ACCESS TO ELECTRONIC NETWORKS

Electronic networks, including the Internet, are a part of the District's instructional program and serve to promote educational excellence by facilitating resource sharing, innovation, and communication. The Superintendent shall develop an implementation plan for this policy and appoint system administrator(s).

The 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. 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 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 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 networks 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 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 networks 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

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. 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 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 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.

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 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 Access*, or this policy, will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

SOURCE:	Illinois Association of School Boards
ADOPTED:	October 15, 1996
REVISED:	January 19, 1999; March 16, 1999; October 18, 2005; December 19, 2006; and February 16, 2010
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.

ADMINISTRATIVE PROCEDURES

Acceptable Use of Electronic Networks

All use of electronic networks shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. These procedures do not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. **The failure of any user to follow these procedures will result in the loss of privileges, disciplinary action, and/or appropriate legal action.**

Terms and Conditions

1. Acceptable Use - Access to the District's electronic networks must be for the purpose of education or research, and be consistent with the educational objectives of the District.

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 administration will make all decisions regarding whether or not a user has violated this *Authorization* and may deny, revoke, or suspend access at any time.

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 or installing of files, regardless of source;

   c. Using the network for private financial or commercial gain;

   d. Wastefully using resources, such as file space;

   e. Gaining unauthorized access to resources or entities;

   f. Invading the privacy of individuals;

   g. Using another user's account or password;

   h. Posting material authored or created by another without his/her consent;

   i. Posting anonymous messages;

   j. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and

   k. 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 personally identifying information of students or colleagues.

d. Recognize that electronic communications are not private. People who operate the system have access to all information flowing through the system. 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.

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 network, 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. Attempts to log-on to the network as a system administrator or user with higher privileges will result in cancellation of user privileges and possible disciplinary action. Any user identified as a security risk may be denied access to the network.

8. Vandalism - Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as but not limited to:
   a. Any malicious attempt to harm or destroy data of another user or component on the electronic network,
   b. Uploading or creation of computer viruses, spyware or other malicious software,
   c. Removal of any computer part including tags, stickers and logos,
   d. Marking or scratching the computer,
   e. Inserting foreign objects in the computer

9. 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.

10. Copyright Web Publishing Rules - Copyright law and District policy prohibit the republishing 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 specialists 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.

11. Use of Electronic Communications

a. Student use of electronic communications is limited to teacher discretion for academic purposes.

b. Staff use of electronic communications is limited to the fulfillment of their duties and responsibilities, and as an educational tool.

c. The District reserves the right to access and disclose the contents of any information on or flowing through its system, without prior notice or permission from the account's user. Unauthorized access by any student or staff member to an electronic communication is strictly prohibited.

d. Each person should use the same degree of care in drafting an electronic communication as would be put into a written memorandum or document. Nothing should be transmitted in an electronic communication that would be inappropriate in a letter or memorandum.

e. Electronic communications transmitted via the District's Internet gateway carry with them specific identifying information. This information 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 of their electronic communications.

f. Any message received from an unknown sender 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.

12. Unauthorized computer use is defined as
    a. Playing of non-educational games at the discretion of supervising staff.
    b. Electronic messaging without direct teacher consent and supervision.
    c. Accessing internet without permission.
    d. Downloading or installing any file or program without direct permission.
    e. Making changes to backgrounds, screen savers, or other default settings of student use computers.

UNIT 10

HAMILTON COUNTY
COMMUNITY UNIT DISTRICT NO. 10
P.O. Box 369
109 North Washington
McLeansboro, Illinois 62859
(618) 643-2328

IFBG - E1

Letter to Parent(s)/Guardian(s)
Regarding Student Use of the District's Electronic Networks

Dear Parent(s)/Guardian(s):

We now have the ability to enhance your child's education through the use of electronic networks, including the Internet. The electronic networks offer vast, diverse, and unique resources. The District's goal in providing this service is to promote educational excellence by facilitating resource sharing, innovation, and communication. Your authorization is needed before your child may use this resource.

Electronic networks connect many thousands of users and computers throughout the world. Students and teachers may have access to:

- Electronic communications with people all over the world
- Information from government sources, research institutions, and other sources
- Discussion groups
- Many libraries, including the catalog to the Library of Congress, and the Educational Resources Information Clearinghouses (ERIC).

With this educational opportunity also comes responsibility. You and your child should read the enclosed *Authorization for Electronic Network Access* and discuss it together. The use of inappropriate material or language, or violation of copyright laws, may result in the loss of the privilege to use this resource and/or other disciplinary action. Remember that you are legally responsible for your child's actions.

The District takes precautions to prevent access to materials that may be defamatory, inaccurate, offensive, or otherwise inappropriate in the school setting. On an unregulated network, however, it is impossible to control all material and a user may discover inappropriate material. Ultimately, parent(s)/guardian(s) are responsible for setting and conveying the standards that their child or ward should follow. To that end, the School District supports and respects each family's right to decide whether or not to authorize electronic network access.

Please read and discuss the attached *Authorization for Electronic Network Access* with your child. If you agree to allow your child to have an account, sign the *Authorization* form and return it to your school.

Sincerely,

Jeff Fetcho,
Superintendent

AUTHORIZATION FOR ELECTRONIC NETWORK 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 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 electronic networks 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 prescribed 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 for the purpose of education or research, and be consistent with the educational objectives of the District.

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 administration will make all decisions regarding whether or not a user has violated this *Authorization* and may deny, revoke, or suspend access at any time.

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 or installing of files, regardless of source;

    c. Using the network for private financial or commercial gain;

    d. Wastefully using resources, such as file space;

    e. Gaining unauthorized access to resources or entities;

    f. Invading the privacy of individuals;

    g. Using another user's account or password;

    h. Posting material authored or created by another without his/her consent;

    i. Posting anonymous messages;

    j. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and

    k. 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 personally identifying information of students or colleagues.

   d. Recognize that electronic communications are not private. People who operate the system have access to all information flowing through the system. 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.

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 network, 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. Attempts to log-on to the network as a system administrator or user with higher privileges will result in cancellation of user privileges and possible disciplinary action. Any user identified as a security risk may be denied access to the network.

8. Vandalism - Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as but not limited to:
   a. Any malicious attempt to harm or destroy data of another user or component on the electronic network,
   b. Uploading or creation of computer viruses, spyware or other malicious software,
   c. Removal of any computer part including tags, stickers and logos,
   d. Marking or scratching the computer,
   e. Inserting foreign objects in the computer

9. 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.

10. Copyright Web Publishing Rules - Copyright law and District policy prohibit the republishing 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 specialists 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.

11. Use of Electronic Communications

a. Student use of electronic communications is limited to teacher discretion for academic purposes.

b. Staff use of electronic communications is limited to the fulfillment of their duties and responsibilities, and as an educational tool.

c. The District reserves the right to access and disclose the contents of any information on or flowing through its system, without prior notice or permission from the account's user. Unauthorized access by any student or staff member to an electronic communication is strictly prohibited.

d. Each person should use the same degree of care in drafting an electronic communication as would be put into a written memorandum or document. Nothing should be transmitted in an electronic communication that would be inappropriate in a letter or memorandum.

e. Electronic communications transmitted via the District's Internet gateway carry with them specific identifying information. This information 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 of their electronic communications.

f. Any message received from an unknown sender 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.

12. Unauthorized computer use is defined as
    a. Playing of non-educational games at the discretion of supervising staff.
    b. Electronic messaging without direct teacher consent and supervision.
    c. Accessing internet without permission.
    d. Downloading or installing any file or program without direct permission.
    e. Making changes to backgrounds, screen savers, or other default settings of student use computers.

Authorization for Electronic Network Access Form

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.

I understand and will abide by the above *Authorization for Electronic Network Access*. I understand that the District and/or its agents may access and monitor my use of the electronic network, including my electronic communications and downloaded material, without prior notice to me. 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 of, or inability to use the electronic network.

DATE _____

_____

USER (STUDENT OR STAFF) (Please Print) Student ID#

_____

USER (STUDENT OR STAFF) SIGNATURE

(*Required if the user is a student*:)

I have read this *Authorization for Electronic Network Access*. I understand that access is designed for educational purposes and that the District has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the District to restrict access to all controversial and inappropriate materials. I will hold harmless the District, its employees, agents, or Board members, for any harm caused by materials or software obtained via the network. I accept full responsibility for supervision if and when my child's use is not in a school setting. I have discussed the terms of this *Authorization* with my child. I hereby request that my child be allowed access to the District's Internet.

DATE _____

_____

PARENT/GUARDIAN NAME (Please Print)

_____

PARENT/GUARDIAN NAME SIGNATURE

Please return this page only to office