

PERSONNEL

POLICY TITLE	POLICY NUMBER	ADOPTED	REVIEW FREQUENCY
Employee Technology and Internet Access and Acceptable Use	428	Adopted: 6/11/2020 Revised: 12.20.22	Annually

I. PURPOSE

The School Board recognizes that technological resources can enhance employee performance by offering effective tools to assist in providing a quality instructional program, facilitating communications with parents/guardians, students, and the community, supporting district and school operations, and improving access to and exchange of information. The Board expects all employees to learn to use the available technological resources that will assist them in the performance of their job responsibilities. As needed, employees shall receive professional development in the appropriate use of these resources.

Employees shall be responsible for the appropriate use of technology and shall use the district's technological resources primarily for purposes related to their employment. Employees may have limited personal use of technology that is confined to break-times and does not negatively impact the technology, the employee's job performance, or their work environment, as long as all other policies and regulations are being adhered to.

II. NOTICE TO EMPLOYEES

The Superintendent or designee shall provide copies of related policies, regulations, and guidelines to all employees who use the district's technological resources. Employees shall be required to acknowledge that they have read and understood the district's policies related to technology.

III. CONTENT FILTERING FOR EMPLOYEES

The Superintendent or designee shall ensure that all District computers with Internet access have a technology protection measure that prevents access to visual depictions that are obscene or child pornography and that the operation of such measures is enforced. The Superintendent or designee may disable the technology protection measure during use by an adult to enable access for bona fide research or other lawful purpose.

IV. PRIVACY STATEMENT

To ensure proper use, the Superintendent or designee may monitor employee usage of technological resources, including all network traffic, email, and stored files. Monitoring may occur at any time without advance notice or consent.

Employees shall be notified that computer files and electronic communications, including

email and voicemail, are not private. Technological resources shall not be used to transmit confidential information about students, employees, or district operations without authority. When authorized, any electronic transmission of confidential information must be clearly noted as such in the header, subject line, or footer.

V. PUBLISHING STUDENT WORK

The board recognizes that staff want to celebrate student achievement and work by publishing their accomplishments online. The Board expects staff to acquire prior approval from a student's parent/guardian prior to publishing any student images or work as needed. (public publishing)

VI. ELECTRONIC COMMUNICATION WITH STUDENTS

Employees shall communicate electronically (2-Way communication) only with students through their District approved technology resources. Violation of this article will result in disciplinary action, and/or legal action in accordance with law, Board policy, and administrative procedures.

A. Texting Exception

1. Staff may use text-based messaging with any student with whom they share a familial relationship without conditions.
2. Staff may use text-based messaging with students under the following conditions:
 - a. Proper notice has been provided to parents regarding the use of text-based messaging, including the person(s), purpose(s), and time frame(s) during which such communications will take place.
 - b. The content and context of the text-based messages directly relate to the academic, athletic, or club to which the staff and student need text-based communication to support.
 - c. Parents and students are provided an opportunity to opt-out of text-based communications between a staff and student.

VII. USE OF INTERNET-BASED RESOURCES

The Board recognizes that employees require the use of Internet-based resources beyond the scope of what has been officially adopted by the District. Employees must notify their site Principal or Superintendent of any Internet-based resources which they control that directly relate to their employment with the District. Employees must also remove any content immediately upon the request of their site Principal, Superintendent or direct supervisor. Employees must take offline and stop using any Internet-based services upon the request of their site Principal, Superintendent or direct supervisor.

Any district staff member who uses an Internet based resource with students is responsible for ensuring that parents/guardians are informed of the tool being used and the student data being shared with or created on the tool. This information must be present in the syllabus and must be proactively sent to parents/guardians at the beginning of the term, before the

tool is used.

Employees using Internet-based resources to publish information to web sites, blogs, forums, or other online communications representing the school or district shall do so unidirectionally; whereby information is only provided via One-way Communication*. These resources must be set up in such a way that they cannot be used as two-way communication platforms. Such resources shall be subject to rules and guidelines established for district online publishing activities including, but not limited to, copyright laws, privacy rights, and prohibitions against obscene, libelous, and slanderous content. The District retains the right to delete material on any such online resource and employees must comply with the District request to do so.

VIII. EMPLOYEE USE OF TECHNOLOGY RULES AND RESPONSIBILITIES

- A. Employees are authorized to use district equipment to access the Internet or other online services in accordance with Board policy, including the user obligations and responsibilities specified below.
1. The employee in whose name an online services account is issued is responsible for its proper use at all times. Employees shall keep account information private. Each employee shall only use the account(s) to which they have been assigned. Under no circumstance shall employees reveal their passwords to anyone.
 2. Employees shall use computer systems and the Internet safely, responsibly, and primarily for work-related purposes.
 3. Employees shall not access, post, submit, publish, or display harmful or inappropriate manner that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others based on their race, ethnicity, national origin, sex, gender, gender identity, sexual orientation, age, disability, religion, or political beliefs.
 4. Employees shall not use the district computer systems or the Internet to promote unethical practices or any activity prohibited by law, Board policy, or administrative procedure.
 5. Employees shall not use district computer systems or the Internet to engage in commercial or other for-profit activities without permission of the Superintendent or designee.
 6. Copyrighted material shall be posted online only in accordance with applicable copyright laws.
 7. Employees shall not engage in computer **hacking**; broadly **defined** as intentionally accessing a computer, computer system, network, network system, or user account without authorization or exceeding one's authorized access.
 8. Users shall report any security problem or misuse of the services to the Superintendent or designee.

9. When using email to discuss issues and data surrounding individual students, staff is required to indicate that the email contains confidential information by including the word “confidential” in either the email’s subject or main message area.
10. When using email to transfer one or more sets of student data (i.e. an excel document of student names and addresses), staff are required to secure the email’s attachment(s) using encryption.
11. Unless authorized by an employee’s supervisor, staff are only to use District email groups to which they are a member or are inclusive of the building that they work in. Wider message distribution must occur in cooperation with Building or District leadership.

IX. DEFINITIONS

“One-way Communication” is defined as any Internet, app, or cellular based communication where a message is sent or posted with no continuing dialogue. An example would be a staff member using an internet based texting service to notify the class of an upcoming test, where that service is one-way and doesn’t facilitate the recipient’s action to reply.

“Two-way Communication” is defined as any Internet, app, or cellular based conversation where there is a message, a response, and a response to the response. For instance, a staff member could post a notice on Facebook (message), and people could comment on that post (a response) without this being considered two-way communication. When the teacher responds with a comment (a response to a response), there is now a two-way communication and therefore a conversation is taking place.

“Text Messaging” is defined as any communication platform that is enabled from a cellular phone, tablet device, or messaging application that facilitates private communication between two parties via text, videos, or images being sent and received. This includes standard cellular text messaging, sms and mms protocols, and any apps that perform similar functions such as, but not limited to, WhatsApp, Snapchat, Signal, Facebook Messenger, etc.

“District authorized Internet-based resources” are any communication platform adopted and/or paid for by the school district including but not limited to district email, gradebook software, student information system(s), learning management systems, etc.

Legal References:

17 U.S.C. § 101 et seq. (Copyrights)

47 C.F.R. § 54.520 (FCC rules implementing CIPA)

Minn. Stat. § 125B.26 (Telecommunications/Internet Access Equity Act)