# St. Joseph Public Schools Bylaws & Policies

# 7540 - TECHNOLOGY

The Board of Education is committed to the effective use of technology to both enhance the quality of student learning and the efficiency of District operations.

Students' use of District Technology Resources (see definitions in Bylaw 0100) is a privilege, not a right. Students and their parents must sign and submit a *Student Technology Acceptable Use and Safety* form annually. (See also, Policy 7540.03)

The Superintendent shall develop a written District Technology Plan (DTP). One (1) of the primary purposes of the DTP is to evaluate new and emerging technologies and how they will play a role in student achievement and success and/or efficient and effective District operations. The Board will financially support, as the budget permits, the DTP, including recommendations to provide new and developing technology for students and staff.

The DTP shall set forth procedures for the proper acquisition of technology. The DTP shall also provide guidance to staff and students about making safe, appropriate and ethical use of District Technology Resources, as well as inform both staff and students about disciplinary actions that will be taken if its Technology Resources are abused in any way or used in an inappropriate, illegal, or unethical manner. See Policy 7540.03 and AG 7540.03 - Student Technology Acceptable Use and Safety, and Policy 7540.04 and AG 7540.04 – Staff Technology Acceptable Use and Safety.

The Superintendent, in conjunction with the Technology Director, shall review the DTP and report any changes, amendments, or revisions to the Board annually.

This policy, along with the Student and Staff Technology Acceptable Use and Safety policies, and the Student Code of Conduct, further govern students' and staff members' use of their personal communication devices (see Policy 5136 and Policy 7530.02). Users have no right or expectation of privacy when using District technology resources (including, but not limited to, privacy in the content of their personal files, e-mails and records of their online activity when using the District's computer network and/or Internet connection).

Further safeguards shall be established so that the Board's investment in both hardware and software achieves the benefits of technology and inhibits negative side effects. Accordingly, students shall be educated about appropriate online behavior including, but not limited to, using social media to interact with others online; interacting with other individuals in chat rooms or on blogs; and, recognizing what constitutes cyberbullying, understanding cyberbullying is a violation of Board policy, and learning appropriate responses if they experience cyberbullying.

For purposes of this policy, social media is defined as Internet-based applications that facilitate communication (e.g., interactive/two-way conversation/dialogue) and networking between individuals or groups. Social media is "essentially a category of online media where people are talking, participating, sharing, networking, and bookmarking online. Most social media services encourage discussion, feedback, voting, comments, and sharing of information from all interested parties." [Quote from Ron Jones of Search Engine Watch] Social media provides a way for people to stay "connected or linked to

other sites, resources, and people." Examples include Facebook, Twitter, Instagram, webmail, text messaging, chat, blogs, and instant messaging (IM). Social media does not include sending or receiving e-mail through the use of District-issued e-mail accounts.

Staff may use social media for business-related purposes. Authorized staff may use District Technology Resources to access and use social media to increase awareness of District programs and activities, as well as to promote achievements of staff and students, provided the Superintendent approves, in advance, such access and use. Use of social media for business-related purposes is subject to Michigan's public records laws and staff members are responsible for archiving their social media and complying with the District's record retention schedule. See Policy 8310 – Public Records and AG 8310A – Public Records.

Instructional staff and their students may use District Technology Resources to access and use social media for educational purposes, provided the Principal approves, in advance, such access and use.

Students must comply with Policy 7540.03 and Policy <u>5136</u> when using District Technology Resources to access and/or use social media. Similarly, staff must comply with Policy 7540.04 and Policy 7530.02 when using District Technology Resources to access and/or use social media.

It is policy of the District to:

- A. prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;
- B. prevent unauthorized access and other unlawful online activity;
- C. prevent unauthorized online disclosure, use, or dissemination of person identification information of minors;
- D. comply with the Children's Internet Protection Act (Pub. L. No. 106-554 and 47 USC 254(h)).

## **Definitions**

Key terms are as defined in the Children's Internet Protection Act.\*

#### Access to Inappropriate Material

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, or access to inappropriate information.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other law purposes.

### **Inappropriate Network Usage**

To the extent practical, steps shall be taken to promote the safety and security of users of the St. Joseph Public Schools online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children's Internet Protection Ace, prevention of inappropriate network usage includes:

- A. unauthorized access, including so-called "hacking," and other unlawful activities;
- B. unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

## **Education, Supervision and Monitoring**

It shall be the responsibility of all members of the St. Joseph Public schools staff to educate, supervise and monitor appropriate usage of online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Superintendent/Designee.

\*CIPA definitions of terms:

**Technology Protection Measure**. The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:

- A. OBSCENE, as that term is defined in Section 1460 of Title 18, United States Code;
- B. CHILD PORNOGRAPHY, as that term is defined in Section 2256 of Title 18, United States Code;
- C. harmful to minors.

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

- A. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion:
- B. 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 exhibition of the genitals;
- C. taken as a whole, lacks serious literary, artistic, political, or scientific values as to minors.

**Sexual Act; Sexual Contact**. The terms "sexual act" and "sexual contact" have the meanings given such terms in Section 2246 of Title 18, United States Code.

Revised 12/12/16

© Neola 2016