Policy 524.2 ACCEPTABLE USE AND SAFETY OF TECHNOLOGY AND TELECOMMUNICATION SYSTEMS BY STUDENTS

I. PURPOSE

To prepare every student for lifelong success, the Northfield School District provides technology and telecommunications resources for district students to equitably support and enhance student learning so they can become critical thinkers who are curious and ready to engage in our society. Access to and use of technology resources for students and employees is a fundamental part of education. This policy covers district student use of all technology and telecommunications resources in the district. The purpose of this policy is to govern and guide the appropriate use of these resources as we prepare every student to be academically and socially ready to choose their preferred pathway after high school graduation.

II. GENERAL STATEMENT OF POLICY

The district provides students with access to computers and peripherals, district networks, on campus and hotspot Internet access, software applications and other technology services in order to support and enhance student learning and to prepare them for work and life.

III. ACCEPTABLE/UNACCEPTABLE USES

A. Each student shall act responsibly when utilizing technology resources.

1. The use of the school district networks/computers/peripherals and internet/software applications and systems is a privilege that can be revoked at any time for abusive behavior. All activity and utilization of district technology resources must comply with Student Citizenship Handbook and school board policies.

2. While not an exhaustive list, students will not:
   - Use district technology resources to access, review, display, store, upload, download, distribute, post, receive, transmit, or print pornographic, obscene or sexually explicit materials or language, or other visual depictions that are harmful to minors.
   - Use district technology resources to access, display, store, upload, download, distribute or print materials that advocate violence, harassment or discrimination (hate literature) or are disruptive in any way.
   - Send abusive, intimidating, harassing, or unwanted material causing the work of others to be disrupted.
   - Use the district technology resources to vandalize, damage or disable the property of another person, will not make deliberate attempts to degrade, vandalize or disrupt equipment, software, or system performance, will not violate the network's security in any way, and will not use the district network/Internet/email system in any way so as to disrupt the use of the system by other users.
   - Use district technology resources to gain unauthorized access to resources, passwords, accounts, information or files without direct permission from the district.

- Use district technology resources to violate copyright laws, download or pirate software or plagiarize information, or engage in any illegal act or violate any local, state, or federal statute or law.
- Send or forward unnecessary or frivolous emails or messages in any quantity to other users of the district email system or other digital applications. Transmission of chain letters and pyramid schemes is strictly prohibited.
- Use district technology resources for commercial purposes, political lobbying or solicitation of any kind.
- Use non-district owned equipment or devices to access networks and file servers that require district-provided credentials.
- Use district technology resources to communicate under a false name or designation or a name or designation they are not authorized to use, including instances in conjunction with representing that they are somehow acting on behalf of or under the auspices of the district.
- Use the name "Northfield Public Schools" in any form or use any symbol or logo or graphic used by Northfield Schools without the district's prior consent.
- Utilize the district system to post personal information about a user or another individual on social networks, including, but not limited to, social networks such as Facebook, Twitter, Instagram, Snapchat, TikTok, Reddit, and similar websites or applications.

3. Students will use electronic information resources in compliance with all existing school board policies. Non-district owned equipment may access district guest networks but must comply with district policy and procedures.

B. Each student shall respect private passwords, copyright and other intellectual property rights.

1. Copying of data, files or using passwords belonging to others will be considered a violation of district policies, a violation of law, and may constitute fraud, plagiarism or theft.
2. Software licensed by the district must only be used in accordance with applicable license specifications and agreements. Illegal copying and/or installing of software on district computers is strictly prohibited. Illegal copying and/or installing of district licensed software on personal devices is strictly prohibited.
3. Modifying or damaging information without authorization including but not limited to altering data, introducing viruses or damaging files or data is unethical and a violation of district policies.

C. Each student shall abide by security restrictions on all systems and information.

1. Distributing or making your password or another person's password or access code available to others or otherwise attempting to evade, disable or "crack" passwords, desktop security systems, or other security precautions, or assisting others in doing so threatens work, privacy and the integrity of district information, and is a serious violation of district policy.
2. Attempts to "bypass" virus protection software on workstations or servers are violations of district security procedures.

3. Software or applications are generally installed by District technology services staff. Software or applications may only be installed by students with specific permission from the district.

D. Each student shall recognize limitations to privacy and use of electronic communications. Employees, staff and students do not own district technology and telecommunications equipment or software. The district reserves the right to access user files at any time to protect the integrity of the systems and property of the district.

1. The district may examine or make copies of files that are suspected of misuse, or that have been corrupted or damaged. Files may be subject to search by law enforcement agencies if files contain information, which may be used as evidence in a court of law.
2. An individual investigation or search will be conducted if school authorities have a reasonable suspicion that the search will uncover a violation of law or district policy. The district will cooperate fully with local, state and federal authorities in any investigation concerning or related to any illegal activities and activities not in compliance with district policies.

E. Each student shall be aware that data and other materials in files maintained on district property or hosted solutions licensed by the district may be subject to review, disclosure or discovery under State and Federal legislation, including the Minnesota Government Data Practices Act.

1. The district can and will monitor the online activities of all employees and students, and employ "filtering" protection measures during any use by employees and/or students. The "filtering" measures are intended to block Internet sites that contain violent, obscene, pornographic or sexually explicit materials. The district will comply with any and all state and federal requirements around Internet filtering for student use. The use of this software does not guarantee that students or staff will not be able to obtain objectionable or pornographic materials over the Internet, but the chances have been minimized.
2. It is mandatory that staff closely monitor and supervise student use of the Internet and all other technology resources at school to ensure appropriate, educational use.

F. The district has a special interest in regulating off-campus speech that materially disrupts classwork or involves substantial disorder or invasion of the rights of others. A student or employee engaging in the foregoing unacceptable uses of the internet when off district premises also may be in violation of this policy as well as other district policies. Examples of such violations may include, but are not limited to, serious or severe bullying or harassment targeting particular individuals, threats aimed at teachers or other students, failure to follow rules concerning lessons, the writing of papers, the use of computers, or participation in other online school activities, and breaches of school security devices. If the district receives a report of an unacceptable use originating from a non-school computer or resource, the district may investigate such reports to the best of its ability. Students or employees may be subject to disciplinary action for such conduct, including, but not limited to, suspension or cancellation of the use or access to the district computer system and

the internet and discipline under other appropriate district policies, including suspension, expulsion, exclusion, or termination of employment.

IV. PARENTS' RESPONSIBILITY; NOTIFICATION OF STUDENT INTERNET USE

Outside of school, parents are responsible for monitoring their student's use of the district system and of the Internet if the student is accessing the district system from home or a remote location.

Parents may have the right at any time to investigate or review the contents of their child's files and email files in accordance with the school district's Protection and Privacy of Pupil Records Policy. Parents have the right to request the termination of their child's individual account at any time.

V. NOTIFICATION REGARDING TECHNOLOGY PROVIDERS

A. "Technology provider" means a person who:

1. Contracts with the district, as part of a one-to-one program or otherwise, to provide a school-issued device for student use.

2. Creates, receives, or maintains educational data pursuant or incidental to a contract with the district.

B. "Parent" means a parent of a student and includes a natural parent, a guardian, or an individual acting as a parent in the absence of a parent or a guardian.

C. Within 30 days of the start of each school year, the district must give parents and students direct and timely notice, by United States mail, e-mail, or other direct form of communication, of any curriculum, testing, or assessment technology provider contract affecting a student's educational data. The notice must:

1. Identify each curriculum, testing, or assessment technology provider with access to educational data.

2. Identify the educational data affected by the curriculum, testing, or assessment technology provider contract.

3. Include information about the contract inspection and provide contact information for a school department to which a parent or student may direct questions or concerns regarding any program or activity that allows a curriculum, testing, or assessment technology provider to access a student's educational data.

D. The district must provide parents and students an opportunity to inspect a complete copy of any contract with a technology provider.

E. A contract between a technology provider and the district must include requirements to ensure appropriate security safeguards for educational data. The contract must require that:

1. The technology provider's employees or contractors have access to educational data only if authorized.

2. The technology provider's employees or contractors may be authorized to access educational data only if access is necessary to fulfill the official duties of the employee or contractor.

F. All educational data created, received, maintained, or disseminated by a technology provider pursuant or incidental to a contract with a public educational agency or institution are not the technology provider's property.

VI. SCHOOL-ISSUED DEVICES

A. "School-issued device" means hardware or software that the school district, acting independently or with a technology provider, provides to an individual student for that student's dedicated personal use. A school-issued device includes a device issued through a one-to-one program.

B. Except as provided in paragraph C, the district or a technology provider must not electronically access or monitor:

1. Any location-tracking feature of a school-issued device.

2. Any audio or visual receiving, transmitting, or recording feature of a school-issued device., or

3. Student interactions with a school-issued device, including but not limited to keystrokes and web-browsing activity.

C. The school district or a technology provider may only engage in activities prohibited by paragraph B if:

1. The activity is limited to a noncommercial educational purpose for instruction, technical support, or exam-proctoring by district employees, student teachers, staff contracted by the district, a vendor, or the Minnesota Department of Education, and notice is provided in advance.

2. The activity is permitted under a judicial warrant.

3. The district is notified or becomes aware that the device is missing or stolen.

4. The activity is necessary to respond to an imminent threat to life or safety and the access is limited to that purpose.

5. The activity is necessary to comply with federal or state law, including but not limited to Minnesota Statutes section 121A.031., or

6. The activity is necessary to participate in federal or state funding programs, including but not limited to the E-Rate program.

D. If the district or a technology provider interacts with a school-issued device as provided in paragraph C, clause 4, it must, within 72 hours of the access, notify the

student to whom the school-issued device was issued or that student's parent and provide a written description of the interaction, including which features of the device were accessed and a description of the threat. This notice is not required at any time when the notice itself would pose an imminent threat to life or safety, but must instead be given within 72 hours after that imminent threat has ceased.

VII. LIMIT ON SCREEN TIME FOR CHILDREN IN PRESCHOOL AND KINDERGARTEN

A child in a publicly funded preschool or kindergarten program may not use an individual-use screen, such as a tablet, smartphone, or other digital media, without engagement from a teacher or other students. This section does not apply to a child for whom the school has an individualized family service plan, an individualized education program, or a 504 plan in effect.

VIII. CELL PHONE USE

The board directs the superintendent and district administration to establish rules and procedures regarding student possession and use of cell phones in schools. These rules and procedures should minimize the impact of cell phones on student behavior, mental health, and academic attainment. These rules and procedures may be designed for specific school buildings, grade levels, or similar criteria.

Policy 524.2 Use of Technology and Telecommunications Systems by Students
Adopted: 04.13.1998; Updated: 07.19.2001, 05.10.2004, 06.10.2013, 03.09.2020, 09.27.2021; Statutory Update: 02.14.2022, 11.14.2022, 11.25.2024

Board of Education
INDEPENDENT SCHOOL DISTRICT NO. 659
Northfield, Minnesota

Legal References: Minn. Stat. Ch. 13 (Minnesota Government Data Practices Act)
Minn. Stat. § 13.32 (Educational Data)
Minn. Stat. § 121A.031 (School Student Bullying Policy)
Minn. Stat. § 121A.73 (School Cell Phone Policy)
Minn. Stat. § 124D.166 (Limit on Screen Time for Children in Preschool and Kindergarten)
Minn. Stat. § 125B.15 (Internet Access for Students)
Minn. Stat. § 125B.26 (Telecommunications/Internet Access Equity Act)
15 U.S.C. § 6501 et seq. (Children's Online Privacy Protection Act)
17 U.S.C. § 101 et seq. (Copyrights)
20 U.S.C. § 1232g (Family Educational Rights and Privacy Act)
47 U.S.C. § 254 (Children's Internet Protection Act of 2000 (CIPA)
47 C.F.R. § 54.520 (FCC rules implementing CIPA)
Mahanoy Area Sch. Dist. v. B.L., 594 U.S., 180, 141 S. Ct. 2038 (2021)
Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503 (1969)
United States v. Amer. Library Assoc., 539 U.S. 194 (2003)
Sagehorn v. Indep. Sch. Dist. No. 728, 122 F.Supp.2d 842 (D. Minn. 2015)
R.S. v. Minnewaska Area Sch. Dist. No. 2149, 894 F.Supp.2d 1128 (D. Minn. 2012)
Tatro v. Univ. of Minnesota, 800 N.W.2d 811 (Minn. App. 2011), aff'd on other grounds 816 N.W.2d 509 (Minn. 2012)
S.J.W. v. Lee's Summit R-7 Sch. Dist., 696 F.3d 771 (8th Cir. 2012)
Parents, Families and Friends of Lesbians and Gays, Inc. v. Camdenton R-III Sch. Dist., 853 F.Supp.2d 888 (W.D. Mo. 2012)
M.T. v. Cent. York Sch. Dist., 937 A.2d 538 (Pa. Commw. Ct. 2007)

Cross References: MSBA/MASA Model Policy 403 (Discipline, Suspension, and Dismissal of School District Employees)
MSBA/MASA Model Policy 406 (Public and Private Personnel Data)
MSBA/MASA Model Policy 505 (Distribution of Nonschool-Sponsored Materials on School Premises by Students and Employees)

MSBA/MASA Model Policy 506 (Student Discipline)
MSBA/MASA Model Policy 514 (Bullying Prohibition Policy)
MSBA/MASA Model Policy 515 (Protection and Privacy of Pupil Records)
MSBA/MASA Model Policy 519 (Interviews of Students by Outside Agencies)
MSBA/MASA Model Policy 521 (Student Disability Nondiscrimination)
MSBA/MASA Model Policy 522 (Title IX Sex Nondiscrimination Grievance Procedures and Process)
MSBA/MASA Model Policy 603 (Curriculum Development)
MSBA/MASA Model Policy 604 (Instructional Curriculum)
MSBA/MASA Model Policy 606 (Textbooks and Instructional Materials)
MSBA/MASA Model Policy 806 (Crisis Management Policy)
MSBA/MASA Model Policy 904 (Distribution of Materials on School District Property by Nonschool Persons)