INTERNET SAFETY POLICY
For Brandon Valley School District

I. Introduction

The Children's Internet Protection Act (CIPA), 47 U.S.C. §254(h)(5), and South Dakota Consolidated Statutes Section 22-24-55 require public schools to implement certain measures and actions to ensure that students are restricted from accessing inappropriate materials online using school-owned computers. This policy is adopted to implement these state and federal requirements.

II. Internet Safety

It is the policy of the Brandon Valley School District to protect computer users from harassment and unwanted or unsolicited electronic communications. Any network user who receives threatening or unwelcome electronic communications or inadvertently visits or accesses an inappropriate site shall report such such immediately to a teacher or administrator

A. The organization has implemented a technology protection measure that blocks access to inappropriate matter such as child pornography, obscene material and materials that is harmful to minors.
B. In order to protect their safety and security of its students, network users are prohibited from revealing personal information to other users when engaging in online activities including but not limited to chat rooms, email, social networking web sites.
C. All network users are prohibited from hacking and engaging in any unlawful online activitiy.
D. All network users are prohibited from disclosing or disseminating personal information without proper authorization regarding minors.
E. All network users are prohibited from accessing sites or online materials that are blocked by the technology protection measure.

III. Implementation of Technology Protection Measure

A. All school owned computers (used on campus) must be equipped with a technology protection measure.
B. Adult users may request the Technology Protection Measure to be temporarily disabled in order to conduct bona fide research or for another lawful purpose. The Technology Protection Measure must be re-activated as soon as the adult finishes using the computer for authorized bona fide research or other lawful purpose.

IV. Acceptable Use Policy

Each network user shall be required to sign an Acceptable Use Policy annually in the form prescribed by the Superintendent or his/her designee. The Acceptable Use Policy shall implement this Internet Safety Policy. Violation of this policy and/or the Acceptable Use Policy shall be subject to appropriate discipline and sanctions.

V. Monitoring of Online Activities

It shall be the responsibility of all personnel of this organization to monitor students' online activities and use of the network to ensure that their use is in compliance with CIPA and this Internet Safety Policy.

VI. Cyberbullying and Appropriate Online Education

Students will be educated annually about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response. The implementation of this provision is delegated to the Superintendent who shall report annually to the Board on the educational activities undertaken to comply with this subsection.

VII. Definitions Used in this Policy

A. *Minor:* The term "minor" means any individual who has not attained the age of 17 years.

B. *Obscene:* The term "obscene" is defined as material – (1) the dominant theme of which, taken as a whole, appeals to the prurient interest; (2) which is patently offensive because is affronts contemporary community standards relating to the description or representation of sado-masochistic abuse or sexual conduce; and (3) lacks serious literary, artistic, political, or scientific value.

C. *Child pornography:* The term "child pornography" is a visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

D. *Harmful to minors:* The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that – (i) taken as a whole and with the respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (ii) 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; and, (iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

E. *Technology protection measure:* The term "technology protection measure" means a specific technology that blocks or filters Internet access to the material that is obscene, contain child pornography and/or is harmful to minors.

F. *Computer:* Any electronic device that has the ability to connect to the Internet including, but not limited to, desktop computers, laptop computers, tablet computers, and electronic book readers.

(ADOPTION DATE: October 14, 1996)
(REVISION DATE: August 27, 2001)
(REVISION DATE: January 13, 2004)
(REVISION DATE: July 12, 2004)
(REVISION DATE: June 11, 2007)
(REVISION DATE: August 13, 2012)