POLICY 441 – DIGITAL TECHNOLOGIES AND DIGITAL SYSTEMS ACCEPTABLE USE

I. Purpose: The purpose of this policy is to set forth policies and guidelines for access to the Osseo Area School District's digital technologies, digital systems, digital security and acceptable and safe use of the Internet, including electronic communications.

II. General Statement of Policy

A. The school district provides students and employees with access to district digital technologies and digital systems including Internet access, in order to further educational and professional goals consistent with the policies and mission of the school district.

B. Use of district digital technology and Internet resources must support the curriculum and enhance student learning opportunities, support accurate and appropriate communication of school district information, or increase efficiency and effectiveness of school district work.

C. All electronic communication that is sent or received on the school district digital technology and digital systems is considered property of the school district.

D. The school district monitors online activities and operates technology protection measures that protect against access to unacceptable material through school district technologies and digital systems.

E. Ultimately, parents and guardians of minors are responsible for setting and conveying the standard that their children should follow when using technology and Internet resources. While the school district will monitor student technology and Internet uses as closely as possible, the school district cannot guarantee that students will not independently access technology and Internet resources.

F. The Superintendent or Superintendent's designee will establish plans, procedures, and guidelines for technology asset management, cybersecurity, and internet safety.

III. Definitions

A. Digital Systems- means systems to transmit and store electronic data. This includes but is not limited to the interconnected WAN (wide area network), LAN (local area network), internet, SIS (student information system), LMS (learning management system), FIS (finance information system), HRIS (human resource information system), and SAN (storage area network).

B. Digital Technology- means physical hardware or components that gather, transmit, or display digital media and/ or information. This includes but is not limited to computers, switches, phones, monitors, servers, digital displays, document cameras, security cameras, and access points.

C. Digital Resource- software, application, web-based software utilized for teaching, learning, or district operations.

IV. Guidelines for Acceptable Use

A. School district employees will provide guidance and instruction to students in the use of the Internet and other digital resources for educational and informal purposes that enhance student learning such as research, instruction, collaboration, education projects and other support of the curriculum.

B. The school district will educate students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

C. Users will use the Internet, digital technologies, digital systems, and digital resources for professional learning, teaching and learning, collaborative education projects, school district operations, and dissemination of school district information.

D. School district employees may utilize district issued digital technology for incidental personal use.

V. Security

A. The District establishes data security classifications, implements procedural and electronic security controls, and maintains records regarding assigned security authorization. Data security measures apply to all users of school district digital systems and digital technologies.

B. Access to school district digital systems is controlled by the use of unique credentials (usernames and passwords). Unique credentials are assigned to specific users and each user is accountable for all actions occurring under their access credentials.

C. Users may not allow anyone else to use their credentials to access the district digital technologies or digital systems.

D. Users may not leave their user accounts logged in on an unattended district digital technology.

E. Users should not store credentials where others may access them. Users that suspect their account has been compromised must report it to the technology division and change their password as soon as possible.

F. Users should immediately report to Technology Department (i.e. within 24 hours if possible) when they believe that a digital technology under their control has been lost, stolen, compromised or significantly damaged.

G. All acquisitions whether by purchase or otherwise of digital technologies or digital resources must be approved in advance by the Technology Division to assure functionality with district digital technologies and digital systems.

H. User accounts will be disabled and users are required to return district issued digital technology to the district upon unenrollment or unemployment with the district.

VI. Internet Safety

Under the Children's Internet Protection Act (CIPA), districts are required to restrict minors' access to Internet-based materials. The District has a licensed a commercial Internet filtering package that meets or exceeds the CIPA requirements for student protection.

A. With respect to any of its computers with Internet access, the school district will monitor the online activities of both minors and adults and employ technology protection measures during any use of such computers by minors and adults. The technology protection measures utilized will be designed to block or filter Internet access to any visual depictions that are:

1. Obscene;
2. Child pornography; or
3. Harmful to minors.

B. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or

2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd

3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

C. Software filtering technology must be narrowly tailored and should not discriminate based on viewpoint.

D. An administrator, supervisor, or other person authorized by the Superintendent may disable the technology protection measure, during use by an adult, to enable access for bona fide research or other lawful purposes.

E. The school district will educate students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

F. Internet content filtering tools do not guarantee inappropriate content from being accessed. The district will make best effort to prevent this content through a CIPA compliant content filter and establish a process to address content that inadvertently does not get filtered.

VII. Prohibited Uses

A. The following uses of the school district system and Internet resources or accounts are considered unacceptable:

1. Users will not use the school district system to access, review, upload, download, store, print, post, receive, transmit, or distribute:

a) pornographic, obscene, or sexually explicit material or other visual depictions that are harmful to minors;

b) obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language;

c) materials that use language or images that are inappropriate in the education setting or disruptive to the educational process;

d) information or materials that could cause damage or danger of disruption to the educational process;

e) materials that use language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination;

f) materials that promote harmful or illegal activities or behavior.

2. Users will not use the school district system to knowingly or recklessly post, transmit, or distribute false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.

3. Users will not use the school district digital systems or technologies to engage in any illegal act or violate any local, state, or federal statute or law.

4. Users will not use the school district digital system or technologies to vandalize, damage, or disable the property of another person or organization, will not make deliberate attempts to degrade or disrupt equipment, software, or system performance by spreading computer viruses or by any other means, will not tamper with, modify, or change the school district system software, hardware, or wiring or take any action to violate the school district's security system, and will not use the school district system in such a way as to disrupt the use of the system by other users.

5. Users will not use the school district system to gain unauthorized access to information resources or to access another person's materials, information, or files without the implied or direct permission of that person.

6. Employees will not use the school district's digital systems or technology to publicly post private educational or personnel data about a student, a district employee, or themselves including, but not limited to, addresses, telephone numbers, identification numbers, account numbers, access codes or passwords, labeled photographs, or other information that would make the individual's identity easily traceable.

   a) This paragraph does not prohibit the posting of employee contact information on school district webpages or communications between employees and other individuals when such communications are made for education-related purposes (i.e., communications with parents or other staff members related to students).

   b) Employees creating or posting school-related webpages may include personal contact information about themselves on a webpage. However, employees may not post personal contact information or other personally identifiable information about students unless:

      (1) such information is classified by the school district as directory information and verification is made that the school district has not received notice from a parent/guardian or eligible student that such information is not to be designated as directory information in accordance with Policy 515 and related appendices; or

      (2) Such information is not classified by the school district as directory information but written consent for release of the information to be posted has been obtained from a parent/guardian or eligible student in accordance with Policy 515 and related appendices.

      (3) In addition, prior to posting any personal contact or personally identifiable information on a school-related webpage, employees shall obtain written approval of the content of the postings from the building administrator.

   c) These prohibitions specifically prohibit a user from utilizing the school district system to post private information about a user or another individual on social media networks.

7. Students are prohibited from using the school district systems and technology in a manner that invades the privacy of others or compromises other users credentials. This includes but is not limited to disclosing private information such as addresses, telephone numbers, identification numbers, account numbers, access codes or passwords.

8. Users will not use the school district system to violate copyright laws or usage licensing agreements, or otherwise to use another person's property without the person's prior approval or proper citation, including the downloading or exchanging of pirated software or copying software to or from any school computer, and will not plagiarize works they find on the Internet.

9. Users will not use the school district system for conducting business, for unauthorized commercial purposes, or for financial gain unrelated to the mission of the school district. Users will not use the school district digital systems or technologies to offer or provide goods or services or for product advertisement. Users will not use the school district system to purchase goods or services for personal use without authorization from the appropriate school district official.

10. Users will not use the school district system to engage in bullying or cyberbullying in violation of the school district's Bullying Prohibition Policy - 514 or Prohibition Against Discrimination, Harassment and Violence – Policy 413. This prohibition includes using any technology or other electronic communication off school premises to the extent that student learning or the school environment is substantially and materially disrupted.

11. Users may not use school district systems or technology to directly or indirectly advance or advocate against a ballot proposition or the election of any person to public office. This provision only applies to local, state or federal elections which are regulated under state or federal law.

B. A student or employee engaging in the foregoing unacceptable uses of the Internet when off school district premises or by use of personal digital technology also may be in violation of this policy as well as other school district policies. Examples of such violations include, but are not limited to, situations where the school district digital system or digital technologies are compromised or if such use creates a substantial disruption to the educational or work environment. If the school district receives a report of an unacceptable use originating from a non-school computer or resource, the school district may investigate such reports. 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 school district computer system and the Internet and discipline under other appropriate school district policies, including suspension, expulsion, exclusion, or termination of employment.

C. If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the inadvertent access to a teacher, advisor or principal (in the case of students) or to their immediate supervisor and/or the building administrator (in the case of a school district employee or other users).

VIII. Privacy Expectations

A. The school district maintains control of the materials on its digital systems and technologies. Users should not expect privacy in the contents of personal files on the school district digital systems and technologies. Files stored on district computers and servers should not be considered the private property of individuals and may be viewed by supervisory school employees or other authorized representatives of the district.

B. Routine maintenance and monitoring of school district systems may lead to a discovery that a user has violated this policy, another school district policy, or the law.

C. An individual investigation or search may be conducted if school authorities have a reasonable suspicion that the search will uncover a violation of law or school district policy.

D. Parents have the right to request the termination of their child's individual account at any time.

E. School district employees and students should be aware that the school district retains the right at any time to investigate or review the contents of their files and email files. In addition, school district employees and students should be aware that data and other materials in files maintained on the school district system may be subject to review, disclosure or discovery under Minn. Stat. Ch. 13 (the Minnesota Government Data Practices Act).

F. The school district may contact and will cooperate with local, state and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with school district policies conducted through the school district systems.

IX. Social Media

The School Board recognizes the unique characteristics of online social media and/or networks. When social media are used in the classroom or for related school activities, teachers or the responsible employee must ensure compliance with applicable terms of the media site and adhere to all relevant District policies and procedures.

Users should be aware that the unacceptable uses outlined in this policy as well as behavioral expectations identified in Osseo Area Schools policies apply to school related social media use.

To ensure that there are student curriculum materials and structured learning experiences that address proper social media use and general internet safety, the district will work with media specialists and other staff members to create, modify, and continually review appropriate curriculum materials and learning experiences.

To assist employees with social media use and expectations, guidelines for employee use of online social media will be formulated from the superintendent or superintendent designee and provided to employees.

X. Limitations on school district liability

The district assumes no responsibility for any loss or corruption of data resulting from the use of district digital technologies and digital systems. The school district will not be responsible for financial obligations arising through unauthorized use of the school district digital systems, digital technologies, or digital resources.

XI. Consequences for Violation of Policy

Users who use district digital technologies, digital systems, or digital resources in violation of this policy are subject to discipline including but not limited to revoked access, suspension, expulsion, and termination of employment.

XII. User Notification

All users shall be notified of the policies related to the use of district digital resources, technologies, and systems.

Policy Revised 04/16/2019
Policy Revised: 07/29/2014
Policy Revised: 01/08/2013
Policy Revised 11/27/2012
Policy Revised: 5/2/06
Policy Revised 10/15/2002
Policy 441 Adopted: 5/4/99 (formerly Policy 4132 & 4232)

Policy Adopted 04/15/97

Cross References:
Policy 652 – Instructional Materials Selection and Production
Policy 654 – Instructional Materials Re-evaluation, Selection, Production, and Re-evaluation
Policy 524 – Internet Acceptable Use and Safety Policy 506 – Student Discipline

Legal References
17 U.S.C. 101 et seq. (Copyrights)
15 U.S.C. 6501 et seq. Children's Internet Protection Act of 2000 (CIPA)
47 U.S.C. 254 47 C.F.R. 54.250 (FCC rules implementing CIPA)
Title III of the Elementary and Secondary Education Act of 1965, 20 U.S.C. 1601, et seq., as amended
Minn. Stat. § 125B.15 United States v. American Library Association, 123 S. Ct. 2297 (2003)

Notification Statement School Board INDEPENDENT SCHOOL DISTRICT 279 Maple Grove, Minnesota