Instruction

Access to Electronic Networks

Electronic networks, including the Internet, are a part of the District's instructional program in order 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 Director of Technology.

The School District is not responsible for any information that may be lost, damaged, or unavailable when using the 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 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-media center materials. As required by federal law and Board policy 6:60, *Curriculum Content,* 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) cyber-bullying awareness and response. Staff members may, consistent with the Superintendent's implementation plan, use the Internet throughout the curriculum.

The District's electronic network is part of the curriculum and is not a public forum for general use.

Acceptable Use

All use of the District's electronic network must be (1) in support of education and/or research, and be in furtherance of the Board of Education's stated goal, 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 electronic network or District computers. General rules for behavior and communications apply when using electronic networks. The District's *Authorization for Electronic Network Access* contains the appropriate uses, ethics, and protocol. Electronic communications and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by school officials.

Internet Safety

Technology protection measures shall be used on each District computer with Internet access. They shall include a filtering device that 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 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. Limiting student access to inappropriate matter as well as restricting access to harmful materials;
2. Student safety and security when using electronic communications;
3. Limiting unauthorized access, including "hacking" and other unlawful activities; and
4. Limiting unauthorized disclosure, use, and dissemination of personal identification information.

Authorization for Electronic Network Access

Each staff member must sign the District's *Authorization for Electronic Network Access* as a condition for using the District's electronic 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 and means of Internet access 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 Access*, or this policy, will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

LEGAL REF.: Children's Internet Protection Act, 47 U.S.C. § 254(h) and (l).
No Child Left Behind Act, 20 U.S.C § 6777.
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 for Publication or Sale of Instructional Materials and Computer Programs Developed by Employees), 6:40 (Curriculum Development), 6,60 (Curriculum Content), 6:210 (Instructional Materials), 6:230 (Enrichment Learning Center), 6:260 (Complaints About Curriculum, Instructional Materials, and Programs), 7:130 (Student Rights and Responsibilities), 7:190 (Student Discipline), 7:310 (Publications)

ADOPTED: December 17, 2001

R: 08/12

Instruction

Authorization for Internet Access

Each teacher must sign this Authorization as a condition for using the District's Electronic Network connection. Each student and his or her parent(s)/guardian(s) must sign the Authorization before being granted unsupervised access. School Board members and administrators are treated like teachers for purposes of this Authorization. Please read this document carefully before signing.

All use of the Internet shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. This *Authorization* does not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. **The failure of any user to follow the terms of the *Authorization for Electronic Network Access* will result in the loss of privileges, disciplinary action, and/or appropriate legal action.** The signature(s) at the end of this document is legally binding and indicates the party who signed has read the terms and conditions carefully and understands their significance.

Terms and Conditions

1. Acceptable Use - Access to the District's electronic networks must be (a) for the purpose of education or research, and be consistent with the educational objectives of the District or (b) for a legitimate business use.

2. Privileges - The use of the District's electronic networks is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The system administrator will make all decisions regarding whether or not a user has violated this *Authorization* and may deny, revoke, or suspend access at any time; his or her decision is final.

3. Unacceptable Use - You are responsible for your actions and activities involving the network. Some examples of unacceptable uses are:

   a. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or State law;
   b. Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused;
   c. Downloading copyrighted material for other than personal use;
   d. Using the network for private financial or commercial gain;
   e. Wastefully using resources, such as file space;
   f. Gaining unauthorized access to resources or entities;
   g. Invading the privacy of individuals;
   h. Using another user's account or password;
   i. Posting material authored or created by another without his/her consent;
   j. Posting anonymous messages;
   k. Using the network for commercial or private advertising;
   l. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and
   m. Using the network while access privileges are suspended or revoked.

4. Network Etiquette - You are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

   a. Be polite. Do not become abusive in your messages to others.
   b. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
   c. Do not reveal the personal addresses or telephone numbers of students or colleagues.
   d. Recognize that electronic mail (E-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
   e. Do not use the network in any way that would disrupt its use by other users.
   f. Consider all communications and information accessible via the network to be private property.
   g. All diskettes and CDs brought into school must receive authorization from the building principal or designee to determine relevance to the school curriculum. Further all diskettes and CDs will be scanned for viruses prior to use on district equipment.

5. No Warranties - The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages you suffer. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or your errors or omissions. Use of any information obtained via the Internet is at your own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

6. Indemnification - The user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any breach of this *Authorization*.

7. Security - Network security is a high priority. If you can identify a security problem on the Internet, you must notify the system administrator or Building Principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account without written permission from that individual. Hacking into any network, program, Internet site, or attempts to log-on to the Internet or to our network as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to network.

8. Vandalism - Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.

9. Software programs may not be installed on district equipment or on our network without prior consent of the system administrator.

10. Telephone Charges - The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.

11. Copyright Web Publishing Rules - Copyright law and District policy prohibit the re-publishing of text or graphics found on the Web or on District Web sites or file servers, without explicit written permission.
    a. For each re-publication (on a Web site or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting

how and when permission was granted. If possible, the notice should also include the Web address of the original source.

b. Students and staff engaged in producing Web pages must provide library media specialist with e-mail or hard copy permissions before the Web pages are published. Printed evidence of the status of "public domain" documents must be provided.
c. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the Web site displaying the material may not be considered a source of permission.
d. The "fair use" rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.
e. Student work may only be published if there is written permission from both the parent/guardian and student.

12. Use of Electronic Mail

a. The District's electronic mail system, and its constituent software, hardware, and data files, are owned and controlled by the School District. The School District provides e-mail to aid students and staff members in fulfilling their duties and responsibilities, and as an education tool.
b. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student or staff member to an electronic mail account is strictly prohibited.
c. Each person should use the same degree of care in drafting an electronic mail message as would be put into a written memorandum or document. Nothing should be transmitted in an e-mail message that would be inappropriate in a letter or memorandum.
d. Electronic messages transmitted via the District's Internet gateway carry with them an identification of the user's Internet "domain." This domain name is a registered domain name and identifies the author as being with the School District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of this School District. Users will be held personally responsible for the content of any and all electronic mail messages transmitted to external recipients.
e. Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.
f. Use of the School District's electronic mail system constitutes consent to these regulations.

Students, parent(s)/guardian(s), and teachers need only sign this *Authorization for Electronic Network Access* once while enrolled or employed by the School District

Please detach and return the permission slip below:

I understand and will abide by the above *Authorization for Electronic Network Access*. I further understand that should I commit any violation, my access privileges may be revoked, and school disciplinary action and/or appropriate legal action may be taken. In consideration for using the District's electronic network connection and having access to public networks, I hereby release the School District and its Board members, employees, and agents from any claims and damages arising from my use, or inability to use the Internet.

DATE: _____

_____

USER SIGNATURE

ADOPTED: 12/17/01

General Personnel

Personal Technology and Social Media; Usage and Conduct

Definitions

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

Social media – Media for social interaction, using highly accessible communication techniques through the use of web-based and mobile technologies to turn communication into interactive dialogue. This includes *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 such as BlackBerry®, android®, iPhone®, and other devices, such as iPads® and iPods®.

Usage and Conduct

All District employees 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;* 5:210, *Ethics and Conduct;* 6:235, *Access to Electronic Networks;*7:20, *Harassment of Students Prohibited;* and the Ill. Code of Educator Ethics, 23 Ill.Admin.Code §22.20.
2. Choose a District-provided or supported method whenever possible 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. For District employees, proper approval may include implied consent under the circumstances.
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 and social media.

8. Be subject to remedial and any other appropriate disciplinary action for violations of this policy ranging from prohibiting the employee from possessing or using any personal technology or social media at school to dismissal and/or indemnification of the District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any violation of this policy.

The Superintendent shall:

1. Inform District employees about this with a copy of this policy during the in-service on educator ethics, teacher-student conduct, and school employee-student conduct required by Board policy 5:120, *Ethics and Conduct.*
2. Direct Building Principals to annually:
   a. Provide their building staff with a copy of this policy.
   b. Inform their building staff about the importance of maintaining high standards in their school relationships.
   c. Remind their building staff that those who violate this policy will be subject to remedial and any other appropriate disciplinary action up to and including dismissal.
3. Build awareness of this policy with students, parents, and the community.
4. Periodically review this policy and any procedures with District employee representatives and electronic network system administrator(s) and present proposed changes to the Board.

LEGAL REF.: 105 ILCS 5/21-23 and 5/12-23a.
Ill. Human Rights Act, 775 ILCS 5/5A-102
Code of Ethics for Ill. Educators, 23 Ill.Admin.Code §22.20
Garcetti v. Ceballos, 547 U.S. 410 (2006)
Pickering v. High School Dist. 205, 391 U.s. 563 (1968)
Mayer v. Monroe County Community School Corp., 474 F.3d477 (7th Cir.2007)

CROSS REF.: 5:20 (Workplace Harassment Prohibited), 5:30 (Hiring Process and Criteria), 5:120 (Ethics and Conduct), 5:130 (Responsibilities Concerning Internal Information), 5:150 (Personnel Records), 5:170 (Copyright), 5:200 (Terms and Conditions of Employment and Dismissal), 6:235 (Access to Electronic Networks), 7:20 (Harassment of Students Prohibited), 7:340 (Student Records)

ADOPTED: September 12, 2011

REVIEWED: January 2012

FRANKFORT C.C. SCHOOL DISTRICT 157-C
EMPLOYEE RECEIPT OF BOARD POLICY ON PERSONAL TECHNOLOGY AND SOCIAL MEDIA

I, the individual whose signature appears below, acknowledge receipt of the Board policy 5:125, *Personal Technology and Social Media; Usage and Conduct.* I affirm that I have read the policy and agree to comply with its requirements.

_____
Name (*please print)*

_____ _____
Signature Date