

District Policy Manual Natomas Unified School District

Policy 6163.4 Student Use of Technology

Status: ADOPTED

Original Adopted Date: 06/1995

Last Revised Date: 06/25/2025

The Governing Board believes that effective use of technology is integral to the education and development of students. In order to promote digital citizenship, the Board recognizes that students must have access to the latest digital tools and receive instruction that allows students to positively engage with technology in ways that respect human rights and avoids Internet dangers. Technological resources provided to students, including technology based on artificial intelligence (AI), shall be aligned to district goals, objectives, and academic standards. The use of technology shall augment the use of Board adopted instructional materials.

The Board intends that technological resources provided by the district be used in a safe and responsible manner in support of the instructional program and for the advancement of student learning. Students shall be allowed to use such technology, including AI technology, in accordance with district policies, including, but not limited to, policies on academic honesty, data privacy, nondiscrimination, and copyright protections. All students using these resources shall receive instruction in the proper and appropriate use of technology. Such instruction shall incorporate students' responsibilities regarding academic honesty, honoring copyright provisions, assessing the reliability and accuracy of information, protecting personal data, and the potential for biases and errors in artificially generated content.

District technology includes, but is not limited to, computer hardware, software, or software as a service provided or paid for by the district, whether accessed on or off site or through district-owned or personally owned equipment or devices, including tablets and laptops; computer servers, wireless access points (routers), and wireless computer networking technology (wi-fi); the Internet; email; applications (apps), including AI apps; telephones, cellular telephones, smartphones, smart devices, and wearable technology; or any wireless communication device, including radios.

Teachers, administrators, and/or library media specialists are expected to review the technological resources and online sites that will be used in the classroom or assigned to students in order to ensure that they are appropriate for the intended purpose and the age of the students.

The Superintendent or designee shall notify students and parents/guardians about authorized uses of district technology, user obligations and responsibilities, and

consequences for unauthorized use and/or unlawful activities in accordance with this board policy and the district's Acceptable Use Agreement.

Before a student is authorized to use district technology, the student and the student's parent/guardian shall sign and return the Acceptable Use Agreement. In that agreement, the student and parent/guardian shall agree not to hold the district or any district staff responsible for the failure of any technology protection measures or user mistakes or negligence and shall agree to indemnify and hold harmless the district and district staff for any damages or costs incurred.

The district reserves the right to monitor student use of technology within the jurisdiction of the district without advance notice or consent. Students shall be informed that the use of district technology, as defined above, is not private and may be accessed by the district for the purpose of ensuring proper use. Students have no reasonable expectation of privacy in the use of district technology. Students' personally owned devices shall not be searched except in cases where there is a reasonable suspicion, based on specific and objective facts, that the search will uncover evidence of a violation of law, district policy, or school rules.

The Superintendent or designee may gather and maintain information pertaining directly to school safety or student safety from the social media activity of any district student in accordance with Education Code 49073.6 and Board Policy/Administrative Regulation 5125 - Student Records.

Whenever a student is found to have violated board policy or the district's Acceptable Use Agreement, the principal or designee may cancel or limit a student's user privileges or increase supervision of the student's use of the district's equipment and other technological resources, as appropriate. Inappropriate use also may result in disciplinary action and/or legal action in accordance with law and board policy.

The Superintendent or designee, with input from students and appropriate staff, shall regularly review and update procedures to enhance the safety and security of students using district technology and to help ensure that the district adapts to changing technologies and circumstances.

Internet Safety

The Superintendent or designee shall ensure that all district computers with Internet access have a technology protection measure that protects against access to visual depictions that are obscene, child pornography, or harmful to minors and that the operation of such measures is enforced. (20 USC 7131; 47 USC 254; 47 CFR 54.520)

To reinforce these measures, the Superintendent or designee shall implement rules and procedures designed to restrict students' access to harmful or inappropriate matter on

the Internet and to ensure that students do not engage in unauthorized or unlawful online activities.

Harmful matter includes matter, taken as a whole, which to the average person, applying contemporary statewide standards, appeals to the prurient interest and is matter which depicts or describes, in a patently offensive way, sexual conduct and which lacks serious literary, artistic, political, or scientific value for minors. (Penal Code 313)

The district's Acceptable Use Agreement shall establish expectations for appropriate student conduct when using the Internet or other forms of electronic communication, including, but not limited to, prohibitions against:

1. Accessing, posting, submitting, publishing, or displaying harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit, 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
2. Intentionally uploading, downloading, or creating computer viruses and/or maliciously attempting to harm or destroy district equipment or materials or manipulate the data of any other user, including so-called "hacking"
3. Distributing personal identification information, including the name, address, telephone number, Social Security number, or other personally identifiable information, of another student, staff member, or other person with the intent to threaten, intimidate, harass, or ridicule that person

The Superintendent or designee shall regularly review current guidance regarding cybersecurity, data privacy, and digital media awareness and incorporate recommended practices into the district's processes and procedures related to the protection of the district's network infrastructure, the monitoring and response to cyberattacks, ensuring data privacy, and monitoring suspicious and/or threatening digital media content, in accordance with Board Policy 5125 - Student Records.

The Superintendent or designee shall provide age-appropriate instruction regarding safe and appropriate behavior on social networking sites, chat rooms, and other Internet services. Such instruction shall include, but not be limited to, the dangers of posting one's own personal identification information online, misrepresentation by online predators, how to report inappropriate or offensive content or threats, behaviors that constitute cyberbullying, and how to respond when subjected to cyberbullying.

06/1995
11/12/1997
8/12/1998
7/2001

11/2005
10/18/2006
07/2007
12/12/2007
06/2012
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

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

5125	Student Records
5125.2	Withholding Grades, Diploma Or Transcripts
5131	Conduct
5131.2	Bullying
5131.2	Bullying
5131.8	Mobile Communication Devices
5131.9	Academic Honesty
5144	Discipline
5144	Discipline
5144.1	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