## Policy 441 USE OF TECHNOLOGY AND TELECOMMUNICATIONS SYSTEMS BY EMPLOYEES

## I. PURPOSE

The Northfield School District provides technology and telecommunications resources for district employees to support the educational and operational mission of the school district. Access to and use of technology resources for students and employees is a fundamental part of the school day. This policy covers district employee 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 district provides technology to employees in order to support quality education, information and communication systems. It is the expectation that staff will use these technologies for meaningful educational activities that support the curriculum and district operations needs, as well as provide strong guidance and supervision toward appropriate student use.

## III. EMPLOYEE EXPECTATIONS FOR TECHNOLOGY USE

1. Each employee shall act responsibly when utilizing technology resources.

    a. The use of the school district network/internet/email system is a privilege, not a right. Employees may occasionally access district networks/internet/email/devices for personal use as long as it does not interfere with the employee's job duties and performance. Employees will use electronic information resources in compliance with all existing school board policies.

    b. Employees will not:
        - Use district technology resources to access student, guardian, or staff data that is not needed to carry out their role for the district.
        - Use the school district technology resources to access, display, store, upload, download, distribute or print pornographic, obscene or sexually explicit materials.
        - 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.
        - Send abusive, intimidating, harassing, or unwanted material, such as advertising, causing the work of others to be disrupted.
        - 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.
        - Use the school district technology resources to gain unauthorized access to resources, passwords, accounts, information or files without direct permission from a network authority.
        - Use school district technology resources to violate copyright laws, download or pirate software or plagiarize information.

- 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.
- Use school district technology resources for commercial purposes, political lobbying or solicitation of any kind.
- Use non-district equipment to access the school district wired, password-protected wireless networks, or district accounts without explicit permission of the director of technology services, network manager, or their designee. This does not apply to district systems for which users have their own username and password.
- 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.
- Use the name "Northfield Public Schools" in any form or use any symbol or logo or graphic used by Northfield School District without the district's prior consent.

2. Each employee 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 or personal 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 employee 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 authorized for installation by district technology services staff. In most cases, users are able to install their own software via school district software installation portals.

4. Each employee shall recognize limitations to privacy and use of electronic communications. Employees and staff 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.
c. District-owned laptops and mobile devices may be used outside of school except when employees are directed by technology or administrative staff to leave equipment on site.

5. Each employee 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 monitor and supervise student use of the internet and all other technology resources at school to ensure appropriate, educational use.

6. Each employee shall be aware of limitations of school district liability.
   Use of the school district system is at the user's own risk. While the school district will take precautions with the installation of hardware and software in the security of data and systems, there are no foolproof means for absolutely securing all data and systems.

    a. The school district will not be responsible for any damage users may suffer, including, but not limited to, loss, damage or unavailability of data stored on school district disks, tapes, hard drives, servers, vendor-provided systems, cloud-based services, and/or for delays or changes in or interruptions of service.
    b. The school district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the school district network/internet/email system. The school district will not be responsible for financial obligations arising through unauthorized use of the school district system or the Internet.

7. Each employee shall refrain from text messaging or using electronic mail while driving. In compliance with Minnesota Statute 169.475 Use of Wireless Communications Device, it is the policy of the district to:

    a. Prohibit all text messaging, including electronic mail, by all district employees and encourage contractors to adopt policies that prohibit text messaging while driving. This prohibition includes the time waiting for a traffic signal to change.
        (1) While driving district owned, leased or rented vehicles,
        (2) While driving a personally owned vehicle when on official district business; and
        (3) While driving any vehicle, even during off-duty hours, and using electronic equipment supplied by the district;

b. Take appropriate disciplinary action for violation of this mandatory ban on texting, up to and including removal from employment; and
c. Encourage district employees and contractors and their families to refrain from texting, or from engaging in any behavior that distracts attention from driving safely, at any time.

Policy 441 Use of Technology and Telecommunication Systems By Employees

Adopted: 04.13.1998; Revised: 07.19.2001, 05.10.2004, 06.10.2013, 11.24.2014; Updated: 07.12.2021
Renumbered: 03.28.2005

School Board
INDEPENDENT SCHOOL DISTRICT NO. 659
Northfield, Minnesota