Agenda of Regular Board Meeting

The Board of Directors
North Sanpete School District

A Regular Board Meeting of the Board of Directors of North Sanpete School District will be held June 16, 2026, beginning at 6:30 PM in the North Sanpete School District Office: Board Room, 220 East 700 South, Mt. Pleasant, UT 84647.

1. BUSINESS ITEMS
   A. Prayer
   B. Pledge of Allegiance
   C. Board Recognition and Board Reports
2. BOARD PRESENTATIONS
   A. Education Support Personnel of the Year
      District Office: Angela Thompson
   B. School Report
      Principal Straatman will present the school report for North Sanpete High School. Ben Cox will present on high school counseling progress.
3. CONSENT CALENDAR
   A. Approval of Minutes
      Minutes for the May 19, 2026 board meeting will be presented to the board for approval.
   B. Financial Report and Payment Request
   C. Adoption of Agenda
4. BOARD VISION / GOALS
5. PERSONNEL SERVICES
   A. Resignations
      Letter of Resignation from A. Sosa will be presented to the board.
   B. Substitute, Certificated and Classified Positions
6. SUPPORT SERVICES
   A. Construction Projects
   B. Capital Projects
7. STUDENT SERVICES
   A. School Choice
      School choice requests for the 2026-2027 school year will be presented to the board for approval.
   B. NSMS 2026-2027 Handbook
      The NSMS 2026-2027 Handbook will be presented to the board for approval.
8. TRAVEL REQUESTS

- NSH Journalism is requesting out-of-state travel to attend the National Journalism Conference in Orlando, Florida, November 18-22, 2026.
- Boys Football is requesting overnight travel to attend the USU Eastern Football Camp in Price, Utah, July 13-16, 2026.

9. POLICIES
   A. D-66 Employee Technology Acceptable Use Policy
      The D-66 Employee Technology Acceptable Use Policy will be presented to the board in second read.
   B. E-30 Student Technology Acceptable Use Policy
      The E-30 Student Technology Acceptable Use Policy will be presented to the board in second read.
   C. G-39 Content Filtering and Online Access Policy
      The G-39 Content Filtering and Online Access Policy will be presented to the board in first read.
   D. G-35 Mobile Computing and Storage Devices Policy
      The G-35 Mobile Computing and Storage Devices Policy will be presented to the board in first read.
10. CURRICULUM & INSTRUCTION
11. DISCUSSION / INFORMATION ITEMS
   A. Alumni Discussion
   B. 2026-2027 Board Meeting Schedule
      The 2026-2027 Board Meeting Schedule will be presented to the board.
12. MATTERS FROM THE BOARD
13. EXECUTIVE SESSION
   A. Executive Session
      Possible closed session to discuss the character, professional competence, or physical or mental health of an individual and pending or reasonably imminent litigation pursuant to Utah Code § 52-4-205.
14. ADJOURN
   Adjourn

Notice of Special Accommodations (ADA)

In compliance with the Americans with Disabilities Act, individuals needing special accommodations (including ancillary communication aids and services) during this meeting should notify: O'Dee Hansen, Assistant Superintendent, North Sanpete School District Office, 220 E. 700. S Mt. Pleasant, UT 84647; 435-462-2485

Notice of Electronic or Telephone Participation

One or more members of the North Sanpete School District may participate electronically or telephonically pursuant to UCA 52-4-7.8

Book Policy Manual

Section D - Personnel

Title Employee ~~and Student Technology~~ Acceptable Use of District Technology Resources

Code ~~E-30,~~ D-66

Adopted July 17, 2001

Last Revised June 16, 2026; May 18, 2021

~~INTRODUCTION~~PURPOSE

~~Technology use is a valuable and necessary component of student learning, employee work and school/District communication. The District encourages employees and students to use district technology resources and/or services for educational purposes. Students and District employees shall use the District-issued technology resources and/or services primarily to support student learning and instruction and for communication among employees and between employees and parents. Incidental employee and student use of District-issued technology resources and/or services must not interfere with the education of students and shall always be consistent with the District Internet Acceptable Use Policy.~~

~~The information maintained on District technology devices or accounts, resources, and/or services is the District's property. Students and employees do not have an expectation of privacy in their communications through District technology devices or accounts. The District reserves the right to monitor the information contained on District computers or accounts. Any use inconsistent with educational purposes shall be grounds for terminating the account, confiscating the information saved in the account, employee discipline, student discipline and/or limiting the employee s or student s use of District computer equipment, resources, and/or services.~~District technology resources are provided to employees to support educational instruction, District operations, communication, administration, professional responsibilities, and other authorized District activities. The Board of Education recognizes that technology use is an essential component of educational and operational effectiveness and expects employees to use District technology resources in a lawful, responsible, ethical, secure, and educationally appropriate manner.

Employees are responsible for using District technology resources in compliance with this policy, applicable law, District procedures, cybersecurity requirements, and professional

standards of conduct.

For purposes of this policy, District technology resources include, but are not limited to, District-owned or District-authorized:

- Computers,
- Mobile devices,
- Networks,
- Internet Services,
- Cloud-based Systems,
- Telecommunications Systems,
- Software,
- Digital Applications,
- Electronic Communication Systems,
- Data Systems,
- Employee Accounts,
- Other Electronic Resources or Services.

Incidental personal use is permitted only when such use:

1. Does not interfere with employee responsibilities or District operations;

2. Does not consume excessive District resources;

3. Complies with District policy and applicable law; and

4. Does not compromise District security or confidentiality obligations.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

OWNERSHIP AND EXPECTATION OF PRIVACY

All data created, transmitted, received, stored, or accessed using District technology resources is District property to the extent permitted by law. Employees shall have no expectation of privacy regarding information created, transmitted, received, stored, or accessed using District-owned systems, networks, devices, accounts, or technology resources, except as otherwise protected by applicable law. The District reserves the right to access, monitor, review, retrieve, preserve, disclose, or delete information maintained on District technology resources for legitimate educational, operations, legal, investigative, cybersecurity, records retention, safety, or compliance purposes.

District monitoring and access shall be conducted consistent with:

- Applicable federal and state law,
- Employee due process protections,
- Student privacy protections,
- Records Retention Requirements.

Employees are responsible for safeguarding District devices and systems from unauthorized access or misuse and shall immediately report any known or suspected unauthorized access, data breach, cybersecurity incident, or loss of District technology resources.

Citations

- Utah Code § 53E-9-301 through 53E-9-309
- FERPA, 34 CFR Part 99
- Utah Code § 63G-2-101 et seq.

~~SYSTEM FILTER~~INTERNET SAFETY, FILTERING, AND CYBERSECURITY

~~The District utilizes internet filtering systems to assist in restricting access to internet sites containing material that is obscene, pornographic, or harmful to minors. Even though the District takes reasonable efforts to block this material, no filtering systems or technology will filter out all such material. It is the responsibility of the end user to maintain a high level of integrity to protect themselves and others from such inappropriate material. Parents and students are advised that some materials accessible via the internet may be inappropriate. As used herein, references to the terms obscene, obscenity, pornographic, pornography, child pornography, and harmful to minors are defined by applicable state and federal laws, regulations, and causes.~~

~~All users, including District employees, students, administrators and educational organizations that have access to District-owned technology resources, and/or services and District-authorized Internet access are subject to this policy and are expected to be familiar with the provisions. This policy may be supplemented by more specific policies, administrative procedures, directives, and rules governing the day-to-day management and operation of District technology resources and services.~~

~~PROVISIONS/REQUIREMENTS~~

~~1. **Privilege**~~

~~a. The use of Internet and computer equipment is a privilege, not a right. Inappropriate use, including any violation of these conditions and rules, may result in cancellation of the privilege. The North Sanpete School and District Administration has the authority to determine appropriate use and the power to deny, revoke, suspend or close any user account at any time based upon its determination of inappropriate use by account holders or users.~~

~~b. The materials and products derived and/or produced from District technology resources and services and/or District technology device use are District property.~~

~~c. Students in grades 7-12 may obtain an approved school e-mail account. Outside e-mail accounts such as Hotmail are not permitted or accessible using school technology devices.~~

Formatted: Font: Not Bold

Formatted: Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

d. Communications on District-issued devices or through District Internet access are accessible to school employees and parents where those communications are maintained as part of a student's education record, in accordance with the Family Education Rights and Privacy Act (FERPA), 34 CFR § 99.

2. **Acceptable Use Agreements and Training**

a. All users shall access Internet and District-issued computer equipment and technology devices consistent with Federal and State law and the purposes, goals, and policies of the District.

b. The Acceptable Use Agreement must be signed by District employees (both licensed and unlicensed) prior to the first day of work in the District and annually thereafter.

c. The Acceptable Use Agreement must be signed by students and parent(s) upon enrollment in the District and annually in the first month of the school year thereafter. Following initial enrollment all students shall receive training at the beginning of each school year on internet safety, on this Policy and Policy VII - 35 "Mobile Computing and Storage Devices"

d. The District will provide students and employees with annual training on acceptable Internet use and the appropriate use of District-issued technology devices. The District will collaborate with District school community councils to provide education and awareness of safe technology utilization and digital citizenship for students and school personnel. The District may create subcommittees of community council and District staff members and/or partner with a non-profit entity to develop and provide this training.

e. Internet access shall be filtered and logged consistent with State Law.

3. **Unacceptable Internet and District-issued Technology Use** - The following are examples of unacceptable Internet and technology device uses. This list is not inclusive. A District network or technology device user must not intentionally:

a. Seek and/or acquire unauthorized access to computer of telecommunications networks.

b. Intercept communications intended for other persons.

c. Interfere with the operations of technology resources, and/or services including placing a computer virus on any computer system.

d. Create, store, send, or access or attempt to create, store, send or access sexually explicit, obscene, potentially damaging, dangerous, disruptive, or otherwise inappropriate materials, false or defamatory information or materials and personal or

generalized attacks or harassment against individuals or groups of individuals.

e. Create, store, send, or access or attempt to create, store, send or access materials that offensively address age, race, ethnicity, gender, sexual orientation, religious or political beliefs, national origin, or disabilities of a person or a group of people.

f. Log in through another person s account or attempt to access another user s password or files.

g. Further any illegal act, including infringing on any intellectual property rights.

h. Download, upload, or distribute any files, software, or other material that is not specifically related to an educational project or is otherwise authorized by an appropriate school official.

i. Download, upload, or distribute any files, software, or other material in violation of copyright laws.

j. Plagiarize.

k. Access, transmit or retransmit materials which promotes violence or advocates destruction of property including, but not limited to, access to information concerning the manufacture of destructive devices such as explosives, fireworks, smoke bombs, incendiary devices or the like.

l. View, use or send materials or information that violate state or federal law including pornographic or inappropriate images or language, materials that encourage others to violate the law, confidential information or copyrighted materials.

m. Sell or purchase illegal items or substances.

n. Obtain and/or use anonymous email sites or spam.

o. Commit or attempt to commit any willful act involving the use of the network which disrupts the operation of the network within the school district, or any network connected to the Internet including the use or attempted use or possession of computer viruses.

p. Post personal contact information without express parental permission or about students or adults.

q. Delete, copy, modify or forge other users' names, emails, files, or data; disguise one's identity, impersonate other users, or send anonymous email, unless authorized by a school official.

r. Damage computer equipment or technology devices, files, data or the District network in any way.

s. Use any District technology device or personal device on school property to pursue hacking, internal or external to the District, or attempt to access information protected by state or federal laws.

t. Interfere with other users' ability to access their account(s).

u. Disclose private password(s) to others.

v. Use the District network or Internet for commercial purposes.

w. Use the District network or Internet for personal financial gain, personal advertising, or personal promotion.

x. Engage in non-school related fundraising or activities such as Solicitation for religious, personal or political purposes.

y. Otherwise violate student code of conduct or any other policy through the use of the District network and/or District-issued accounts.

4. **Monitoring System**

a. The District monitors District computers or accounts internally or may contract with a monitoring service provider to monitor the information contained on District computers or accounts, including communications from and to students and employees.

b. All such contracts will be entered into in accordance with the Utah Student Data and Privacy Protection Act, Utah Code, Title 53E, Chapter 9, Part 3 and FERPA.

c. The purpose of any monitoring system is to ensure compliance with this and other District policies, and state and federal law.

d. An alternate purpose of a monitoring system is to assure appropriate supports are in place for students whose communication contain information that could lead a reasonable person to believe the student is at risk of harm to themselves of or others.

e. The use of a monitoring system does not impose an obligation on the District to monitor students' and employees' communications and information contained on District computers or accounts twenty-four hours a day, seven days a week, and students, employees, and parents should be aware that information reasonably suggesting a student is at risk of harm to self or others may not be received and addressed immediately.

f. To the extent that a monitoring system in use by the District provides notifications of communications containing information that a student or employee may be at risk of harm to self or others, when a District employee receives and reviews such notification after hours, a District employee will notify parents or law enforcement of the communication.

g. The District will NOT do home visits after hours.

The above prohibitions are examples only; the District reserves the right:

- To take immediate action regarding activities that use District-issued devices or Internet that create security and/or safety concerns for the District, District students, District employees, District schools or property or District network or technology resources and/or services.

- To prohibit or terminate online activities that expend District resources that the District determines lack legitimate educational content or purpose.

The District shall maintain technology protection measures, internet filtering systems, cybersecurity safeguards, monitoring systems, and security controls consistent with applicable laws and industry standards. District technology systems shall be configured to:

- Restrict access to unlawful, harmful, obscene, malicious, or inappropriate content;
- Protect confidential and student information;
- Reduce cybersecurity risks;
- Monitor system integrity and network security; and
- Support safe and secure educational operations.

Employees shall not intentionally disable, bypass, interfere with, or attempt to circumvent District filtering systems, cybersecurity safeguards, endpoint protections, authentication controls, monitoring systems, or security procedures. Employees shall comply with all District cybersecurity protocols, password requirements, multifactor authentication requirements, device management standards, and security procedures established by the District.

Citations

- 47 USC § 254(h) CIPA
- Utah Code § 53E-9-306
- Utah Code § 53E-9-309

Formatted: Font: Not Bold

Formatted: Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

STAFF AND STUDENTEMPLOYEE RESPONSIBILITIES

1. **General User Responsibilities**

a. It is the responsibility of any user of District electronic resources to read, understand, and follow this policy. Users are expected to exercise reasonable judgment in interpreting the policy and examples in making decisions about the appropriate use of

District electronic resources. Any person with questions regarding the application or meaning of the information in this policy should seek clarification from a District administrator. Use of District electronic resources constitutes acceptance of the terms of this policy and Acceptable Use Agreement.

b. Users shall not exceed the District- or supervisor-authorized access to the District network or other computer equipment, system performance, or data.

2. **Administrator Responsibilities**

a. An administrator is responsible for assuring that educators and students in the District under his control and supervision understand and abide by the Acceptable Use Agreement and Policy as stated in this document. If a District administrator has reason to believe that a user (educator or student) is misusing the system or violating any provision of this Agreement, the administrator may report the misuse to District Technology Department.

b. It is also the responsibility of the administrator to report any misuse of the system immediately to the District and law enforcement, if required by law.

c. Administrators will also immediately report to the District, parents, and law enforcement any information that leads the administrators to reasonably believe a student or employee is at risk of harming themselves or others.

d. Administrators are not responsible for monitoring information contained on District computers or accounts or communications from and to students and employees when the administrator is off contract hours.

e. If an administrator does receive and review after hours information that suggest a student or employee in the administrator s building is at risk of harm to self or others, the administrator shall contact the student s parents or law enforcement or both but will not conduct further investigation into the communication received after hours.

3. **Educator/Employee Responsibilities**

a. Educators/Employees who supervise students with access to District-owned technology resources and/or services shall be familiar with the District Acceptable Use Agreement and enforce its provisions.

b. It is the responsibility of District educators/employees to teach students with whom they work about safe and responsible use of the Internet and District owned technology.

c. Educators/Employees are responsible for monitoring students' use of electronic resources, and to intervene promptly if students are using them inappropriately.

d. Educators/Employees must assure that students read and act consistent with the District Acceptable Use Agreement and policy. If an educator/employee has reason to believe that a student is misusing the system, the educator/employee must report this activity to his/her direct administrator. Access and/or review of information or records by an educator or employee must take place consistent with District policy.

e. It is also the responsibility of the educator/employee to report any misuse of the system to the appropriate District administrator and/or to law enforcement, if required by law.

f. Educators/Employees are responsible for the security of their District-issued and personal electronic devices and equipment, files and passwords. Educators/Employees shall promptly notify the District of security problems. Educators/Employees with access to student records may not use, release, or share student records except as expressly authorized by federal and State law and District policy.

g. Educators/Employees have no expectation of privacy in files, disks, documents, etc. which were created in, entered in, stored in, downloaded from, or used on District equipment, technology, resources and/or services.

4. **Student Responsibilities**

a. Students have a personal and individual responsibility to learn about safe and responsible use of the Internet and District-issued devices.

b. Students are responsible to use District resources appropriately and consistent with this Agreement and District policy.

c. If a student misuses resources, the District may discontinue the student s use of the District network, the Internet and/or District-issued devices.

d. The District may also take disciplinary action against the student, as appropriate and consistent with District policy.

e. Parents and students are advised that some materials accessible via the Internet may contain items that are illegal, defamatory, inaccurate, or potentially offensive to some people. The District cannot guarantee that filtering software will, in all instances, successfully block access to all inappropriate materials.

f. Students have no expectation of privacy while using the District network, technology, resources and/or services.

g. The District has the right to monitor users' online activities if they are using District-provided Internet and/or District-issued or owned devices and may do so through a contracted monitoring service provider. The District may access, review, copy, and store or delete any electronic communication or files and disclose them to school

officials and law enforcement, if required by law.

h. Any stored copy of electronic communications or files become part of the student s education record and is subject to the provisions of FERPA.

DISTRICT NETIQUETTE

1. All users are expected to abide by generally accepted rules of network etiquette. These include, but are not limited to the following:

a. both staff and students must be polite, use appropriate language, and avoid abusive messages;

b. both staff and students must not engage in activities, which are prohibited under school/District Policy or State and Federal Law.

2. Messages relating to or in support of illegal activities may be reported to the authorities and could result in the immediate and permanent loss of user privileges and/or report to law enforcement.

3. Users should not reveal personal information.

4. Users must not use the network in such a way that they could disrupt the use of the network by other users.

5. Users should assume all communications and information accessible via the network to be public records or property.

Employees shall use District technology resources in a professional, lawful, ethical, secure, and educationally appropriate manner. Employees shall:

1. comply with District technology procedures, cybersecurity standards, and applicable law;
2. protect passwords, authentication credentials, and account access information;
3. use only District-approved software applications, digital tools, and technology services for District business;
4. protect confidential, protected, and student information from unauthorized disclosure;
5. comply with copyright, licensing, and intellectual property laws;
6. maintain professional standards in electronic communications;
7. comply with records retention and public records obligations;

8. protect District devices and systems from theft, damage, unauthorized access, malware exposure, or misuse;

9. immediately report suspected cybersecurity incidents, phishing attempts, unauthorized disclosures, or system vulnerabilities to appropriate District personnel;

10. complete all required acceptable use, cybersecurity, and student data privacy training.

Employees shall not share passwords or permit unauthorized individuals to access District systems using the employee's credentials.

SUPERVISION OF STUDENT TECHNOLOGY USE

Employees who supervise, instruct, authorize, or facilitate student access to District technology resources shall provide reasonable supervision of student technology use consistent with the employee's assigned duties and the age and maturity of students. Employees shall:

1. monitor student use of District technology resources during instructional activities to the extent reasonably practicable;

2. enforce District technology, internet safety, student conduct, and student data privacy policies;

3. use only District-approved applications, instructional technology platforms, and digital services for student activities involving student data;

4. restrict student access to unauthorized applications, websites, or online services when reasonably able to do so;

5. report suspected misuse, inappropriate content access, cybersecurity concerns, or student data privacy concerns to appropriate District personnel.

Employees shall not knowingly permit students to use District technology resources in violation of District policy, student safety requirements, or applicable law.

Citations

Formatted: Font: Not Bold

- 47 U.S.C. § 254(h)
- Utah Code § 53E-9-306
- Utah Code § 53E-9-309

ACCEPTABLE USE AGREEMENT AND TRAINING

Each employee shall sign an Acceptable Use Agreement before receiving access to District technology resources and annually thereafter as required by the District. The District shall provide employees with periodic training regarding:

- acceptable technology use,
- cybersecurity practices,
- internet safety,
- student data privacy,
- records retention obligations,
- and appropriate use of electronic communications.

The District shall maintain documentation of employee acknowledgment and completion of required training. Failure to complete required training or acknowledgment requirements may result in suspension or limitation of access to District technology resources.

Citations

Formatted: Font: Not Bold

- Utah Code § 53E-9-309
- Utah Admin. Rules R277-487

PROHIBITED USES

Employees shall not use District technology resources to:

1. access, create, transmit, store, or distribute unlawful, obscene, sexually explicit, threatening, discriminatory, defamatory, harassing, abusive, fraudulent, or disruptive material;

2. engage in cyberbullying, harassment, intimidation, retaliation, or abusive conduct;

3. access systems, accounts, or data without authorization;

4. attempt to bypass security controls or monitoring systems;

5. introduce malware, ransomware, malicious code, unauthorized software, or other cybersecurity threats;

6. engage in political campaigning or prohibited political activity using District resources;

7. conduct unauthorized commercial activity or personal business unrelated to District operations;

8. improperly disclose confidential, protected, or student information;

9. use District technology resources for personal financial gain;

10. impersonate another user or falsify electronic communications;

11. violate copyright, licensing, or intellectual property laws;

12. use artificial intelligence tools or external technology services in a manner that compromises confidential information, student data, academic integrity, cybersecurity, or District operations;

13. connect unauthorized devices, software, applications, or network services to District systems;

14. interfere with the operation, security, or performance of District technology resources.

This list is illustrative and not exhaustive.

Citations

Formatted: Font: Not Bold

- Utah Code § 53G-8-202
- Utah Code § 67-16-4
- Utah Code § 53E-9-309
- Utah Code § 20A-11-1202
- Utah Code § 63A-16-701 et seq.

STUDENT DATA PRIVACY AND THIRD-PARTY APPLICATIONS

Employees shall use only District-authorized software applications, digital instructional tools, cloud services, and technology vendors when accessing, transmitting, storing, or processing student information or District data. Employees shall not:

1. disclose student data to unauthorized individuals or entities;

2. upload student information into non-approved applications or systems;

3. authorize third-party access to student data without District approval;

4. use student information for non-educational purposes;

5. permit third-party technology providers to access student data except as authorized by the District.

All third-party technology providers with access to student data shall comply with applicable federal and state student data privacy laws and District contractual requirements.

Citations

Formatted: Font: Not Bold

- Utah Code § 53E-9-301 through § 53E-9-309
- FERPA, 34 CFR Part 99

RECORDS RETENTION AND PUBLIC RECORDS

Electronic communications, digital records, and information created or maintained using District technology resources may constitute government records subject to retention, preservation, disclosure, or production requirements under applicable law. Employees shall comply with:

- District records retention schedules,
- public records requirements,
- litigation hold directives,
- and lawful preservation obligations.

Employees shall not intentionally destroy, alter, conceal, or improperly delete records subject to retention or preservation requirements.

Citations

Formatted: Font: Not Bold

- Utah Code § 63G-2-101 et seq.
- Utah Code § 63A-12-101 et seq.

VIOLATIONS AND DISCIPLINARY ACTION

Violation of this policy may result in:

- restriction, suspension, or revocation of technology privileges;
- disciplinary action;
- termination of employment;
- referral to law enforcement;
- civil liability;
- or other action authorized by law or District policy.

Disciplinary action shall be administered consistent with:

- District personnel policies,
- employee due process requirements,
- and applicable law.

The District reserves the right to suspend access to District technology resources immediately when necessary to protect District systems, student information, operational integrity, or cybersecurity.

Citations

Formatted: Font: Not Bold

- Utah Code § 53G-11-512
- Utah Code § 67-16-4
- Utah Code § 63G-2-801

IMPLEMENTATION

The Superintendent or Superintendent's designee shall develop administrative procedures, training requirements, cybersecurity protocols, technology standards, and implementation guidelines consistent with this policy. The District may adopt additional administrative procedures governing:

- device management,
- electronic communications,
- artificial intelligence use,
- cybersecurity incident response,
- records retention,
- remote access,
- mobile devices,
- and approval of instructional technology resources.

Formatted: No bullets or numbering

Book Policy Manual

Section E - Students

Title ~~Employee and~~ Student ~~Technology~~ Acceptable Use of District Technology Resources

Code E-30~~, D-66~~

Adopted July 17, 2001

Last Revised June 16, 2026; May 18, 2021

~~**INTRODUCTION**~~

~~Technology use is a valuable and necessary component of student learning, employee work and school/District communication. The District encourages employees and students to use district technology resources and/or services for educational purposes. Students and District employees shall use the District-issued technology resources and/or services primarily to support student learning and instruction and for communication among employees and between employees and parents. Incidental employee and student use of District-issued technology resources and/or services must not interfere with the education of students and shall always be consistent with the District Internet Acceptable Use Policy.~~

~~The information maintained on District technology devices or accounts, resources, and/or services is the District's property. Students and employees do not have an expectation of privacy in their communications through District technology devices or accounts. The District reserves the right to monitor the information contained on District computers or accounts. Any use inconsistent with educational purposes shall be grounds for terminating the account, confiscating the information saved in the account, employee discipline, student discipline and/or limiting the employee s or student s use of District computer equipment, resources, and/or services.~~

~~**SYSTEM FILTER**~~

~~The District utilizes internet filtering systems to assist in restricting access to internet sites containing material that is obscene, pornographic, or harmful to minors. Even though the District takes reasonable efforts to block this material, no filtering systems or technology will filter out all such material. It is the responsibility of the end user to maintain a high level of integrity to protect themselves and others from such inappropriate material. Parents and students are advised~~

that some materials accessible via the internet may be inappropriate. As used herein, references to the terms obscene, obscenity, pornographic, pornography, child pornography, and harmful to minors are defined by applicable state and federal laws, regulations, and causes.

All users, including District employees, students, administrators and educational organizations that have access to District-owned technology resources, and/or services and District-authorized Internet access are subject to this policy and are expected to be familiar with the provisions. This policy may be supplemented by more specific policies, administrative procedures, directives, and rules governing the day-to-day management and operation of District technology resources and services.

PROVISIONS/REQUIREMENTS

1. **Privilege**

a. The use of Internet and computer equipment is a privilege, not a right. Inappropriate use, including any violation of these conditions and rules, may result in cancellation of the privilege. The North Sanpete School and District Administration has the authority to determine appropriate use and the power to deny, revoke, suspend or close any user account at any time based upon its determination of inappropriate use by account holders or users.

b. The materials and products derived and/or produced from District technology resources and services and/or District technology device use are District property.

c. Students in grades 7-12 may obtain an approved school e-mail account. Outside e-mail accounts such as Hotmail are not permitted or accessible using school technology devices.

d. Communications on District-issued devices or through District Internet access are accessible to school employees and parents where those communications are maintained as part of a student's education record, in accordance with the Family Education Rights and Privacy Act (FERPA), 34 CFR § 99.

2. **Acceptable Use Agreements and Training**

a. All users shall access Internet and District-issued computer equipment and technology devices consistent with Federal and State law and the purposes, goals, and policies of the District.

b. The Acceptable Use Agreement must be signed by District employees (both licensed and unlicensed) prior to the first day of work in the District and annually thereafter.

c. The Acceptable Use Agreement must be signed by students and parent(s) upon enrollment in the District and annually in the first month of the school year thereafter. Following initial enrollment all students shall receive training at the beginning of

each school year on internet safety, on this Policy and Policy VII - 35 "Mobile Computing and Storage Devices"

d. The District will provide students and employees with annual training on acceptable Internet use and the appropriate use of District-issued technology devices. The District will collaborate with District school community councils to provide education and awareness of safe technology utilization and digital citizenship for students and school personnel. The District may create subcommittees of community council and District staff members and/or partner with a non-profit entity to develop and provide this training.

e. Internet access shall be filtered and logged consistent with State Law.

3. **Unacceptable Internet and District-issued Technology Use -** The following are examples of unacceptable Internet and technology device uses. This list is not inclusive. A District network or technology device user must not intentionally:

a. Seek and/or acquire unauthorized access to computer of telecommunications networks.

b. Intercept communications intended for other persons.

c. Interfere with the operations of technology resources, and/or services including placing a computer virus on any computer system.

d. Create, store, send, or access or attempt to create, store, send or access sexually explicit, obscene, potentially damaging, dangerous, disruptive, or otherwise inappropriate materials, false or defamatory information or materials and personal or generalized attacks or harassment against individuals or groups of individuals.

e. Create, store, send, or access or attempt to create, store, send or access materials that offensively address age, race, ethnicity, gender, sexual orientation, religious or political beliefs, national origin, or disabilities of a person or a group of people.

f. Log in through another person s account or attempt to access another user s password or files.

g. Further any illegal act, including infringing on any intellectual property rights.

h. Download, upload, or distribute any files, software, or other material that is not specifically related to an educational project or is otherwise authorized by an appropriate school official.

i. Download, upload, or distribute any files, software, or other material in violation of copyright laws.

j. Plagiarize.

k. Access, transmit or retransmit materials which promotes violence or advocates destruction of property including, but not limited to, access to information concerning the manufacture of destructive devices such as explosives, fireworks, smoke bombs, incendiary devices or the like.

l. View, use or send materials or information that violate state or federal law including pornographic or inappropriate images or language, materials that encourage others to violate the law, confidential information or copyrighted materials.

m. Sell or purchase illegal items or substances.

n. Obtain and/or use anonymous email sites or spam.

o. Commit or attempt to commit any willful act involving the use of the network which disrupts the operation of the network within the school district, or any network connected to the Internet including the use or attempted use or possession of computer viruses.

p. Post personal contact information without express parental permission or about students or adults.

q. Delete, copy, modify or forge other users' names, emails, files, or data; disguise one's identity, impersonate other users, or send anonymous email, unless authorized by a school official.

r. Damage computer equipment or technology devices, files, data or the District network in any way.

s. Use any District technology device or personal device on school property to pursue hacking, internal or external to the District, or attempt to access information protected by state or federal laws.

t. Interfere with other users' ability to access their account(s).

u. Disclose private password(s) to others.

v. Use the District network or Internet for commercial purposes.

w. Use the District network or Internet for personal financial gain, personal advertising, or personal promotion.

x. Engage in non-school related fundraising or activities such as Solicitation for religious, personal or political purposes.

y. Otherwise violate student code of conduct or any other policy through the use of the District network and/or District-issued accounts.

4. **Monitoring System**

a. The District monitors District computers or accounts internally or may contract with a monitoring service provider to monitor the information contained on District computers or accounts, including communications from and to students and employees.

b. All such contracts will be entered into in accordance with the Utah Student Data and Privacy Protection Act, Utah Code, Title 53E, Chapter 9, Part 3 and FERPA.

c. The purpose of any monitoring system is to ensure compliance with this and other District policies, and state and federal law.

d. An alternate purpose of a monitoring system is to assure appropriate supports are in place for students whose communication contain information that could lead a reasonable person to believe the student is at risk of harm to themselves of or others.

e. The use of a monitoring system does not impose an obligation on the District to monitor students' and employees' communications and information contained on District computers or accounts twenty-four hours a day, seven days a week, and students, employees, and parents should be aware that information reasonably suggesting a student is at risk of harm to self or others may not be received and addressed immediately.

f. To the extent that a monitoring system in use by the District provides notifications of communications containing information that a student or employee may be at risk of harm to self or others, when a District employee receives and reviews such notification after hours, a District employee will notify parents or law enforcement of the communication.

g. The District will NOT do home visits after hours.

The above prohibitions are examples only; the District reserves the right:

- To take immediate action regarding activities that use District-issued devices or Internet that create security and/or safety concerns for the District, District students, District employees, District schools or property or District network or technology resources and/or services.

- To prohibit or terminate online activities that expend District resources that the District determines lack legitimate educational content or purpose.

STAFF AND STUDENT RESPONSIBILITIES

1. General User Responsibilities

a. It is the responsibility of any user of District electronic resources to read, understand, and follow this policy. Users are expected to exercise reasonable judgment in interpreting the policy and examples in making decisions about the appropriate use of District electronic resources. Any person with questions regarding the application or meaning of the information in this policy should seek clarification from a District administrator. Use of District electronic resources constitutes acceptance of the terms of this policy and Acceptable Use Agreement.

b. Users shall not exceed the District- or supervisor-authorized access to the District network or other computer equipment, system performance, or data.

2. Administrator Responsibilities

a. An administrator is responsible for assuring that educators and students in the District under his control and supervision understand and abide by the Acceptable Use Agreement and Policy as stated in this document. If a District administrator has reason to believe that a user (educator or student) is misusing the system or violating any provision of this Agreement, the administrator may report the misuse to District Technology Department.

b. It is also the responsibility of the administrator to report any misuse of the system immediately to the District and law enforcement, if required by law.

c. Administrators will also immediately report to the District, parents, and law enforcement any information that leads the administrators to reasonably believe a student or employee is at risk of harming themselves or others.

d. Administrators are not responsible for monitoring information contained on District computers or accounts or communications from and to students and employees when the administrator is off contract hours.

e. If an administrator does receive and review after hours information that suggest a student or employee in the administrator s building is at risk of harm to self or others, the administrator shall contact the student s parents or law enforcement or both but will not conduct further investigation into the communication received after hours.

3. Educator/Employee Responsibilities

a. Educators/Employees who supervise students with access to District-owned technology resources and/or services shall be familiar with the District Acceptable Use Agreement and enforce its provisions.

b. It is the responsibility of District educators/employees to teach students with whom they work about safe and responsible use of the Internet and District owned technology.

c. Educators/Employees are responsible for monitoring students' use of electronic resources, and to intervene promptly if students are using them inappropriately.

d. Educators/Employees must assure that students read and act consistent with the District Acceptable Use Agreement and policy. If an educator/employee has reason to believe that a student is misusing the system, the educator/employee must report this activity to his/her direct administrator. Access and/or review of information or records by an educator or employee must take place consistent with District policy.

e. It is also the responsibility of the educator/employee to report any misuse of the system to the appropriate District administrator and/or to law enforcement, if required by law.

f. Educators/Employees are responsible for the security of their District-issued and personal electronic devices and equipment, files and passwords. Educators/Employees shall promptly notify the District of security problems. Educators/Employees with access to student records may not use, release, or share student records except as expressly authorized by federal and State law and District policy.

g. Educators/Employees have no expectation of privacy in files, disks, documents, etc. which were created in, entered in, stored in, downloaded from, or used on District equipment, technology, resources and/or services.

4. **Student Responsibilities**

a. Students have a personal and individual responsibility to learn about safe and responsible use of the Internet and District-issued devices.

b. Students are responsible to use District resources appropriately and consistent with this Agreement and District policy.

c. If a student misuses resources, the District may discontinue the student s use of the District network, the Internet and/or District-issued devices.

d. The District may also take disciplinary action against the student, as appropriate and consistent with District policy.

e. Parents and students are advised that some materials accessible via the Internet may contain items that are illegal, defamatory, inaccurate, or potentially offensive to some people. The District cannot guarantee that filtering software will, in all instances, successfully block access to all inappropriate materials.

f. Students have no expectation of privacy while using the District network, technology, resources and/or services.

g. The District has the right to monitor users' online activities if they are using District-provided Internet and/or District-issued or owned devices and may do so through a contracted monitoring service provider. The District may access, review, copy, and store or delete any electronic communication or files and disclose them to school officials and law enforcement, if required by law.

h. Any stored copy of electronic communications or files become part of the student s education record and is subject to the provisions of FERPA.

DISTRICT NETIQUETTE

1. All users are expected to abide by generally accepted rules of network etiquette. These include, but are not limited to the following:

a. both staff and students must be polite, use appropriate language, and avoid abusive messages;

b. both staff and students must not engage in activities, which are prohibited under school/District Policy or State and Federal Law.

2. Messages relating to or in support of illegal activities may be reported to the authorities and could result in the immediate and permanent loss of user privileges and/or report to law enforcement.

3. Users should not reveal personal information.

4. Users must not use the network in such a way that they could disrupt the use of the network by other users.

5. Users should assume all communications and information accessible via the network to be public records or property.

PURPOSE

District technology resources are provided to support student learning, educational opportunities, communication, research, digital citizenship, creativity, collaboration, and other authorized educational activities. The Board of Education recognizes that responsible technology use is an important component of a student's educational experience and expects students to use District technology resources in a lawful, safe, respectful, ethical, and educationally appropriate manner. For purposes of this policy, District technology resources include, but are not limited to:

- District-owned devices,
- computers,

- mobile devices,
- internet services,
- cloud-based systems,
- software,
- digital applications,
- learning management systems,
- telecommunications systems,
- electronic communication systems,
- student accounts,
- and other electronic resources or services provided or authorized by the District.

Student use of District technology resources is a privilege, not a right. The District may suspend, restrict, or revoke student access to District technology resources when a student violates this policy, related District policies, or applicable law. Students are responsible for using District technology resources in compliance with:

- District policies and procedures,
- applicable law,
- cybersecurity and safety requirements,
- and standards of appropriate digital citizenship and conduct.

OWNERSHIP AND EXPECTATION OF PRIVACY

All data created, transmitted, received, stored, or accessed using District technology resources is District property to the extent permitted by law. Students shall have no expectation of privacy regarding information created, transmitted, received, stored, or accessed using District-owned systems, networks, devices, accounts, or technology resources, except as otherwise protected by applicable law.

The District reserves the right to access, monitor, review, retrieve, preserve, disclose, or delete information maintained on District technology resources for legitimate educational, operational, legal, investigative, cybersecurity, records retention, safety, or compliance purposes. District monitoring and access shall be conducted consistent with:

- applicable federal and state law,
- student privacy protections,
- educational record protections,
- and student due process requirements.

Parents and guardians may access student education records and information regarding a student's use of District technology resources to the extent required or permitted by applicable law, including information maintained through District monitoring, filtering, device management, learning management, or internet safety systems. The District may provide parents and guardians access to:

- student technology usage information,

- internet activity records,
- digital learning activity,
- content filtering information,
- and other student technology records maintained by the District,

consistent with:

- federal and state law,
- student safety requirements,
- cybersecurity protections,
- and operational capabilities of District systems.

Citations

- FERPA, 34 CFR Part 99
- Utah Code § 53E-9-301 through § 53E-9-309
- Utah Code § 63G-2-201 et seq.

INTERNET SAFETY, FILTERING, AND CYBERSECURITY

The District shall maintain technology protection measures, internet filtering systems, cybersecurity safeguards, monitoring systems, and security controls consistent with applicable federal and state law. District technology systems shall be configured to:

- restrict access to unlawful, harmful, obscene, malicious, or inappropriate content;
- protect confidential and student information;
- reduce cybersecurity risks;
- support safe educational use of technology resources;
- and promote digital safety and responsible online behavior.

Although the District uses filtering and monitoring systems, no filtering system is capable of preventing access to all inappropriate material. Students are expected to use District technology resources responsibly and to immediately report accidental access to inappropriate content or suspected cybersecurity concerns to a teacher or administrator.

Students shall not intentionally disable, bypass, interfere with, or attempt to circumvent District filtering systems, cybersecurity safeguards, endpoint protections, monitoring systems, or security procedures.

Citations

- 47 U.S.C. § 254(h) (Children's Internet Protection Act)
- Utah Code § 53E-9-306
- Utah Code § 53E-9-309

Formatted: Font: Not Bold

Formatted: Font: Not Bold

STUDENT RESPONSIBILITIES

Students shall use District technology resources in a lawful, respectful, safe, responsible, and educationally appropriate manner. Students shall:

1. use District technology resources primarily for educational purposes;
2. comply with District technology procedures and classroom expectations;
3. protect passwords and account access information;
4. use only District-authorized applications, software, and digital services for school activities;
5. protect District devices from damage, theft, misuse, or unauthorized access;
6. respect the privacy and rights of others;
7. immediately report suspected cybersecurity incidents, unauthorized access, device damage, or accidental access to inappropriate content to a teacher or administrator;
8. comply with copyright, licensing, and intellectual property laws;
9. follow staff directions regarding appropriate use of technology resources.

Students shall not share passwords or permit another individual to use the student's account or credentials.

DIGITAL CITIZENSHIP AND ONLINE CONDUCT

Students are expected to demonstrate appropriate digital citizenship and responsible online conduct when using District technology resources. Students shall:

1. communicate respectfully and appropriately in electronic communications;
2. use technology resources in ways that support learning and school safety;
3. respect the intellectual property, privacy, and digital rights of others;
4. engage in online behavior consistent with District conduct standards.

Students shall not use District technology resources to engage in:

- cyberbullying,
- harassment,
- intimidation,

- threats,
- retaliation,
- abusive conduct,
- impersonation,
- or other conduct that disrupts the educational environment or violates District policy.

Citations

Formatted: Font: Not Bold

- Utah Code § 53G-8-202
- Utah Code § 53G-8-203
- Utah Code § 53G-8-210

ACCEPTABLE USE AGREEMENT AND TRAINING

Students and a parent or guardian shall sign an Acceptable Use Agreement before the student is provided access to District technology resources and annually thereafter as required by the District. The District shall provide students with instruction and training regarding:

- internet safety,
- cybersecurity awareness,
- responsible digital citizenship,
- student data privacy,
- and appropriate use of District technology resources.

The District may limit or suspend student access to District technology resources if required agreements or training requirements are not completed.

Citations

Formatted: Font: Not Bold

- Utah Code § 53E-9-306
- Utah Code § 53E-9-309

PROHIBITED USES

Students shall not use District technology resources to:

1. access, create, transmit, store, or distribute unlawful, obscene, sexually explicit, threatening, discriminatory, defamatory, harassing, abusive, fraudulent, or disruptive material;

2. engage in cyberbullying, harassment, intimidation, retaliation, or abusive conduct;

3. access systems, accounts, or data without authorization;

4. attempt to bypass security controls, filtering systems, or monitoring systems;

5. introduce malware, ransomware, malicious code, unauthorized software, or other cybersecurity threats;

6. improperly disclose confidential or student information;

7. impersonate another individual or falsify electronic communications;

8. violate copyright, licensing, or intellectual property laws;

9. use District technology resources for unlawful activity or unauthorized commercial activity;

10. record, photograph, or distribute images, audio, or video of individuals without authorization when prohibited by District policy or law;

11. use artificial intelligence tools or external technology services in a manner that violates District policy, academic integrity standards, cybersecurity protections, or student privacy protections;

12. connect unauthorized devices, software, applications, or network services to District systems;

13. interfere with the operation, security, or performance of District technology resources.

This list is illustrative and not exhaustive.

Citations

Formatted: Font: Not Bold

- Utah Code § 53G-8-202
- Utah Code § 53G-8-203
- Utah Code § 53E-9-309

STUDENT DATA PRIVACY AND THIRD-PARTY APPLICATIONS

The District shall use reasonable measures to protect student data and educational records consistent with applicable law. Students shall use only District-approved applications, instructional technology platforms, and digital services for educational activities involving student information or schoolwork when directed by District staff.

Students shall not:

1. access, disclose, or misuse another student's information;

2. upload confidential or student information into unauthorized applications or services;

3. share student information with unauthorized individuals or entities;

4. attempt to access restricted or protected data.

The District may authorize third-party technology providers to provide educational services consistent with applicable law and District contractual requirements governing student data privacy and security.

Citations

Formatted: Font: Not Bold

- Utah Code § 53E-9-301 through § 53E-9-309
- FERPA, 34 CFR Part 99

DISTRICT-ISSUED DEVICES

Students who are assigned District-issued devices are responsible for the reasonable care, appropriate use, and security of those devices. Students shall:

- keep District-issued devices secure;
- comply with District device management procedures;
- promptly report device damage, loss, theft, or malfunction;
- return District-issued devices, accessories, and equipment upon request or upon withdrawal from enrollment.

The District may inspect District-issued devices at any time consistent with applicable law and District policy.

VIOLATIONS AND DISCIPLINARY ACTION

Violation of this policy may result in:

- restriction, suspension, or revocation of technology privileges;
- school disciplinary action;
- restitution for damaged District property;
- parent notification;
- referral to law enforcement;
- or other action authorized by District policy or law.

Disciplinary action shall be administered consistent with:

- District student conduct policies,
- student due process protections,
- and applicable law.

The District reserves the right to suspend access to District technology resources immediately when necessary to protect District systems, student safety, cybersecurity, or operational integrity.

Citations

Formatted: Font: Not Bold

- Utah Code § 53G-8-205
- Utah Code § 53G-8-210

IMPLEMENTATION

The Superintendent or Superintendent's designee shall develop administrative procedures, training requirements, cybersecurity standards, device management procedures, and implementation guidelines consistent with this policy. The District may adopt additional procedures governing:

- student device use,
- electronic communications,
- artificial intelligence use,
- cybersecurity incident response,
- remote learning,
- mobile devices,
- instructional technology approval,
- and internet safety education.

Book	Policy Manual
Section	G – School / Community Relations
Title	Content Filtering and Online Access
Code	G-39
Status	1st Read – June 16, 2026

Purpose

The North Sanpete Board of Education recognizes that access to electronic information resources supports instruction, communication, research, and educational opportunities. The Board also recognizes its obligation to protect students from access to material that is obscene, harmful to minors, or otherwise inconsistent with the educational mission of the District.

Internet Content Filtering

The District shall maintain technology protection measures and internet content filtering systems on all District-managed networks and District-approved electronic devices used by students. The District shall restrict access to internet sites, online services, and electronic resources that contain obscene material or other content prohibited by law. The District shall establish administrative procedures governing implementation, monitoring, and enforcement of content filtering requirements.

Preapproved Content Filtering Upon Parent Request

Upon request of a parent of a student, the District shall require the use of a preapproved content filtering system when the student uses a District-approved electronic device. For purposes of this policy, a preapproved content filtering system means a method of internet access control that permits use only of websites, applications, or online resources specifically approved by the District.

Parent-Accessible Monitoring System

The District shall maintain and utilize a parent-accessible monitoring system that enables a parent to review activity occurring on a District-managed device assigned to the parent's student, consistent with applicable privacy laws and District procedures. Information generated through filtering, monitoring, and device management systems shall be collected, retained, disclosed, and protected in accordance with District student privacy, student records, data governance, and information security requirements.

Administrative Procedures

The District shall maintain administrative procedures and guidelines for employees responsible for implementing and enforcing this policy. The administrative procedures shall address content filtering, monitoring systems, reporting obligations, device management, access controls, response to inappropriate access, corrective actions for violations, parent requests for preapproved content filtering, monitoring

system access procedures, records retention, cybersecurity safeguards, and complaint processing. Implementation of this policy shall be coordinated with applicable District technology, student conduct, student privacy, records management, data governance, and information security policies.

Complaints

The District shall maintain procedures for receiving and addressing complaints concerning:

1. This policy;
2. Enforcement of this policy; and
3. Observed conduct related to student internet access and use.

Complaints concerning implementation or enforcement of this policy shall be processed in accordance with Policy G-06, Public Complaints, and Policy G-08, Public Complaints About School Personnel and/or Services, as applicable. Complaints involving student conduct, cyberbullying, electronic device misuse, student privacy, student records, data governance, or information security may also be reviewed under the applicable District policies governing those matters.

Related Policies

This policy should be read in conjunction with:

- E-30 / D-66 Employee and Student Technology Acceptable Use
- E-48 Bullying, Cyberbullying, Hazing, and Abusive Conduct
- E-39 Student Privacy
- E-55 Student Records
- G-06 Public Complaints
- G-08 Public Complaints About School Personnel and/or Services
- G-21 Records Access and Management
- G-35 Mobile Computing and Storage Devices
- G-38 Data Governance Plan
- H-36 Information Security Policy

Book	Policy Manual
Section	G - School-Community Relations
Title	Mobile Computing, ~~and~~ Storage Devices, and Personal Electronic Devices
Code	G-35
Status	~~Active~~1st Read – June 16, 2026
Adopted	May 15, 2012
Revised	

Formatted Table

Formatted: Left

Formatted: Space Before: 12 pt

~~PHILOSOPHY~~PURPOSE

~~Advances in computer technology, mobile computing, and storage devices have become useful tools in meeting the various student, employee, educational and business needs of the District. These mobile computing and storage devices are especially susceptible to loss, theft, hacking, and the distribution of malicious software (malware) because they are easily portable and can be used anywhere. As mobile computing and storage devices become more widely used, it is necessary to address security issues in order to protect the information resources, technology, and equipment of the District.~~

~~Therefore, the North Sanpete Board of Education has established this Policy in order to control and monitor mobile computing and storage devices, to minimize the risk of loss or exposure of the District's sensitive information, and to reduce the risk of acquiring malware infections on District computers.~~The Board of Education recognizes that technology is an essential component of instruction, communication, business operations, and student learning. The Board is committed to ensuring that technology resources are used in a manner that support educational objectives, protects District information systems and data, promotes cybersecurity, and maintains a safe and effective learning environment.

The Board further recognizes that personal electronic devices may interfere with instruction, student engagement, and school safety when used during the school day. This policy establishes standards governing the use of mobile computing devices, storage devices, District technology resources, and personal electronic devices.

DEFINITIONS

District Data means information created, received, maintained, transmitted, or stored by the District, including student records, employee records, financial information, operational records, and other information maintained in electronic form.

District Network means any wired, wireless, cloud-based, or virtual technology system owned, leased, operated, or managed by the District.

Mobile Computing Device means any portable electronic device capable of storing, processing, transmitting, or accessing electronic information, including laptops, tablets, smartphones, wearable devices, and similar technologies.

Personal Electronic Device means a personally owned cellular telephone, smartphone, smartwatch, tablet, earbuds, wireless communication device, wearable technology device, or any other electronic device capable of communication, messaging, internet access, recording, photography, gaming, or similar functions.

Portable Storage Device means any removable electronic storage medium including flash drives, memory cards, external hard drives, or similar devices.

~~**Handheld Wireless Device**: A communication device small enough to be carried in the hand. Various brands are available, and each performs some similar or some distinct functions. It can provide access to other Internet services, can be centrally managed via a servicer, and can be configured for use as a phone or pager. In addition, it can include software for transferring files and from maintaining a built-in address book and personal schedule. PDAs, iPods, tablets, netbooks, and laptops are all examples.~~

~~**Mobile Devices**: Device or medium that is readable and/or writeable by users and is able to be moved from computer to computer without modification to the computer. Mobile media devices include, but are not limited to: PDA.s, USB port devices, CDs, DVDs, cameras, MP3 players (iPods), flash drives, removable hard drives, modems, handheld wireless devices, wireless networking cards, and other existing or future media devices.~~

~~**Guest Network**: A guest network or VLAN (Virtual Local Area Network) will be set up in each school as needed. This will allow access to the network but separate from the school's network or VLAN. Guest networks will be filtered and require authentication for logging activity. The guest network and school's networks will not have access to the other, helping to ensure the integrity and reliability of the school's network.~~

APPLICABILITY

This policy applies to all students, employees, volunteers, contractors, consultants, vendors, and other individuals who access District technology resources, District networks, District-owned devices, or District data.

DISTRICT TECHNOLOGY RESOURCES

The District may provide technology resources to support educational and operational needs. Use of District technology resources shall be consistent with District Policies, administrative procedures, and acceptable use requirements. The District may establish security, registration, monitoring, management, and access requirements for any device or technology resource that connects to District systems or accesses District data. The District reserves the right to restrict, suspend, or deny access to technology resources that present operational, instructional, legal, privacy, or cybersecurity concerns.

PERSONAL ELECTRONIC DEVICES

Students may possess personal electronic devices while on school property and at school-sponsored activities unless otherwise prohibited by school administration. Students shall not use personal electronic devices during the school day. For purposes of this policy, the school day includes instructional time, passing periods, lunch periods, assemblies, study periods, and other school-sponsored activities occurring during regular school hours. Personal electronic devices shall remain stored and inaccessible during the school day except as expressly authorized under this policy. A student may use a personal electronic device only when:

1. Required because of a documented medical necessity;
2. Required by an Individualized Education Program (IEP), Section 504 Plan, health care plan, or other legally required accommodation;
3. Authorized by a teacher or administrator for a specific educational purpose;
4. Necessary during and emergency affecting health or safety; or
5. Otherwise required by law or approved by District administration.

School-issued devices authorized for instructional purposes are not personal electronic devices under this section and may be used as directed by District employees. The Superintendent shall establish administrative procedures governing storage requirements, enforcement procedures, confiscation procedures, parent notification, and disciplinary consequences for violations of this policy.

PROHIBITED USES

Personal electronic devices shall not be used in restrooms, locker rooms, changing areas, other locations where privacy interests are reasonably expected. Students shall not use personal electronic devices in a manner that violates District policies regarding harassment, bullying, cyberbullying, academic integrity, student conduct, privacy, or school safety.

Formatted: Font: Not Bold

DISTRICT DATA PROTECTION

District users shall protect District Data from unauthorized access, disclosure, modification, destruction, or loss. Confidential, private, protected, or sensitive District information shall not be stored on personally owned devices unless specifically authorized by the District and protected through District-approved security measures. Users shall comply with all District policies governing student records, student data protection, information security, and records management. Only District-approved application, vendors, and technology services may access District Data.

SECURITY REQUIREMENTS

The District may require security controls for devices accessing District systems or District Data, including passwords, encryption, software updates, malware protection, access controls, device management tools, and other safeguards deemed necessary by the District. Users shall not intentionally disable, circumvent, or interfere with District security controls.

LOST, STOLEN, OR COMPROMISED DEVICES

Any individual who becomes aware that a District-owned device, District account, or device containing District Data has been lost, stolen, compromised, or subject to unauthorized access shall immediately report the incident to the appropriate administrator or the District Technology Department. The District may take appropriate actions to protect District systems and information, including restricting access, disabling accounts, removing District information from devices, or implementing other security measures authorized by law.

MONITORING

Use of District-owned devices, District accounts, District networks, and District technology resources may be monitored, reviewed, or inspected as permitted by law and District policy. Users should have no expectations of privacy regarding information created, stored, transmitted, or received using District technology resources except as otherwise provided by law.

ENFORCEMENT

Violation of this policy may result in loss of technology privileges, confiscation of devices as permitted by law, disciplinary action for students, disciplinary action for employees, termination of contractual access for non-employees, other corrective action authorized by District policy or law. The District may refer suspected unlawful conduct to appropriate law enforcement or governmental agencies.

~~**GUIDELINES**~~

~~1. This Policy applies to all District employees, students, consultants, vendors, contractors, and others who choose to use mobile computing and storage devices on the District's network. Each District employee and student will review the Policy annually in conjunction with the Acceptable Use Police.~~

~~2. It is the Policy of North Sanpete School District that mobile computing and storage devices containing or accessing the information resources of the District must be approved prior to connecting to the District's information systems. This pertains to all devices regardless of ownership. Devices not owned by the District may only access guest networks.~~

~~3. Mobile computing and storage devices either personally owned or District owned, that may connect to or access the District's information systems must be pre- approved before using. A risk analysis for each new media type shall be conducted and documented by the School/District Technology Specialist prior to its use or connection to the District's network.~~

~~4. Technical personnel and users, which include employees, consultants, vendors, contractors, and students, shall have knowledge of, sign and adhere to the Computer Use and Information Security Policy Agreement. Compliance with other applicable policies, procedures, and standards is mandatory.~~

5. Students who bring personal storage devices (such as flash drives) to school may only plug these devices into computers with software that will prevent against unwanted workstation changes. The school/District also reserves the right to review the files on these devices before students use them. This review shall be done by the School Site Specialist or the District Technology Director.

6. Portable computing devices and portable electronic storage media that contain confidential, personal, or sensitive information must use encryption or equally strong measures to protect the date while it is being stored. Confidential or sensitive data shall never be stored on a personal device.

7. Charges for repair due to misuse of equipment or misuse of services may be the responsibility of the user, as determined on a case-by-case basis by District or Regional Technology Specialists at CUES.

8. Minimum Requirements by Users:

    a. Employees and students shall report lost or stolen mobile computing and storage technologies that are owned by the District or have sensitive District information on them.

    b. The District shall approve all new mobile computing and storage technologies that may connect to the District's information systems.

    c. The District's technical personnel must first approve any non-departmental owned device that may connect to the District's network.

    d. Devices not owned by the District shall only connect to the guest networks.

9. Penalties for Improper Use: A violation of this Policy or applicable State and Federal Laws may result in appropriate student or employee discipline in accordance with District policies and the disciplinary measures outlined in the District Acceptable Use Policies: IV-66, and V-30. In addition, the site administrator/supervisor or systems administrator may limit, suspend, or revoke access to electronic resources at any time. All penalties for improper use will also be documented and placed in the employee's file or a student's records.