

## Series 3000: Operations, Finance, and Property

### 3100 General Operations

#### *3116 District Technology and Acceptable Use*

The Board will provide students, staff, volunteers, and other authorized users access to the District's technology resources, including its computers and network resources, in a manner that encourages responsible use. Any use of District technology resources that violates federal or state law is expressly prohibited.

##### A. Children's Internet Protection Act

The Board complies with the Children's Internet Protection Act ("CIPA") and directs its administration to:

1. Monitor minors' online activities and use technology protection measures on the District's computers with internet access to block minors' access to visual depictions that are obscene, constitute child pornography, or are 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 as to minors, appeals to a prurient interest in nudity, sex, or excretion;
  - b. depicts, describes, or represents, in a patently offensive way as 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; and
  - c. taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.
2. Use technology protection measures on the District's computers with internet access to block all access to visual depictions that are obscene or that constitute child pornography. The technology protection measures may be disabled by authorized personnel during adult use to enable access to bona fide research or for other lawful purposes. The Superintendent or designee will determine which District personnel are authorized to disable the protection measures.
3. Educate minors about appropriate online behavior, including interacting with other people on social networking websites and chat rooms, as well as cyberbullying awareness and response.
4. Prohibit access by minors to inappropriate matter on the internet.
5. Prohibit unauthorized access, including hacking and other unlawful online activity by minors.

6. Prohibit the unauthorized disclosure, use, and dissemination of personal identification information about minors.
7. Restrict minors' access to materials that are inappropriate for minors. The Board defines materials that are "inappropriate for minors" to include obscene depictions, child pornography, and any other material harmful to minors.
8. Encourage the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communication.

The Superintendent or designee will take steps necessary to implement this Policy and to otherwise comply with CIPA.

## B. Acceptable Use Agreement

The Superintendent or designee will develop, review, and revise as necessary an acceptable use agreement that must be signed before a user is provided access to the District's technology resources. Different acceptable use agreements may be developed based on the user's status. At a minimum, the Superintendent or designee will develop an acceptable use agreement to be signed by each of the following groups:

- adult users, including employees, volunteers, and Board members;
- students in grades 7 and above and their parent/guardian; and
- students in grades 6 and below and their parent/guardian.

The acceptable use agreement must be consistent with this Policy and must include, at a minimum, all of the following:

1. A statement that:
  - a. use of District technology resources is a privilege that may be revoked at any time;
  - b. a user has no expectation of privacy when using District technology resources;
  - c. District technology resources use may be monitored by the District and that the use may be subject to FOIA or disclosure in litigation;
  - d. District technology resources may not be used to bully, harass, or intimidate others;
  - e. misuse of District technology resources may result in loss of access to the resources and potential disciplinary action; and
  - f. the District does not guarantee that the District's technology resources will be error free or uninterrupted.

2. Provisions to protect the integrity of District technology resources, including a requirement that each user only access the resources by using that user's assigned user name and password.
3. A list of what constitutes misuse of District technology resources.
4. A prohibition against:
  - a. accessing other user accounts or files without authorization;
  - b. conducting personal business or activities;
  - c. accessing pornography;
  - d. communicating inappropriately with students;
  - e. accessing or downloading confidential student information which the employee has no legitimate educational need to know; and
  - f. accessing or downloading unauthorized software or programs.
5. A requirement that users report any material that is threatening, harassing, or bullying.
6. A release of all claims and liability against the District for use of District technology resources.

#### C. District Personnel Use

District personnel must comply with Policies 4215 and 4216.

#### D. Public Access to Technology

1. Pursuant to the Michigan Library Privacy Act, each school library offering public access to the internet or a computer, computer program, computer network, or computer system (a "Qualifying School Library") will limit minors to only use or view those terminals that do not receive material that is obscene, sexually explicit, or harmful to minors. Persons age 18 or older, or a minor accompanied by the minor's parent/guardian, may access a school library terminal that is not restricted from receiving such material, if any.
2. Only when a Qualifying School Library offers public access as described in subsection D.1., the District must designate at least 1 terminal that is not restricted from receiving such material and at least 1 terminal that is restricted from receiving such material. Library staff must take steps to ensure that minors not accompanied by a parent or guardian do not access the unrestricted terminal. The Superintendent or designee will determine which employees will implement subsection D in each Qualifying School Library.
3. As used in this Policy, "terminal" means a device used to access the internet or a computer, computer program, computer network, or computer system.

Legal authority: 47 USC 254; MCL 397.602, 397.606

Date adopted: 11/09/2020

Date revised: