

ENCINITAS UNION SCHOOL DISTRICT

Responsible Use Policies – One-to-One Digital Learning

Student/Parent or Guardian Participation Agreement – E 6163.4(1)

Including Student Responsible Use Agreement for Using District-Owned Technology
Revised 7/2026

The Encinitas Union School District allows students to use technology, as defined in Board Policy 6163.4 — Student Use of Technology. The term “district technology” includes: district-issued devices, networks, apps, accounts, online services, learning platforms, cameras, microphones, keyboards, headphones, and cloud storage. The use of district technology is a privilege allowed by the district and is subject to the conditions and restrictions outlined in applicable board policies, administrative regulations, and this Agreement. The district reserves the right to stop access at any time, without notice, for any reason.

The district expects all students to use technology responsibly in order to avoid potential problems and liability. The district may place reasonable limits on the sites, material, and/or information that students may access through the system. The district makes no promise that the functions or services provided by or through the district will be without problems. In addition, the district is not responsible for financial obligations arising from unauthorized use or misuse of the system. Each student who is allowed to use district technology and the student’s parent/guardian shall use their electronic signature online for this Agreement, indicating that the student and guardian have read and understand the agreement—Board Policy 6163.4 — Student Use of Technology.

Student Obligations and Responsibilities

Students are expected to use district technology safely, responsibly, and for educational purposes only, in accordance with the accompanying board policy and applicable copyright laws. The student in whose name district technology is issued is responsible for its proper use at all times. Students shall not share their assigned online services account information, passwords, badges, QR codes, login cards, or other information used for identification and authorization purposes, and shall use the system only under the account to which they have been assigned. Students shall not get into the files or equipment of others without permission, access electronic resources by using another person’s name or electronic identification, or send anonymous electronic communications. Furthermore, students shall not attempt to access any data, documents, emails, or programs in the district’s system for which they do not have permission.

Students are prohibited from using district technology for improper purposes, including, but not limited to, use of district technology to:

1. Access, post, display, create, or otherwise use material that is discriminatory, libelous, defamatory, obscene, sexually explicit, or disruptive.
2. Bully, harass, scare, or threaten other students, staff, or other individuals, "cyberbullying."
3. Share private information or personally identifiable information with an open artificial intelligence "AI" system of themselves, another student, staff member, or other person.
4. Take, record, post, share, edit, or alter photos, videos, audio, screenshots, or recordings of another person without permission from a teacher or staff member.
5. Use artificial intelligence, editing tools, filters, or other technology to change, fake, impersonate, or misuse another person's image, voice, name, identity, schoolwork, or personal information.
6. Adjust the privacy settings on any technology tool or AI app unless directed to do so by a teacher or staff member.
7. Violate the direction of teachers or other staff members, age restrictions, or the intended use of the technology.
8. Copy or use someone else's work, images, music, videos, ideas, or other intellectual property without permission or proper credit.
9. Intentionally disrupt or harm district technology or other district operations, such as destroying district equipment, placing a virus on district computers, bypassing district filters, adding or removing a computer program without permission from a teacher or other district personnel, or changing settings on shared computers.
10. Install or create software/websites, apps, programs, or extensions that are not approved.
11. "Hack" into the system to change or misuse data of the district or other users.
12. Engage in or promote any practice that is unethical or violates any law or board policy, administrative regulation, or district practice.

Digital Literacy

Students are required to successfully complete the Encinitas Union School District's introduction to Digital Literacy and Well-being course. These courses are grade-level specific and are based on the learning requirements of the California Information Literacy Standards. The course includes monthly lessons that must be completed in all classrooms. Each grade level is provided with its own set of learning objectives appropriate to its grade level.

Privacy

Since the use of district technology is intended for educational purposes, students shall not have any expectation of privacy in any use of district technology.

The district reserves the right to monitor and record all use of district technology, including but not limited to access to the Internet or social media, Internet searches, browsing history, use of AI, communications sent or received from district technology, or other uses. Such monitoring/recording may occur at any time without prior notice for any legal purposes, including, but not limited to, record keeping and/or investigation of improper, illegal, or prohibited

activity. Students should be aware that, in most instances, their use of district technology, such as web searches and emails, cannot be erased or deleted. All passwords created for or used on any district technology are the sole property of the district.

Personally Owned Devices

If a student uses a personally owned device to access district technology at home, the student shall follow all applicable board policies, administrative regulations, and this Agreement. 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.

Reporting

If a student becomes aware of any security problems or inappropriate use, including, but not limited to, phishing, suspicious links, QR codes, pop-ups, fake login pages, scams, malware, unauthorized extensions, VPNs/proxies, and attempts to bypass filters, the student shall immediately report such information to the teacher or other district personnel.

Theft or Loss

If the device is lost or stolen on school property, report it immediately to the teacher and the school site principal. For theft or loss off campus, the device should also be reported to the local police department. A copy of the police report must be sent to the district within 48 hours of the discovery of the loss. Parents may be invoiced for any iPad that is not returned to the district.

Consequences for Violation

Violations of the law, board policy, or this Agreement may result in the loss of a student's access to district technology and/or discipline, up to and including suspension or expulsion. In addition, violations of the law, board policy, or this Agreement may be reported to law enforcement agencies as appropriate.

Board Policy #6163.4

<https://simbli.eboardsolutions.com/Policy/ViewPolicy.aspx?S=36030724&revid=dLI3TarjY2aesls h1KRQU251A==&st=technology&mt=Exact>