Policy 363.2

NORTH CAPE SCHOOL DISTRICT

INTERNET SAFETY AND ACCEPTABLE USE OF TECHNOLOGY

Consistent with applicable federal laws, the School Board believes that the best approach to student safety as it relates to use of the Internet and other electronic resources involves a combination of technology protection measures, monitoring and instruction.

It shall be the responsibility of the District Administrator, or his/her designee, to:

1. Ensure that the District's systems and equipment that provide access to the Internet make active use of technology protection measures designed to block or filter Internet access to visual depictions that are:

   a. obscene;
   b. pornographic; or
   c. otherwise harmful to minors.

   Filtering, blocking or other protective technologies will also be used to decrease the likelihood that student users of the District systems and equipment might access other materials or communications, other than visual depictions, that are inappropriate for students. Recognizing that filtering devices will not filter all inappropriate content and that there will always be room for possible improvement in connection with the District's efforts at prevention, all employees, parents/guardians, and students are encouraged to report to school officials any complaints or concerns regarding student access or exposure to any content, activities or communications that may be harmful, deceptive, or otherwise inappropriate or objectionable.

2. Develop and implement procedures that provide for the monitoring of students' and other authorized users' activities when using District-provided equipment or District-provided network access or Internet access. Such monitoring may sometimes take the form of direct supervision of students' online activity by school personnel, but the Board recognizes that constant, direct supervision is not a practical expectation.

3. Ensure that all employees supervising students who use the District's technology resources educate students about acceptable and responsible use of technology and safe and appropriate online behavior, including (a) safety and security issues that arise in connection with various forms of electronic communication (such as e-mail, instant messaging, and similar technologies); (b) interacting with other individuals on social networking sites and in chat rooms; and (c) cyberbullying awareness and response. Such educational activities shall include (but shall not consist exclusively of) reinforcement of the provisions of the District's rules regarding students' acceptable and responsible use of technology while at school.

4. Develop and implement rules and procedures concerning the acceptable, safe, and responsible use of the District's Internet access infrastructure and other technology-related District resources by students. These rules and procedures shall:

a. Address and prohibit the unauthorized collection, disclosure, use and dissemination of personal and personally-identifiable information regarding students, as particularly applicable to technology-based resources;
b. Prohibit unauthorized user access to systems, networks and data;
c. Prohibit the use of District resources to access and/or transmit inappropriate or prohibited material via the Internet, electronic mail, or other forms of electronic communications;
d. Prohibit the use of District resources for illegal purposes, in support of illegal activities, or for any other activity prohibited by Board policy.
e. Provide notice to users that there is no District-created expectation of privacy in their use of District technology resources. Accordingly, except where prohibited by state or federal law: (1) the District reserves the ability to track, monitor, and access all data, files, communications, or other material that users create, store, send, delete, receive, or display on or over the District's Internet connection, network resources, file servers, computers or other equipment; and (2) all aspects of any individual's use of the District's technology-related equipment and resources, including any online activities that make use of District-provided Internet access, may be monitored and tracked by District officials; and
f. Provide notice to users regarding possible consequences for violations of the policies, rules and procedures that govern the acceptable, safe, and responsible use of the District's technology-related resources.

5. Ensure that all users of the District's technology-related resources complete and sign an agreement to abide by the District's acceptable use of technology policies, rules and procedures. All such agreements shall be kept on file by the Technology Coordinator.

The Technology Coordinator shall have responsibility for overseeing the day-to-day implementation of the District's policies, rules and guidelines regarding the acceptable, safe, and responsible use of technology resources. The Technology Coordinator, in consultation with the District Administrator as needed, may approve modified levels of Internet filtering/blocking for an individual user account provided that there is a legitimate educational purpose and any changes in access will not compromise the overall adequacy of protections that are in place for student users.

LEGAL REF.: Wisconsin Statutes
Section 120.12(1) [school board duty; care, control and management of school property and affairs of district]
Section 120.13(1) [school board power to adopt conduct rules and discipline students]
Section 120.18(1)(i) [report on technology used in the District]
Section 943.70 [computer crimes]
Section 947.0125 [unlawful use of computerized communication systems]
Section 995.55 [access to personal Internet accounts]
Wisconsin Administrative Code
PI 8.01(2)(k) [integration of technology literacy and skills in curriculum]
Federal Laws and Regulations
Children's Internet Protection Act (CIPA) and Neighborhood Children's Internet Protection Act (NCIPA) [policy and other requirements related to Internet safety]

Protecting Children in the 21st Century Act [Internet safety policy requirement; education of students regarding appropriate online behavior]

Children's Online Privacy Protection Act (COPPA) [parent control over personal information collected by websites from their children]
Enhancing Education Through Technology Act of 2001 [technology plans and other requirements]

CROSS REF.: Policy 330, Curriculum Development and Improvement
347-Rule, Procedures for the Maintenance and Confidentiality of Student Records
Policy 361.1, Selection and Reconsideration of Textbooks and Other Classroom Instructional Materials
Policy 361.2, Selection and Reconsideration of Library Media Center Materials
Policy 363.3, Technology Concerns for Students with Special Needs
Policy 381, Teaching About Controversial Issues
Policy 411.1, Student Harassment and Bullying
Policy 443.5, Student Use of Personal Electronic Communication Devices
Policy 731.1, Locker Room Privacy
Policy 771.1, Use of Copyrighted Materials
Policy 834, Public Wireless Internet Use
District Employee Handbook

POLICY REVISION AND NEW APPROVAL: January 16, 2017

REVISED: