ACCEPTABLE USE OF ELECTRONIC NETWORKS AND RESOURCES AND AUTHORIZATION FOR ELECTRONIC NETWORK AND RESOURCE ACCESS

All use of electronic networks and resources 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.** The signatures on the Authorization for Electronic Network and Resource Access form are legally binding and indicate that the parties who signed have read the terms and conditions carefully and understand their significance.

Terms and Conditions

1. Acceptable Use - Access to the District's electronic networks and resources must be (a) for the purpose of education or research, and be consistent with the educational objectives of the District, or (b) for legitimate school business use.
2. Curriculum – The use of the District's electronic networks and resources shall: 1) be consistent with the curriculum adopted by the District; 2) address the varied instructional needs, learning styles, abilities and developmental levels of the students; and 3) comply with the selection criteria for instructional materials and learning resource center materials. Staff members may use the Internet throughout the curriculum to support adopted learning outcomes.
3. Privileges - The use of the District's electronic networks and resources is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges, disciplinary action, including by not limited to termination of employment or expulsion, and/or appropriate legal action. The system administrator and/or Building Principal will make all decisions regarding whether or not a user has violated these procedures and may deny, revoke or suspend access at any time. The system administrator or Building Principal's decision is final.
4. Unacceptable Use – Any use which disrupts the proper and orderly operation and discipline of schools in the District; threatens the integrity or efficient operation of the District's network or resources; violates the rights of others; is socially inappropriate or inappropriate for a student's age or maturity level; is primarily intended as an immediate solicitation of funds, is illegal or for illegal purpose of any kind; or constitutes gross disobedience or misconduct, is an unacceptable us. Use of the District's network or resources for any unacceptable use will result in a cancellation of privileges, disciplinary action, including but not limited to expulsion or termination of employment, and/or appropriate legal action. The user is responsible for his or her actions and activities involving the network. General rules for behavior and communications apply when using electronic networks and resources. Some examples of unacceptable uses are, but are not limited to, the following:
    a. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any State or federal law;
    b. Unauthorized downloading of software, regardless of whether it is copyrighted or clear of viruses;
    c. Downloading copyrighted material for other than personal use;
    d. Using the network for private financial or commercial gain, including gambling;
    e. Using the network to harass, threaten, intimidate, bully or demean an individual, or group of individuals, because of sex, color, race, religion, disability, national origin or sexual orientation;
    f. Not following District procedures or directives for using resources, such as file space, printing supplies, etc.;
    g. Using resources such as file space, printing supplies, etc., for non-school related projects without prior authorization from the Director of Technology in consultation with the appropriate Building Principal;
    h. Hacking or gaining unauthorized access to files, resources, or entities;
    i. Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature, including a photograph or digital image;
    j. Using another user's account or password, with or without consent from that user;
    k. Posting material authored or created by another without his/her consent;

l. Posting anonymous messages;

m. Using the network for commercial or private advertising;

n. Accessing, viewing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, pornographic, illegal material or any material that may be harmful or inappropriate for students; and

o. Using the network while access privileges are suspended or revoked.

5. Network Etiquette - The user is 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 messages to others.

   b. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.

   c. Do not reveal personal information, including the 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. All information transmitted via the network or Internet should be treated as if it could be read by anyone.

6. No Warranties - The District makes no warranties of any kind, whether express or implied, for the service of providing computer network access to its users, and bears no responsibility for the accuracy or quality of information or services obtained from the computer network or any loss of data suffered in connection with use of the network. The District will not be responsible for any damages any user suffers, including loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or the user's errors, omissions or negligence. Use of any information obtained via the network is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

   The District has acted in good faith and in a reasonable manner in selecting and implementing filtering applications, blocking software, and other technology protection measures to prevent access to material which is obscene, pornographic, or, with respect to use of computer by minors, harmful to minors. Nevertheless, by using the District's network and resources, users acknowledge that such technology measures do not prevent access to all prohibited material, and may prevent access to non-prohibited material. The District assumes no responsibility for access gained or denied by the technology protection measures that have been implemented.

7. Monitoring – All users of the District technology should recognize that mail use, storage capacity, or evening/night/weekend access might be limited for technical reasons. Network administrators may review files and communications to maintain system integrity and to ensure that users are using the system responsibly and in accordance with this policy. Employees should be aware that any digitally recorded information, even that of a personal nature, and/or documented use of District technology may be inspected and could be subject to public disclosure under the Illinois Freedom of Information Act. Users have no expectation of privacy in any material that is stored, transmitted or received via the District's electronic networks or District technology devices. District 113A has the right to access, review, copy, delete, or disclose as allowed by law, any digitally recorded information stored in, or passed through District technology, regardless of the initial intentions of the user, without prior notification or prior consent of the user. Electronic communications and downloaded materials, including files deleted from a user's account but not erased, may be monitored or read by school officials. The Superintendent or his/her designee shall monitor the activities of users visually, via tracking software, logs or remote access at any time. Other monitoring may occur, as necessary.

8. Indemnification - The user agrees to indemnify the School District for any losses, costs, damages, charges or fees, including, but not limited to, telephone charges, long distance charges, per-minute surcharges, equipment or line costs, or attorney fees, incurred by the District and relating to or arising from the user's use of the District's network or resources or any violation by the user of the Policy, these rules and regulations, or other

rules, regulations or other terms or conditions of computer network or resource access promulgated by the Superintendent, Building Principals or the Director of Technology.

9. Security - Network security is a high priority. Users must keep their account name and password absolutely confidential. If a user can identify a security problem on the Internet, the user must notify the system administrator or Building Principal. Attempts to log-on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.
10. 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.
11. Cooperation with Investigations – The District reserves the right to participate and cooperate fully in any investigation requested or undertaken by either law enforcement authorities or a party alleging to have been harmed by the use of the District's network or resources. Evidence of illegal activity may be reported or turned over to appropriate authorities.
12. 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, relating to, or arising from, an individual user's use of the District's network or resources.

    Copyright Web Publishing Rules - Copyright law and District policy prohibit the re-publishing of text or graphics found on the web or on District websites or file servers without explicit written permission.

    a. For each re-publication (on a website 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 obtain and maintain 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 website 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. Named student work may only be published with written consent from the parent/guardian.
13. Enforcement

    The failure of any user to abide by this Acceptable Use of Electronic Network and Resources, or other rules, regulations or other terms or conditions of network and resource access promulgated by the Superintendent, Building Principals, or the Director of Technology, will result in the suspension or revocation of the user's network and resource privileges, disciplinary action, including but not limited to expulsion or termination of employment, and/or appropriate legal action. Network and resource privileges may be suspended or revoked by the Superintendent or Building Principal with the recommendation of the Director of Technology. Disciplinary measures, if any, will be considered and imposed consistent with District discipline policies and contractual agreements. District 113A will cooperate with all law enforcement agencies (local, state and federal) in any investigatory pursuits related to data transmission originating from District 113A networks and servers. There is no guarantee that e-mail generated on or received by District 113A network/services will remain private.
14. Policy Modifications

    The Board of Education may modify the terms and conditions of use and/or the provisions of this Acceptable Use of Electronic Network and Resources policy and its implementing rules and regulations at any time. The Superintendent, Building Principals or Director of Technology may also promulgate additional rules, regulations or other terms or conditions of network or resource access as may be necessary to ensure the safe, proper and efficient operation of the network, resources and the District's schools. Notice of any such modifications or additional rules, regulations or other terms or conditions of access shall be promptly

communicated to all authorized users, including by posting such modification s on the network or in a conspicuous place at access locations (including the District's website). Use of the District's network constitutes acceptance of the terms of the Policy, the implementing rules and regulations, and any additional rules, regulations or other terms or conditions of network or resource access which may have been promulgated by the Superintendent, Building Principals, Director of Technology or their designees.

15. Reporting Suspected Violations of the Acceptable Use Policy

    District 113A mandates that anyone who believes that there is a violation of this policy and its implementing rules and regulations must direct the information to the Director of Technology or Superintendent in writing or via e-mail. If available, the following information should be provided: 1) the exact nature of the alleged violation; 2) how you came to learn of the violation; 3) the date, time and location of the alleged violation; and 4) evidence of the alleged violation.

    If you believe the violation is e-mail related, please do NOT delete, move or change the message in any way. E-mail with full header information provides many of the clues necessary to investigate possible e-mail violations.

16. Use of E-mail

    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 network users in fulfilling their duties and responsibilities, and as an education tool.

    a. 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 user to an electronic mail account is strictly prohibited.
    b. Each person shall 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.
    c. Electronic messages transmitted via the School District's Internet gateway carry with them an identification of the user's Internet "domain." This domain name is a registered 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.
    d. 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.
    e. If an employee's personal electronic device is enabled to access District e-mail, the user acknowledges these parameters: 1) The device may be subject to the Freedom of Information Act; and 2) If the device is lost or stolen, the user must inform the technology department within 24 hours to ensure the confidentiality of District data stored on the device. This will be accomplished by resetting the user's District password or resetting the device to factory settings.
    f. Use of the School District's electronic mail system constitutes consent to these regulations.

<u>Internet Safety</u>

Internet access is limited to only those "acceptable uses" as detailed in these procedures. Internet safety is almost assured if users will not engage in "unacceptable uses," as detailed in these procedures and otherwise follow these procedures. 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 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 designee.

The Superintendent and Building Principals shall implement procedures that address the following:

1. Ensure staff supervision of student access to online electronic networks and 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;
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.

As required by federal law and Board policy, 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.

Authorization for Electronic Network and Resource Access

Each staff member must sign the District's Authorization for Electronic Network and Resource Access as a condition for using the District's electronic network and resources. Each student's parents must sign the Authorization before being granted use.

All users of the District's electronic network and resources 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 and Resource Access 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 (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 130/0.01.

CROSS REF.: 5:100 (Staff Development Program), 5:170 (Copyright), 6:40 (Curriculum Development), 6:60 (Curriculum Content), 6:210 (Instructional Materials), 6:230 (Library Media Program), 6:260 (Complaints About Curriculum, Instructional Materials, and Programs), 7:130 (Student Rights and Responsibilities), 7:190 (Student Discipline), 7:310 (Student Rights and Responsibilities), 7:190 (Student Discipline), 7:310 (Restrictions on Publications)

ADMIN. PROC.: 6:235-AP1 (Administrative Procedure – Acceptable Use of Electronic Networks and Resources),
6:235-AP1, E1 (Student Authorization for Electronic Network and Resource Access),
6:235-AP2, E2 (Exhibit – Staff Authorization for Electronic Network and Resource Access)

ADOPTED: June 19, 2012

Student Authorization for Electronic Network and Resource Access

Required for ALL Students:
Early Childhood and Kindergarten – Grade 8

Our school district has the ability to enhance your child's education through the use of electronic networks and resources, including the Internet. Our goal in providing this service is to promote educational excellence by facilitating resource sharing, innovation, and communication.

The District filters access to materials that may be defamatory, inaccurate, offensive, or otherwise inappropriate in the school setting. If a filter has been disabled or malfunctions it is impossible to control all material and a user may discover inappropriate material. Ultimately, parents/guardians are responsible for setting and conveying the standards that their child or ward should follow, and the School District respects each family's right to decide whether or not to authorize Internet access.

With this education opportunity also comes responsibility. The use of inappropriate material or language, or violation of copyright laws, may result in the loss of the privilege to use this resource. Parents/guardians are legally responsible for their child's actions. If you agree to allow your child to have access to District 113A's electronic network and resources, please sign the *Authorization* that appears on the receipt for the *Code of Conduct and Student Information.*

AUTHORIZATION FOR ELECTRONIC NETWORK AND RESOURCE ACCESS*

Students must have a parent/guardian read and agree to the following before being granted access:

All use of the Internet shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. **The failure of any user to follow the terms of the *Acceptable Use of Electronic Networks and Resources* will result in the loss of privileges, disciplinary action, and/or appropriate legal action.** The signatures of parents/guardians are legally binding and indicate the parties who signed have read the terms and conditions carefully and understand their significance.

By signing the *Authorization* on the handbook receipt, parents/guardians acknowledge their understanding that access is designed for educational purposes and that the District has taken precautions to eliminate controversial material. However, parents/guardians also recognize it is impossible for the District to restrict access to all controversial and inappropriate materials. By signing the authorization, parents/guardians agree to hold harmless the District, its employees, agents, or Board members, for any harm caused by materials or software obtained via the network and accept full responsibility for supervision if and when their child's use is not in a school setting. By signing the handbook receipt section regarding authorization for network and resource access, parents/guardians acknowledge that they have read the Acceptable Use of Electronic Networks and Resources policy contained in this handbook and discussed the rules and procedures with their child/ren. By signing the handbook receipt, parents/guardians hereby request that their child be allowed access to the District's electronic network and resources, including the Internet, and understand that this authorization will be in effect for the current school year. Should a parent/guardian decide to revoke this authorization at a later date, such notification must be made in writing to the child's current Building Principal.

*Electronic network includes, but is not limited to: e-mail, online connections, network usage and internet connections.