SUMMARY: *This policy was written to inform students, their families, and staff about the acceptable ways in which information technology systems may be used in Pacifica School District. Pacifica School District is committed to improving student achievement and preparing all students to be college/career ready graduates. District Technology, which includes but is not limited to: computer hardware, software, and the Internet, provide powerful tools to access information and communicate with people, enhancing learning and enabling the district to operate. With the constant introduction of new technology, new ways to communicate, and new ways to access and transfer information, it is therefore critical that the district continue to define a policy that ensures a safe learning environment for students and staff as well as the protection of the district's technology. The use of PSD technology is offered to students and staff as a privilege which must be safeguarded by all Users. The use of district technology is a privilege permitted at the district's discretion and is subject to the conditions and restrictions set forth in applicable Board policies, administrative regulations, and this Acceptable Use Agreement. The district reserves the right to suspend access at any time, without notice, for any reason.*

Technology Acceptable Use Policy

The Pacifica School District (PSD) is pleased to provide technology, including, but not limited to: computers, software, networks and Internet services. **Acceptable use of PSD technology is for the purpose of improving student learning and to prepare students to be positive, contributing members of a healthy digital community.** PSD technology remains at all times the property of PSD.

The PSD Technology Acceptable Use Policy ("AUP") is in place to promote a safe, respectful, responsible digital community and to prevent unauthorized access and other unlawful activities by Users online, prevent unauthorized disclosure of or access to sensitive information, and to comply with the Children's Internet Protection Act ("CIPA"). As used in this policy, "User" includes anyone, including employees, students, and guests, using PSD technology, including, but not limited to, computers, networks, Internet, email, chat rooms and other forms of technology services and products. Only Users who agree to this Acceptable Use Policy are authorized to use PSD technology.

This policy describes acceptable uses of district technology systems (hardware, software, network, and Internet) as well as unacceptable uses. These policies are established to:

- Enhance teaching and learning;
- Increase safety for students and staff;
- Improve the efficiency of district technology systems;
- Ensure alignment with PSD Core Beliefs and Commitments;
- Ensure compliance with applicable district policies, state and federal laws; and
- Educate students, staff, and other who use Pacifica School District technology.

Definitions

District technology includes, but is not limited to, computers, the district's computer network including servers and wireless computer networking technology (wi-fi), the Internet, email, USB drives, wireless access points (routers), tablet computers, smartphones and smart devices, telephones, cellular telephones, personal digital assistants, pagers, MP3 players, wearable technology, any wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off site or through district-owned or personally owned equipment or devices.

1. User Responsibilities

Users are required to follow this policy and report any misuse of the District's technology, including network or Internet to a supervisor or other appropriate District personnel. Access is provided primarily for education and District business. Staff

may use the Internet, for incidental personal use during duty-free time. By using the network, Users have agreed to this policy. If a User is uncertain about whether a particular use is acceptable or appropriate, he or she should consult a supervisor or other appropriate District personnel.

2. Acceptable and Unacceptable Uses of PSD Technology

Technology in PSD is intended to promote the District's education goals and develop responsible digital citizenship. Students are responsible for appropriate behavior on the school's network just as they are in a classroom or on a school playground.

The District reserves the right to take immediate action regarding activities 1) that create security and/or safety issues for the District, students, employees, schools, network or computer resources, or 2) that expend District resources on content the District in its sole discretion determines lacks legitimate educational content/purpose, or 3) other activities as determined by the District that engage in or promote any practice that is unethical or violates any law or Board policy, administrative regulation, or district practice.

These are some examples of what the District considers an *inappropriate* use of technology. This list is merely exemplary and is not intended to limit the District's ability to impose discipline for any inappropriate use of technology not listed here:

1. Violating any state or federal law or municipal ordinance, such as: Accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials.
2. Criminal activities that can be punished under the law.
3. Selling or purchasing illegal items or substances.
4. Obtaining and/or using anonymous email sites, spamming, spreading viruses.
5. Causing harm to others or damage to their property.
6. Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others; accessing, transmitting, or downloading offensive, harassing, or disparaging materials. This includes, but is not limited to, any form of cyberbullying and harassment, engaging in personal attacks, cyberstalking, exclusion, trolling, impersonation, trickery, and outing. Harassment is defined as persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending them messages, they must stop.
7. Deleting, copying, modifying, or forging other users' names, emails, files, or data, disguising one's identity, impersonating other users, or sending anonymous email.
8. Disclosing anyone's confidential information or personal identifying information without their consent or (if they are minors) the written consent of their parent or guardian.
9. Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files, software or programs, or disrupting any computer system performance.
10. Using any District computer to pursue "hacking," internal or external to the District, or attempting to access information protected by privacy laws. Users may not attempt to disable filters, antivirus controls, or other technology protection measures.
11. Accessing, transmitting or downloading extraordinarily large files, including, but not limited to, viral downloads.
12. Using web sites, email, networks, or other technology for political uses or personal gain, including profit-making.
13. Users must not intentionally access, create, store or transmit material that may deemed to be offensive, indecent, obscene, intimidating, or hostile; or that harasses, insults or attacks others.
14. Advertising, promoting non-district sites or commercial efforts and events.

15. Users must adhere to all copyright laws.

16. Users are not permitted to use the network for non-academic related bandwidth intensive activities such as network games or transmission of large audio/video or serving as a host for such activities.

3. Security

1. Users must report any weaknesses in PSD Internet and intranet security, any incidents of possible misuse or violation of this agreement to District Webmaster.

2. Every User provided with a User ID and Password must maintain their password privately and not share their password with anyone else.

3. Users must not attempt to access any data or programs for which they do not have authorization or explicit consent.

4. Users must not purposely engage in activity that may degrade the performance of PSD Information Technology systems and related Information Technology property; deprive an authorized PSD User access to a PSD resource; obtain extra resources beyond those allocated; circumvent PSD security measures; change settings on any network devices.

5. Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of PSD Information Technology systems and related Information Technology property.

6. All data must be kept confidential and secure by the User. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. If this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.

7. All software programs, applications, source code, object code, documentation and data shall be guarded and protected.

8. Access to PSD Information Technology equipment must be properly documented, authorized and controlled.

4. Safety

Student Users will not agree to meet with someone they have met online without their parent's approval and participation. Student Users will promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable. Student Users should not delete such messages unless instructed to do so by a staff member after administrative review of the communication.

5. Privacy

The District is the owner of all relevant hardware and software and asserts its right to review and exercise its ownership at any time by search of the system and its equipment, and any information on it. The District reserves the right to monitor Users' online activities and to access, review, copy, and store or delete any electronic communication or files and disclose them to others at any time without prior notice as it deems necessary. Users should have no expectation of privacy regarding their use of District property, network and/or Internet access or files, including, but not limited to, e-mail and social media sites and should be aware that, in most instances, their use of district technology (such as web searches and emails) cannot be erased or deleted.

A Student User may not disclose the personal contact information of another student without the written consent of the student's parent. Other Users may only disclose this information as provided by law and District policy. Personal contact information includes the student's name together with other information that would allow an individual to locate the student, including, but not limited to, parent's name, home address or location, work address or location, or phone number.

6. Cyberbullying

"Cyberbullying" is an act of bullying committed through the transmission of a message, text, sound, or image by means of an electronic device, such as a telephone, wireless communication device, computer, or electronic tablet.

Examples of cyberbullying include, but are not limited to, sending mean, vulgar or threatening messages or images; posting sensitive, private information about another person; pretending to be someone else in order to make that person look bad; and intentionally excluding someone from an online group.

All district policies and procedures regarding bullying apply to cyberbullying, including cyberbullying that occurs using electronic services, accounts, media, and devices owned or used by the District. Not only is District property governed by these policies, but also district-related events, as well as travel to and from District events and school. Several sections of this AUP also address cyberbullying behavior, including Sections 2 (Acceptable and Unacceptable Uses of PSD Technology), 3 (Security), 4 (Safety), 5 (Privacy), 8 (Electronic communications), 9 (Password Policy).

Anyone who participates in or witnesses cyberbullying needs to report it District staff or their parents.

7. Permission to Use the Internet

Pacifica School District is pleased to offer students access to a computer network for use of networked school resources and access to the Internet. All students are permitted to use the Internet on District computers, unless their parents withhold permission on the signature page of this Document (Page 8). Should a parent prefer that a student not have Internet access, use of the computers is still possible for other purposes such as word processing, multimedia, and educational software programs.

Access to the Internet will enable students to explore thousands of libraries, databases, museums, and other repositories of information and to exchange personal communication with other Internet users around the world. Families should be aware that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate, or potentially offensive. While the purposes of the school are to use Internet resources for constructive educational goals, students may find ways to access other materials. We believe that the benefits to students from access to the Internet in the form of information resources and opportunities for collaboration outweigh any potential misuse of the resource. But ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. Therefore, we support and respect each family's right to withhold permission to use the Internet.

8. Electronic Communications

1. Student E-Mail. Students may be provided with District shared classroom accounts for instructional purposes or may be allowed to use personal accounts from non-District providers, under the condition that those students are supervised and monitored at all times in their use of e- mail by staff.

2. Chat Rooms, Online Discussion Groups, and social media. No student may access a chat room, online discussion, or social media site using District technology without permission *and* supervision of the student's instructor.

3. Confidentiality. Student Users will not forward a message that was sent to them privately without permission of the person who sent them the message. Student Users will not release any personal contact about themselves without obtaining the written consent of the parent/guardians of students, and filing such consent with their instructor.

4. Also see Section 2 of this document, regarding acceptable and unacceptable use.

9. Password Policy

1. 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 a student on district technology does not create a reasonable expectation of privacy.

2. Passwords must not be shared with anyone and treated as confidential information.

3. Passwords must have a minimum length of 6 alphanumeric characters.

4. All Users are responsible for managing their use of PSD Information Technology systems and are accountable for their actions relating to security. Users are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management responsible for PSD Information Technology system security incident handling.

5. User account passwords shall be protected by the individual User from use by, or disclosure to, any other individual or organization. All security violations shall be reported to the principal or assistant principal, who will then report the violation to the Network Administrator.

6. Upon termination of the relationship between PSD Information Technology and User, all security policies for PSD apply and remain in force surviving the terminated relationship.

7. Departments and schools that have district technology must provide adequate access controls in order to monitor PSD Information Technology systems to protect business data and associated programs from misuse. All PSD Technology access must be properly documented, authorized and controlled, following PSD standard processes.

10. Copyright and Digital Rights Management

Unless it is otherwise stated, Users should assume that all materials on the internet, including web sites and graphics, are copyrighted. No material may be disseminated through the District Internet system or posted on the District Internet site unless that material is original, in the public domain, used in accord with the fair use provisions of the copyright law, or is disseminated or posted with permission of the copyright owner; this includes music and video.

1. **Liability.** The District shall not be responsible or liable for unauthorized use or distribution of copyrighted materials and reserves the right to seek indemnification from the User for the inappropriate use, distribution or possession of copyrighted material on the District computers or network facilities.

2. **Obtaining Permission to Publish.** To republish text or graphics on the Internet, the Network Administrator or his/her designee for Internet approval must have written permission from the owner to use any copyright protected work. In addition, there must be a notice crediting the original producer and noting how and when written permission was granted, or printed evidence must be provided to document the material's public domain status.

3. **Software**. Staff and students may not copy software on any PSD computer and may not bring software from outside sources for use on PSD equipment without the prior approval of the Information Technology Department or its designee.

11. Incidental Use

As a convenience to the PSD User community, incidental use of PSD technology is permitted outside of instructional time. Incidental use is the use of technology for non-instructional purposes. This AUP still applies to *all* incidental use with the addition of the following terms:

1. Incidental use of District technology by Users does not extend to family members or other acquaintances.

2. Incidental use must not result in direct costs to PSD.

3. Incidental use must not interfere with the normal performance of an employee's work duties or student learning.

4. Incidental use may not involve large amounts of network or computer resources (E.g.- streaming audio or video, Internet-based games, downloading large files, etc.)

12. Use of Personal Technology on District Property

Each school site may set its own policies about whether and how personal technology devices (including, but not limited to: cell phones, smart phones, laptops, etc.) may be used on campus. However, when personal technology devices are used on school property or at school functions, their use is governed by this AUP. 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.

13. Acceptable Use Policy Supporting Information

1. PSD Information Technology Administrators reserve the right to remove any content (organizational or personal) on the Internet or intranet at any time, without cause or notice.

2. Schools and Departments responsible for the custody and operation of District technology shall be responsible for proper authorization and related technology utilization, the establishment of effective use, and reporting of performance to management.

3. All commercial software used on PSD Information Technology systems are copyrighted and designated for District use. Users must abide by all license agreements.

4. If a User damages equipment or alters software, said User may be expected to make restitution that will include financial reimbursement to the district.

14. Limitation of Liability

1. The District accepts no responsibility, or liability for access, or lack of access to computers, computer networks, or Internet services.

2. On any computer system, there is a potential for loss of data, interruption of services and inaccurate or unreliable information. The District makes no warranties for computer services or data, and is not liable for damage to, or loss of, work on District computers. The District will not be responsible for financial or other obligations arising from the use of District computers, computer networks, or the Internet.

3. The Internet opens a world of valuable information to students. However, some information on the Internet may be considered inappropriate for, or harmful to, young people. Parents and guardians are advised that the District has no control over information available on the Internet and is limited in its ability to control access to inappropriate information. Parent/guardians are encouraged to discuss their expectations for appropriate activities on the Internet with their children.

4. The District has installed filtering or blocking software that limits access to material that is obscene, pornographic, or harmful to minors however such software may not adequately protect students from accessing such material or other inappropriate materials.

5. In accordance with Board Policy 6163.4, “the student and his/her parent/guardian shall agree to not hold the district or any district staff responsible for the failure of any technology protection measures, violations of copyright restrictions, or users' mistakes or negligence. They shall also agree to indemnify and hold harmless the district and district personnel for any damages or costs incurred.”

15. Consequences for Violating these Policies

The use of District technology is a privilege, not a right. Violation of these policies may result one or more of the following for Student Users: loss of technology privileges; disciplinary action, including suspension or expulsion. Additionally, individuals are subject to loss of access privileges, civil, and criminal prosecution. The District will attempt to tailor any disciplinary action to the specific issues related to each violation.

16. Compliance / Regulation Contributed to by this Policy

1. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

2. Family Education Rights and Privacy Act 1974 (FERPA)

3. Copyright Act of 1976

4. Foreign Corrupt Practices Act of 1977

5. Computer Fraud and Abuse Act of 1986

6. Computer Security Act of 1987

7. Children’s Internet Protection Act of 2000 (CIPA)