Policy 524-2 - Use of Technology and Telecommunications Systems By Students

I. Purpose

The school district provides technology and telecommunications resources for district students to support and enhance student learning. 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.

II. General Statement of Policy

The school district provides students with access to computers and peripherals, district networks, Internet, software applications and other technology services in order to support and enhance student learning and to prepare them for work and life in the 21st Century.

III. Acceptable/Unacceptable Uses

1. **Each student shall act responsibly when utilizing technology resources**
   a. 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 the District Discipline Guidelines and School Board Policies.
   b. Access to the Internet will be for educational purposes only, and students will not use the school district technology resources to access, display, store, upload, download, distribute or print pornographic, obscene or sexually explicit materials.
   c. Students will not use the school district technology resources to access, display, store, upload, download, distribute or print materials that advocate violence, harassment or discrimination or are disruptive in any way.
   d. Students will not send abusive, intimidating, harassing, or unwanted material causing the work of others to be disrupted.
   e. Students will not use the school 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 school district network/Internet/email system in any way so as to disrupt the use of the system by other users.
   f. Students will not use the school district technology resources to gain unauthorized access to resources, passwords, accounts, information or files without direct permission from the district.
   g. Students will not use school district technology resources to violate copyright laws, download or pirate software or plagiarize information.
   h. Students will not send or forward unnecessary or frivolous emails or messages in any quantity to other users of the district email system. Transmission of chain letters and pyramid schemes is strictly prohibited.
   i. Students will not use school district technology resources for commercial purposes, political lobbying or solicitation of any kind.
   j. No non-district owned equipment (computers, printers, peripherals, etc.) can be used to access the school or district data networks and file servers.
   k. Students will not 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 school district.
   l. Students will not 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.
   m. Students will use electronic information resources in compliance with all existing school board policies.

2. **Each student shall respect private passwords, copyright and other intellectual property rights.**
    a. Copying of data, files or using passwords belonging to others will be considered a violation of school district policies, a violation of law, and may constitute fraud, plagiarism or theft.
    b. Software licensed by the school 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.
    c. 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 school district policies.

3. **Each student shall abide by security restrictions on all systems and information.**
    a. 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 school district information, and is a serious violation of school district policy.
    b. Attempts to "bypass" virus protection software on workstations or servers are violations of district security procedures.
    c. 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.

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

5. **Each student shall be aware that data and other materials in files maintained on school district property may be subject to review, disclosure or discovery under State and Federal legislation, including the Minnesota Government Data Practices Act.**
    a. The School 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.
    b. 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.

Policy 524-2
Adopted: 4/13/98
Policy Revised: 7/19/01, 5/10/04, 6/10/13

School Board
INDEPENDENT SCHOOL DISTRICT 659
Northfield, Minnesota