SANTA ANA UNIFIED SCHOOL DISTRICT
Student Use of Technology Guidelines

This Student Use of Technology Guidelines provides a general overview the District's "Student Use of Technology" policy and administrative regulation 6163.4. It is not meant to take the place of reading the District's "Student Use of Technology" policy and administrative regulation 6163.4.

- A student's parents may be held financially responsible for any harm that may result from the student's intentional misuse of District or Personal Technology.
- Students may use District Technology only if their parents have signed a waiver of claims for damages against the District, which is included in the Student Technology Use Agreement.

Privacy

- Computer files and communications over District electronic networks are not private. The District reserves the right to monitor any use of District Technology, including on-line communications, for improper use and/or for regular maintenance of the District's systems.
- Students are informed that their parents have the right to request to see their student's computer files at any time.

Student Obligations and Responsibilities

The following provisions refer to District Technology; however, use of Personal Technology also may violate this regulation if the District reasonably believes the conduct or speech will cause actual, material disruption of school activities.

1. Students shall keep passwords, personal account numbers, home addresses and telephone numbers private. They shall use the system only under their own password or account number.
2. Students shall use District Technology responsibly for educational purposes. Commercial, political and/or personal use unrelated to an educational purpose is strictly prohibited**.**
3. Students shall not use District Technology to access, post, submit, publish or display "material that is harmful to minors," or matter that is threatening, obscene, lewd, vulgar, or disruptive.
4. Students shall not use District Technology to engage in discrimination, harassment, intimidation or bullying on the basis of actual or perceived disability, gender, gender identity, gender expression, nationality, race or ethnicity, religion, sexual orientation, or any other characteristic.
5. Students shall not use District Technology to engage in hate violence.
6. Students shall not use District Technology to engage in harassment, threats or intimidation.
7. Students shall not engage in cyberbullying using District Technology.
   Examples of cyberbullying might include:
   - **threats to harm another person;**
   - **oral or written assaults, such as teasing or name-calling;**
   - **social isolation or manipulation;**
   - **posting harassing messages, direct threats, social cruelty or other harmful texts, sounds or images on the Internet, including social networking sites;**
   - **posting or sharing false or defamatory information about another person;**
   - **posting or sharing information about another person that is private;**
   - **pretending to be another person on a social networking site or other electronic communication in order to damage that person's reputation or friendships;**
   - **posting or sharing photographs of other people without their permission;**
   - **spreading hurtful or demeaning materials created by another person (i.e., forwarding offensive e-mails or text messages); and**
   - **retaliating against someone for complaining that they have been bullied.**
8. Students shall not disclose, use or disseminate personal identification information about themselves or others when using District Technology. Students should not post or share photographs of other students without the other student's permission.

9. Students shall not use District Technology to encourage the use of drugs, alcohol or tobacco, nor shall they promote unethical practices or any activity prohibited by law or Board policy.
10. Copyrighted material shall be downloaded or shared only in accordance with applicable copyright laws. Any materials utilized for research projects should be given proper credit as with any other printed source of information.
11. Students shall not intentionally upload, download or create computer viruses and/or maliciously attempt to harm or destroy District Technology or manipulate the data of any other user, including so-called "hacking."
12. Students shall report any security problem or misuse of District or Personal Technology to the teacher or principal. If a student mistakenly accesses inappropriate information, the student must immediately report the matter to a teacher or school administrator.
13. Students shall not modify or attempt to repair District Technology without prior authorization.
14. Students shall not connect any personal device in the network, such as wireless access points, routers, hubs, etc.
15. Students shall not use web based proxies/anonymizers or software that attempts to make online activity on the Internet untraceable.
16. Students shall not download large files without permission of a teacher or administrator. Students shall not misuse District or school distribution lists or discussion groups by sending irrelevant messages.
17. Students may not send, share, view or possess pictures, text messages, e-mails or other material of an obscene nature in electronic or any other form on Personal Technology at school or school-related activities, or using District Technology.

Personal Mobile Devices

The use of personal mobile devices, such as laptops, cellular phones, tablets, pagers, or other electronic signaling devices, by students on campus is subject to all applicable School and District policies and regulations concerning technology and personal mobile device use.

- The District accepts no financial responsibility for damage, loss or theft. Devices should not be left unattended.
- All costs for data plans and fees associated with mobile devices are the responsibility of the student.
- The District does not require the use of personal mobile devices and does not rely on personal devices in its instructional program or extracurricular activities.
- Mobile devices with Internet access capabilities will access the Internet only through the school's filtered network while on school property.
- Use during class time must be authorized by the teacher.
- Photographs and audio or video recordings may be taken/made only with the express permission of all individuals being photographed or recorded. Recordings made in a classroom require the advance permission of the teacher and the school principal.
- Students may not take, possess or share obscene photographs or videos.
- Students may not photograph, videotape or otherwise record teacher-prepared materials, such as tests.
- The District will monitor all Internet or intranet access.
- If the District has reasonable cause to believe the student has violated the law or District policy, the device may be searched by authorized personnel and/or law enforcement may be contacted.

Consequences for Violation

- For purposes of disallowing access to District Technology, the principal or designee shall make all decisions regarding whether or not a student has violated Board policy or administrative regulation. The decision of the principal or designee shall be final.
- Inappropriate use shall result in a cancellation of the student's user privileges, disciplinary action and/or legal action in accordance with law and Board policy. Permission to bring personal mobile devices to school or school activities also may be revoked.