**CEDARBURG SCHOOL DISTRICT**
**Board Policy Manual**

363.2

ACCEPTABLE USE OF TECHNOLOGY

## Purpose

The Cedarburg School District provides employees and students opportunities to use technology resources, including the Internet, as tools to support the educational mission of the school district. The Board of Education supports the use of the District's technology resources and believes that access to these resources promotes learning by facilitating collaboration, innovation, and communication that enhances the educational experience for students.

The purpose of this policy is to define the scope of the District technology resources and to provide direction regarding the use or abuse of such resources.

For the purpose of this policy, the term "user" includes employees and students of the District. The term "technology resources" includes, but is not limited to desktop computers, portable computers, tablets, mobile phones, telephones, servers, storage media, handheld devices, network equipment, printers, scanners, software, District network, the Internet Network and Internet resources (including but not limited to email, web sites, blogs, wikis, podcasts, and social networking services) and other services or equipment managed by the District Technology Department. Technology resources are to be used in the interests of the District and for the educational purposes for which they are intended. Users are required to follow the guidelines outlined in this Policy.

## Privileges

Use of District technology resources is a privilege which may be revoked at any time. Users will be held responsible for their actions and obligations.

The following actions are specifically prohibited:

- Accessing, storing, transmitting, or downloading material that is abusive, discriminatory, defamatory, harassing, insulting, offensive, threatening, sexually explicit, pornographic, profane, or obscene.

- Copying and transmitting any confidential or proprietary information or software that is protected by copyright or other laws protecting intellectual property.

- Unauthorized access of other users' accounts, communications, or information.

- Unauthorized recording of audio and/or video of District meetings or proceedings concerning school or District business, including conversations or meetings with

District employees, unless every person present has been notified and agrees to be electronically recorded.

- Use of District technology resources for personal solicitations that are not school related, including commercial, political, and religious activities.

The privilege of the use of technology resources may be revoked by the District at its sole discretion. Users of the District's technology resources will review this policy annually.

**Liability**
The District is not liable for any damage suffered by a user of the system, including but not limited to, loss of data, copyright infringement, or the accuracy or quality of information stored, transmitted, or received. The opinions or views presented in electronic communications are solely those of the author and do not necessarily represent those of the District.

**Security**
Security procedures are of the highest priority to ensure consistent delivery of technology resources. System logins and accounts are to be used only by the authorized owner of the account, for authorized district purposes. Users are prohibited from attempting to disable security measures taken by the District. Users are responsible for all activity on their accounts.

**Privacy**
Users should have no expectation of privacy in the contents of any communications or files stored within District technology resources unless such expectation is granted by law. The District maintains the right to access, inspect, investigate, and monitor all use of District technology resources, including files, communications, and information created or transmitted such as e-mail, text messages, and any other communications or information, at any time, without notice to, or consent of the user.

District employees should be aware that their electronic communications are generally subject to disclosure under Wisconsin's Public Records Law. While there are exceptions, whether a document must be disclosed to the public will be determined by the District and not individual employees. In addition, District employees should be aware that electronic communications regarding individual students may create a student record under FERPA and Wisconsin's Pupil Record.

**Parental Opt-Out Provision for Students**
The District will provide students access to technology resources, including the Internet, unless the parent/guardian notifies the appropriate building principal in writing that the District should prevent access to technology resources for his/her student(s). Parents or guardians have the right to view contents of their child's user account or network activity, if possible, accessible and within the confines of applicable law, or to revoke their child's technology permissions, upon written request.

**CIPA (Children's Internet Protection Act)**
It is the Policy of the School District of Cedarburg to : (a) prevent access to or transmission of inappropriate content in its computers and over its network through electronic mail or other forms of communication; (b) promote the safety and security of minors using the District's computers, electronic mail, chat rooms, text messaging, instant messaging and other forms of communications; (c) prevent unauthorized access (such as "hacking") and other unlawful activities; (d) prevent unauthorized online disclosure, use, or dissemination of student personally identifiable information; and (e) comply with CIPA – the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)] and all other applicable laws.

The District uses an Internet content filtering system to limit access to material that is harmful to students, obscene or disruptive to the educational or work environment, or deemed security risk activities. The District uses software designed to filter and block access to pornographic Internet sites. The District uses commercially reasonable technology protection measures designed to comply with CIPA's requirements. The District reserves the right to block sites that do not enhance educational activities or are not in compliance with CIPA. No technology measure can block 100% of inappropriate content so the District emphasizes the importance of responsible use and of parent and staff supervision in monitoring use of technology.

**Education, Supervision and Monitoring**
It shall be the responsibility of all instructional members of the District and parents to educate, supervise, and monitor appropriate use of the online computer network and access to the Internet in accordance with this Policy.

The District will promote safe online activity for students and educate students about appropriate online behavior, including interacting with other individuals on social networking websites and cyberbullying awareness and response. This includes, but is not limited to:

- Teaching students how to locate and evaluate appropriate electronic sources;
- Teaching students information literacy skills, including understanding of safety, copyright, ethical practice and data privacy; and,
- Teaching students proper safety procedures when using e-mail, social networking websites, texting, and other forms of direct electronic communication.

Home and personal Internet or other communication tool technology use can have an impact on the District, school, and others. If Internet expression creates a substantial disruption at school, offenders may be subject to school disciplinary action and/or legal action. Substantial disruption includes, but is not limited to, any of the following:

- Necessary cessation of instruction or educational activities;
- Inability of students or educational staff to focus on learning or function as an educational unit because of a hostile environment (including cyberbullying);
- Severe or repetitive disciplinary measures are needed in the classroom or during educational activities;

- Exhibition of other behavior by students that substantially interfere with the learning environment;
- Threatening acts or behavior to personnel and students; or,
- Endangering the health and safety of others.

Internet expression that creates a substantial disruption at school is a violation of this Policy and may be a violation of other District policies, guidelines and rules.

**Personal Software**
Installation and use of personal software on District technology devices is generally prohibited.

**Non-District-Provided Technology**
The District allows the use of portable personal technology devices by users in support of teaching and learning. Personal technology devices include, but are not limited to: portable computers, tablets, mobile phones, iPods/MP3 players, digital cameras, storage devices, or other electronics that may be carried on a person.

Personal technology devices are permitted as long as they do not interfere with educational or employment responsibilities nor hinder or disrupt classroom activities, nor consume an unreasonable amount of network resources, or violate state laws, federal, laws, or Board policies.

The District is in no way obligated to provide service on personal technology devices. In the event that the District deems it in its best interest to provide such a service, the District shall not be held liable or responsible for any potential repairs that have been caused by such service. The District is not liable for the loss, damage, or misuse of any personal device while on District property or while attending school-sponsored activities. Users that make use of personal technology devices must follow all rules and guidelines of this Policy.

District Principals may establish specific guidelines regarding scope of permissible use of personal technology devices in their buildings. These guidelines shall not be less restrictive than the direction given by this policy.

In accordance with Policy 731.1, Privacy in School Locker Rooms and Restrooms, cameras, video recorders, cell phones or other personal technology devices may not be used in locker rooms or restrooms. Personal technology devices may not be used to record or capture images or sound in a locker room or restroom at any time.

**Consequences**
Inappropriate use of the District's technology resources may result in suspension of technology privileges, reporting to criminal authorities, District legal action, and/or discipline up to and including discharge for employees, or expulsion for students. Additionally, violations may result in financial charges for repair, replacement or services.

Appeals may be made in accordance with appropriate Board policies, procedures, employee contracts, and student handbooks. Administrators may confiscate and search student personal devices while on District property if the administrator has reasonable suspicion that the use of the device or technology is in violation of this Policy. The District will cooperate fully with local, state, or federal officials regarding any investigation related to illegal activities involving District technology resources.

LEGAL REF.: Sections 120.12(1) Wisconsin Statutes
120.44
943.70
947.0125
Chapter 19, Subchapters II and IV
PL 94-0553 (Federal Copyright Law)
Children's Internet Protection Act

CROSS REF.: 347-Rule, Procedures for the Maintenance and Confidentiality of Student Records
411.1, Harassment
731.1, Privacy in School Locker Rooms and Restrooms
771.1, Use of Copyrighted Material
823, Access to Public Records

APPROVED: November 17, 1998

REVISED: April 14, 2003
August 15, 2005
April 28, 2014