Instruction

Acceptable Use of Electronic Resources Access to Electronic Networks [1]

Electronic networksresources, including but not limited to, the hardware, software, network access, data files including virtual files, Internet resources, social networks, other Web 2.0 resources and personal technology devices, are a part of the District's instructional program and serve to promote educational excellence by facilitating resource sharing, innovation, and communication. [2] The Superintendent shall develop an implementation plan for this policy and appoint system administrator(s). [3]

The North Boone School District is not responsible for any information that may be lost or damaged, or become unavailable when using the network, or for any information that is retrieved or transmitted via the Internet. [4] Furthermore, the District will not be responsible for any unauthorized charges or fees resulting from access to the Internet.

Curriculum

The use of the District's electronic networks resources 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. Staff members may, consistent with the Superintendent's implementation plan, use the Internetelectronic resources throughout the curriculum.

The District's electronic network isresources, including social networks, are part of the curriculum and is are not a public forum for general use. [5]

Acceptable Use [6]

All use of the District's electronic networks resources must be: (1) in support of education and/or research, and be in furtherance of the goals stated herein, or (2) for a legitimate school business

---

The footnotes are not intended to be part of the adopted policy; they should be removed before the policy is adopted.

[1] State or federal law requires this subject matter be covered by policy. State or federal law controls this policy's content. This policy contains an item on which collective bargaining may be required. Any policy that impacts upon wages, hours, and terms and conditions of employment, is subject to collective bargaining upon request by the employee representative, even if the policy involves an inherent managerial right. This policy concerns an area in which the law is unsettled.

A policy on Internet safety is necessary to receive funds under the Elementary and Secondary Education Act, Enhancing Education Through Technology (20 U.S.C. §6751 et seq.) and to qualify for universal service benefits under the Children's Internet Protection Act (47 U.S.C. §254(h) and (l).

[2] This goal is repeated in exhibit 6:235-E2, *Authorization for Electronic Network Access*.

[3] Topics for the implementation plan include integration of the Internet in the curriculum, staff training, and safety issues. The implementation plan can also include technical information regarding service providers, establishing Internet accounts, distributing passwords, software filters, menu creation, managing resources and storage capacity, and the number of dial-up lines or access points for users to connect to their accounts. Another topic is investigation of inappropriate use.

[4] No system can guarantee to operate perfectly or to prevent access to inappropriate material; this policy statement attempts to absolve the district of any liability.

[5] School authorities may reasonably regulate student expression in school-sponsored publications for education-related reasons. Hazelwood School District v. Kuhlmeier, 108 S.Ct. 562 (1988). This policy allows such control by clearly stating that school-sponsored network information resources are not a "public forum" open for general student use but are, instead, part of the curriculum.

[6] This paragraph provides general guidelines for acceptable use regardless of whether Internet use is supervised. The specific rules are provided in exhibit 6:235-E2, *Authorization for Electronic Network Access* (see also footnote 11). This paragraph's application to faculty may have collective bargaining implications.

purpose. Use is a privilege, not a right. [7] Students and staff members have no expectation of privacy in any material that is stored, transmitted, or received via the District's electronic networks or District computers. General rules for behavior and communications apply when using electronic networks. The District's *Authorization for Electronic ~~Network~~ Resource Access* contains the appropriate uses, ethics, and protocol. [8] Electronic communications and downloaded material, including files deleted from a user's account ~~but not erased~~, may be monitored or read by school officials. [9]

Internet Safety [10]

Each District computer with Internet access shall have a filtering device that blocks entry to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by federal law and as determined by the Superintendent or designee. [11] 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. [12]

The footnotes are not intended to be part of the adopted policy; they should be removed before the policy is adopted.

[7] The "privilege, not a right" dichotomy is borrowed from cases holding that a student's removal from a team does not require due process because such participation is a privilege rather than a right. The deprivation of a privilege typically does not trigger the Constitution's due process provision. Clements v. Board of Education of Decatur Public School District No. 61, 478 N.E.2d 1209 (Ill.App.4, 1985). Nevertheless, before access privileges are revoked, the user should be allowed to give an explanation.

[8] If students are allowed only supervised access and are not required to sign the *Authorization for Electronic Network Access*, the provisions from the *Authorization* should be used as administrative procedures for covering student Internet use. See *Acceptable Use of Electronic Networks*, 6:235-AP. This is an optional sentence:

> The Superintendent shall establish administrative procedures containing the appropriate uses, ethics, and protocol for Internet use.

The Harassing and Obscene Communications Act criminalizes harassing and obscene electronic communication (720 ILCS 135/0.01).

[9] The Fourth Amendment protects individuals from searches only when the person has a legitimate expectation of privacy. This provision attempts to avoid Fourth Amendment protection for communications and downloaded material by forewarning users that their material may be read or searched, thus negating any expectation of privacy.

Email and computer files are "public records" as defined in the Illinois Freedom of Information Act if they are, as in this policy, "under control" of the school board (5 ILCS 140/2). They may be exempt from disclosure, however, when they contain information that, if disclosed, "would constitute a clearly unwarranted invasion of personal privacy," (5 ILCS 140/7). Alternatively, a school board may believe that making email semi-private enhances its educational value. The following grants limited privacy to email communications and can be substituted for the sample policy's sentence preceding this footnote:

> School officials will not intentionally inspect the contents of email without the consent of the sender or an intended recipient, unless as required to investigate complaints regarding email that are alleged to contain material in violation of this policy or the *Authorization for Electronic Network Access*.

[10] Supra note 1.

[11] This sample policy is broader than the requirements in federal law (20 U.S.C. §6777, 47 U.S.C. §254), in that the policy does not distinguish between minors (children younger than 17) and non-minors. Federal law defines "harmful to minors" as:

> …any picture, image, graphic image file, or other visual depiction that (i) taken as a whole and with 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.

[12] Permitted by 20 U.S.C. §6777(c). The policy's provision for prior approval is not in the law and may be omitted. The entire sentence may be eliminated if a board does not want the filtering device to be disabled.

The Superintendent or designee shall include measures in this policy's implementation plan to address the following: **13**

1. Ensure staff supervision of student access to ~~online~~ electronic ~~networks,~~resources including social networking and other Web 2.0 resources
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 ~~communications~~resources,
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.

The footnotes are not intended to be part of the adopted policy; they should be removed before the policy is adopted.

13 In order to qualify for universal service benefits under the federal Children's Internet Protection Act, the district's Internet safety policy must address the items listed in the sample policy (47 U.S.C. §254(l). The sample policy accomplishes this task by requiring these items be addressed in the policy's implementation plan or administrative procedure. Note that federal law requires the school board to hold at least one hearing or meeting to address the Internet safety policy.

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 ~~Network~~ Resource Access **14**

Each staff member must sign the District's *Authorization for Electronic ~~Network~~ Resource Access* as a condition for using the District's electronic ~~network~~resources. Each student and his or her parent(s)/guardian(s) must sign the *Authorization* before being granted ~~unsupervised~~ use. **15**

All users of the District's computers ~~to 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 ~~Network~~ Resource Access*, or this policy, will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

The footnotes are not intended to be part of the adopted policy; they should be removed before the policy is adopted.

14 The *Authorization for Electronic Network Access* (6:235-E2), rather than this board policy, specifies appropriate conduct, ethics, and protocol for Internet use. This is consistent with the principle that detailed requirements are not appropriate for board policy; instead, they should be contained in separate district documents that are authorized by board policy. Keeping technical rules specifying acceptable use out of board policy will allow for greater flexibility, fewer changes to the policy manual, and adherence to the belief that board policy should be confined to governance issues and the provision of guidance on significant district issues.

15 The Superintendent's implementation plan should describe appropriate supervision for students on the Internet who are not required, or refuse, to sign the *Authorization*.

LEGAL REF.: No Child Left Behind Act, 20 U.S.C. §6777.
Children's Internet Protection Act, 47 U.S.C. §254(h) and (l).
Enhancing Education Through Technology Act, 20 U.S.C §6751 et seq.
720 ILCS 135/0.01.

CROSS REF.: 5:100 (Staff Development Program), 5:120 (Ethics and Conduct), 5:170 (Copyright), 5:200 (Terms and Conditions of Employment and Dismissal), 6:40 (Curriculum Development), 6:210 (Instructional Materials), 6:230 (Library Media Program), 6:260 (Complaints 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-AP (Administrative Procedure - Acceptable Use of Electronic ~~Networks~~Resources), 6:235-E2 (Exhibit - Authorization for Electronic ~~Network~~ Resource Access)