to the school office annually with a counter signature.

By using District technology resources after reading this AUA, we (Parent and Student) agree to not hold the District, or any District staff, responsible for the failure of any technology protection measures or users' mistakes or negligence and agree to indemnify and hold harmless the District and District staff for any damages or costs incurred as is required by Board Policy 6163.4.