

Exhibit (1) 6163.4 Student Use of Technology

Status: NEW

Original Adopted Date: 06/25/2025

Last Revised Date: 06/25/2025

**ACCEPTABLE USE AGREEMENT AND RELEASE OF DISTRICT FROM LIABILITY
(STUDENTS)**

The Natomas Unified School District authorizes students to use technology, as defined in Board Policy 6163.4 - Student Use of Technology. This Board Policy, 6163.4 Student Use of Technology, aims to create a safe, productive, and respectful digital space while ensuring that students understand their responsibilities when using school technology resources. 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 Agreement. Students are responsible for the ethical use of technology, including computers, networks, and the internet. The district reserves the right to suspend 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 restrictions on the sites, material, and/or information that students may access through the system.

The district makes no guarantee that the functions or services provided by or through the district will be without defect. In addition, the district is not responsible for financial obligations arising from unauthorized use, or misuse, of the system.

Each student who is authorized to use district technology and the student's parent/guardian shall sign this Agreement, which indicates that the student has read and understands the Agreement and 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, and 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 must take care of the school-provided devices, including chargers and accessories. Students shall not share their assigned online services account information, passwords, 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 gain unauthorized access to the files or equipment of others, 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 authorization.

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, intimidate, or threaten other students, staff, or other individuals ("cyberbullying")
3. Disclose, use, or disseminate personal identification information (such as name, address, email, telephone number, Social Security number, or other personal information) of another student, staff member, or other person with the intent to threaten, intimidate, harass, or ridicule that person
4. Share confidential information or personally identifiable information with an open artificial intelligence (AI) system of themselves, another student, staff member, or other person
5. Adjust the privacy settings on any technology tool or AI app unless directed to do so by a teacher or staff member
6. Violate the direction of teachers or other staff members, age restrictions, or the intended use of the technology
7. Infringe on copyright, license, trademark, patent, or other intellectual property rights
8. Intentionally disrupt or harm district technology or other district operations (such as destroying district equipment, placing a virus on district computers, adding or removing a computer program without permission from a teacher or other district personnel, changing settings on shared computers)
9. Install unauthorized software
10. "Hack" into the system to manipulate data of the district or other users

11. Engage in or promote any practice that is unethical or violates any law or board policy, administrative regulation, or district practice

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 retention and distribution 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. The creation or use of a password by a student on district technology does not create a reasonable expectation of privacy.

Personally Owned Devices

If a student uses a personally owned device to access district technology, the student shall abide by 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 problem (including, but not limited to, a cyberattack, phishing, or any compromise of the confidentiality of any login or account information), or misuse of district technology, the student shall immediately report such information to the teacher or other district personnel.

Consequences for Violation

Violations of the law, board policy, or this Agreement may result in revocation 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. Damage or lost devices will result in financial consequences in alignment with BP/AR 3260.

Student Acknowledgment

I have received, read, understand, and agree to abide by this Agreement and other applicable laws and district policies and regulations governing the use of district technology. I understand that there is no expectation of privacy when using district technology. I further understand that any violation may result in loss of user privileges, disciplinary action, and/or appropriate legal action.

Name: _____ Grade: _____
(Please print)
School: _____
Signature: _____ Date: _____

Parent or Legal Guardian Acknowledgment

If the student is under 18 years of age, a parent/guardian must also read and sign the Agreement.

As the parent/guardian of the above-named student, I have read, understand, and agree that my child shall comply with the terms of the Agreement. By signing this Agreement, I give permission for my child to use district technology and/or to access the school's computer network and the Internet. I understand that, despite the district's best efforts, it is impossible for the school to restrict access to all offensive and controversial materials. I agree to release from liability, indemnify, and hold harmless the school, district, district personnel and the Board against all claims, damages, and costs that may result from my child's use of district technology or the failure of any technology protection measures used by the district. Further, I accept full responsibility for supervision of my child's use of my child's access account if and when such access is not in the school setting.

Name: _____ Date: _____
(Please print)
Signature: _____

06/25/2025

Policy Reference Disclaimer:

These references are not intended to be part of the policy itself, nor do they indicate the basis or authority for the board to enact this policy. Instead, they are provided as additional resources for those interested in the subject matter of the policy.

State

Civ. Code 3120-3123
Ed. Code 49073.6
Ed. Code 51006
Ed. Code 51007
Ed. Code 60044
Pen. Code 313
Pen. Code 502
Pen. Code 632
Pen. Code 653.2

Federal

15 USC 6501-6506
16 CFR 312.1-312.12
20 USC 7101-7122
20 USC 7131
47 CFR 54.520
47 USC 254

Management Resources

California Department of Education Publication
Court Decision
CSBA Publication
Federal Trade Commission Publication
U.S. Department of Education Publication
USDOE Office of Educational Technology Publication

Website
Website
Website
Website
Website
Website
Website
Website
Website
Website

Description

Digital equity bill of rights
Student records; social media
Computer education and resources
Programs to strengthen technological skills
Prohibited instructional materials
Harmful matter
Computer crimes; remedies
Eavesdropping on or recording confidential communications
Electronic communication devices; threats to safety

Description

Children's Online Privacy Protection Act
Children's Online Privacy Protection Act
Student Support and Academic Enrichment Grants
Internet Safety
Internet safety policy and technology protection measures; E-rate discounts
Universal service discounts (E-rate)

Description

Artificial Intelligence: Learning With AI Learning About AI
New Jersey v. T.L.O. (1985) 469 U.S. 325
Cyberbullying: Policy Considerations for Boards, Policy Brief, July 2007
How to Protect Kids' Privacy Online: A Guide for Teachers, December 2000
2024 National Education Technology Plan
Artificial Intelligence and the Future of Teaching and Learning: Insights and Recommendations, May 2023
California Governor's Office of Emergency Services
CSBA District and County Office of Education Legal Services
California Coalition for Children's Internet Safety
Center for Safe and Responsible Internet Use
Federal Trade Commission, Children's Online Privacy Protection
American Library Association
Federal Communications Commission
California Department of Education
U.S. Department of Education
CSBA

Cross References**Code**

0440
0440
1113
1113
1113
1114
1114
3260
3260
3512
3512
4040
4040
4131
5125
5125
5125.2
5131
5131.2
5131.2
5131.8
5131.9
5144
5144
5144.1

Description

District Technology Plan
District Technology Plan
District And School Websites
District And School Websites
District And School Websites
District-Sponsored Social Media
District-Sponsored Social Media
Fees And Charges
Fees And Charges
Equipment
Equipment
Employee Use Of Technology
Employee Use Of Technology
Staff Development
Student Records
Student Records
Withholding Grades, Diploma Or Transcripts
Conduct
Bullying
Bullying
Mobile Communication Devices
Academic Honesty
Discipline
Discipline
Suspension And Expulsion/Due Process

5144.1	Suspension And Expulsion/Due Process
5144.2	Suspension And Expulsion/Due Process (Students With Disabilities)
5145.12	Search And Seizure
5145.12	Search And Seizure
5145.3	Nondiscrimination/Harassment
5145.3	Nondiscrimination/Harassment
5145.7	Sex Discrimination and Sex-Based Harassment
5145.7	Sex Discrimination and Sex-Based Harassment
5145.9	Hate-Motivated Behavior
5148.2	Before/After School Programs
5148.2	Before/After School Programs
6142.8	Comprehensive Health Education
6142.8	Comprehensive Health Education
6154	Homework/Makeup Work
6162.5	Student Assessment
6162.6	Use Of Copyrighted Materials
6162.6	Use Of Copyrighted Materials
6162.8	Research
6162.8	Research
6163.1	Library Media Centers