Instruction

~~Acceptable Use of~~Access to Electronic ~~Resources~~Networks

Electronic ~~resources~~networks, including~~, but limited to, hardware, software, network access, data files, including virtual files,~~ the Internet ~~resources, social networks, other Web 2.0 resources and personal technology devices,,~~ are a part of the ~~District's~~District's instructional program ~~in order~~and serve to promote educational excellence by facilitating resource sharing, innovation, and communication. ~~-~~The Superintendent ~~or designee~~ shall develop an implementation plan for this policy and appoint ~~a~~ system administrator(s).

~~North Boone~~The School District is not responsible for any information that may be lost~~,~~ or damaged, or become unavailable when using the ~~resources~~network, or for any information that is retrieved or transmitted via the Internet.~~–~~ Furthermore, the District will not be responsible for any unauthorized charges or fees resulting from access to the Internet.

Curriculum and Appropriate Online Behavior

The use of the District's electronic ~~resources~~networks shall: (1) be consistent with the curriculum adopted by the District as well as the varied instructional needs, learning styles, abilities, and developmental levels of the students, and (2) comply with the selection criteria for instructional materials and library resource center materials. ~~—~~As required by federal law and Board policy 6:60, *Curriculum Content*, ~~student~~students will be educated about appropriate online behavior, including but not limited to:~~-~~ (1) interacting with other individuals on social networking websites and in chat rooms, and (2) cyberbullying awareness and response. ~~—~~Staff members may, consistent with the ~~Superintendent's~~Superintendent's implementation plan, use ~~electronic resources~~the Internet throughout the curriculum.

The District's electronic ~~resources, including social networks, are~~ network is part of the curriculum and ~~are~~is not a public forum for general use.

Acceptable Use

All use of the ~~District's~~District's electronic ~~resources~~networks must be: (1) in support of education and/or research, and be in furtherance of the ~~Board of Education's~~goals stated ~~goal~~herein, or (2) for a legitimate school business purpose. Use is a privilege, not a right.~~–~~ Students and staff members have no expectation of privacy in any material that is stored, transmitted, or received via the ~~District's~~District's electronic ~~network~~networks or District computers. ~~-~~General rules for behavior and communications apply when using electronic ~~resources.~~ networks. The ~~District's *Authorization for*~~District's administrative procedure, *Acceptable Use of the District's Electronic* ~~Resource *Access*~~*Networks*, contains the appropriate uses, ethics, and protocol. ~~-~~Electronic communications and downloaded material, including files deleted from a ~~user's~~user's account but not erased, may be monitored or read by school officials.

Internet Safety

~~Each~~Technology protection measures shall be used on each District computer with Internet access. They shall ~~have~~include a filtering device that ~~blocks entry~~protects against Internet access by both adults and minors to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by ~~the Children's Internet Protection Act~~federal law and as determined by the Superintendent or designee. ~~—~~The Superintendent or designee shall enforce the use of such filtering devices.~~-~~ An administrator, supervisor, or other authorized person may disable the filtering device for

bona fide research or other lawful purpose, provided the person receives prior permission from the Superintendent or system administrator. ~~-~~The Superintendent or designee shall include measures in this policy's implementation plan to address the following:

1. Ensure staff supervision of student access to online electronic ~~resources including social networking and other Web 2.0 resources,~~networks,
2. Restrict student access to inappropriate matter as well as restricting access to harmful materials~~;~~,
3. Ensure student and staff privacy, safety, and security when using electronic ~~resources;~~communications,
4. Restrict unauthorized access, including "hacking" and other unlawful activities~~;~~, and
5. Restrict unauthorized disclosure, use, and dissemination of personal identification information, such as, names and addresses.

~~Social Networks, other Web 2.0 Resources and Personal Technologies~~

~~Definitions:~~

~~**Includes** – Means "includes without limitation" or "includes, but is not limited to."~~

~~**Social Network** – Media for social interaction, using highly accessible communication techniques through the use of web-based and mobile technologies to turn communication into interactive dialogue. Examples include Facebook, LinkedIn, MySpace, Twitter, and YouTube.~~

~~**Personal technology** – Any device that is not owned or leased by the District or otherwise authorized for District use and: (1) transmits sounds, images, text, messages, videos, or electronic information, (2) electronically records, plays, or stores information, or (3) accesses the Internet, or private communication or information networks. This includes smartphones, tablet computers and other personal electronic devices.~~

~~Usage and Conduct~~

~~All District employees and students who use personal technology and social media shall:~~

~~1. Adhere to the high standards for appropriate school relationships in policy 5:120, Ethics and Conduct at all times, regardless of the ever-changing social media and personal technology platforms available. This includes District employees posting images or private information about themselves or others in a manner readily accessible to students and other employees that is inappropriate as defined by policy 5:20, Workplace Harassment Prohibited; 5:120, Ethics and Conduct; 7:20, Harassment of Students Prohibited; and the Ill. Code of Educator Ethics, 23 Ill.Admin.Code §22.20.~~

~~2. Use only District-provided or approved methods to communicate with students and their parents/guardians.~~

~~3. Not interfere with or disrupt the educational or working environment, or the delivery of education or educational support services.~~

~~4. Comply with policy 5:130, Responsibilities Concerning Internal Information. This means that personal technology and social media may not be used to share, publish, or transmit information about or images of students and/or District employees without proper approval.~~

~~5. Refrain from using the District's logos without permission and follow Board policy 5:170, Copyright, and all District copyright compliance procedures.~~

~~6. Use personal technology and social media for personal purposes only during non-work times or hours. Any duty-free use must occur during times and places that the use will not interfere with job duties or otherwise be disruptive to the school environment or its operation.~~

~~7. Assume all risks associated with the use of personal technology and social media at school or school-sponsored activities, including students' viewing of inappropriate Internet materials through the District employee's personal technology or social media. The Board expressly disclaims any responsibility for imposing content filters, blocking lists, or monitoring of its employees' personal technology.~~

~~8. Be subject to remedial and any other appropriate disciplinary action for violations of this policy.~~

Authorization for Electronic ~~Resource~~Network Access

Each staff member must sign the ~~District's~~ *Authorization for Access to the District's Electronic ~~Resource Access~~ Networks* as a condition for using the ~~District's~~District's electronic ~~resources~~network. Each student and his or her parent(s)/guardian(s) must sign the *Authorization* before being granted unsupervised use.

All users of the District's computers that access the Internet shall maintain the confidentiality of student records. ~~-~~ Reasonable measures to protect against unreasonable access shall be taken before confidential student information is loaded onto the network.

The failure of any student or staff member to follow the terms of the ~~*Authorization for Electronic Resource Access*~~District's administrative procedure, *Acceptable Use of the District's Electronic Networks*, or this policy, will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

LEGAL REF.: No Child Left Behind Act, 20 U.S.C. §6777.
Children's Internet Protection Act, 47 U.S.C. §254(h) and (~~1~~)l).
Enhancing Education Through Technology Act, 20 U.S.C §6751 et seq.
47 C.F.R. Part 54, Subpart F, Universal Service Support for Schools and Libraries.
720 ILCS 135/0.01.

CROSS REF.: 5:100 (Staff Development Program), 5:170 (Copyright), 6:40 (Curriculum Development), 6:60 (Curriculum Content), 6:210 (Instructional Materials), 6:220 (Bring Your Own Technology (BYOT) Program; Responsible Use and Conduct), 6:230 (Library Media Program), 6:260 (Complaints ~~about~~About Curriculum, Instructional Materials, and Programs), 7:130 (Student Rights and Responsibilities), 7:190 (Student Discipline), 7:310 (Restrictions on Publications)

ADMIN PROC.: 6:235-AP1 (Administrative Procedure – Acceptable Use of the District's Electronic ~~Resources~~Networks), 6:235-AP1, E1 (~~Exhibit –~~ Student Authorization for Access to the District's Electronic ~~Resource Access Student~~Networks), 6:235-AP1, E2 (Exhibit – Staff Authorization for Access to the District's Electronic ~~Resource Access Employee~~Networks)

ADOPTED: November 6, 2001

AMENDED: August 20, 2012