Policy - 8410

Non-Instructional Operations

District-Provided Access to Electronic Information, Services and Networks

All use of electronic networks shall be consistent with the District's goal of promoting educational excellence by facilitating resources sharing, innovation, and communication. These procedures do not attempt to state all required or proscribed behaviors by users. However, some specific examples are provided. All users must understand that one user's misuse of the network and Internet access may jeopardize the ability of all users to enjoy such access. 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:

    a. for the purpose of education or research and consistent with the educational objectives of the District; or
    b. for legitimate school 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. Users have no expectation of privacy in any materials that are stored, transmitted, or received via the District's electronic network or District computers. The District reserves the right to monitor, inspect, copy, review and store, at any time and without prior notice, any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. The network system administrator, principals and district administration will make all decisions regarding whether or not a user has violated these procedures. The district may deny, revoke, or suspend access at any time. Violations may result in appropriate discipline.

3. Unacceptable Use – The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable use include, but are not limited to, the following:

    a. Using the network for an 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 software or material, regardless of whether it is copyrighted or devirused, such as file sharing programs;
    c. Using the network for private financial, commercial or political gain;

d. Wastefully using network resources and other technology resources, such as file space;
e. Hacking or gaining unauthorized access to files, resources, or entities;
f. Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of a personal nature about anyone;
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. Using the network for commercial or private advertising;
k. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, illegal material, or Cyber-Bullying;
    i. Cyber-Bullying, defined as: the use of electronic information and communication devices, to include but not be limited to, e-mail messages, instant messaging, text messaging, cellular telephone communications, internet blogs, internet chat rooms, internet postings, and defamatory websites, that:
        1. Deliberately threatens, harasses, intimidates an individual or group of individuals; or
        2. Places an individual in reasonable fear of harm to the individual or damage to the individual's property; or
        3. Has the effect of substantially disrupting the orderly operation of the school.
l. Using the network while access privileges are suspended or revoked.

4. 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. Politeness. The user should not become abusive in messages to others;
    b. The use of appropriate language. Users should not swear or use vulgarities or any other inappropriate language;
    c. Users should not reveal personal information, including the addresses or telephone numbers, of students or colleagues;
    d. Users must recognize that electronic mail (email) 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. Users shall not use the network in any way that would disrupt its use by others;
    f. Communications and information accessible via the network is to be considered private property.
    g. The network and Internet should be used in support of education and research consistent with the purposes of McCall Donnelly Joint School District #421.

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 the user suffers, or guarantee the reliability of the network connection. This includes loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's 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 District for any losses, costs, claims or damages, including reasonable attorney fees, incurred by the District, relating to or arising out of any violation of these procedures. The user or, if the user is a minor, the user's parent(s)/legal guardian(s) agrees to cooperate with the District in the event that a school initiates an investigation of a user's use of his/her access to its computer network and the Internet.

7. Security – Network security is a high priority. If the user can identify a security problem on the network or Internet, the user must notify the system administrator or building principal. The user should not demonstrate the problem to other users. The user will keep his/her account and password confidential. Users are not to use another individual's account. Attempts to log on to the network 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.

8. Vandalism – Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm, damage, remove, or destroy data of another user, computer or network hardware/software, printers, or any other technology hardware or network. This includes, but is not limited to, uploading, creating, or intentionally introducing computer or network viruses.

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 line costs.

10. Supervision – The school will monitor the online activities and Internet access, through direct observation and/or technological means, to ensure that no one is accessing such sites, depictions, or other material that is inappropriate. The system administrator or designee shall enforce the use of such filtering devices.

11. Copyright Web Publishing Rules – Copyright law and District policy prohibit the republishing of text or graphics found on the Web or on District Websites or file servers, without explicit written permission.

a. For each republication (on a Website or file server) of a graphic or 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 the system administrator or instructor with e-mail or hard copy permission before the Web pages are published. Printed evidence of the status of the "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. Students work may only be published if there is written permission from both the parent/guardian and the student. Personally identifiable information concerning students may not be disclosed, or published in any way on the Internet without written permission of a parent or guardian or, if the student is 18 or over, the permission of the student.

12. Use of Electronic Mail – The District's electronic mail system, and its constituent software, hardware, and data files, are owned and controlled by the District. The District provides email to aid users in fulfilling their duties and responsibilities and as an educational 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. Any message received from an unknown sender should be immediately deleted.
    c. The District's electronic mail system is the only email system that can be used on the District's network or computers.
    d. Use of the District's electronic mail system constitutes consent to these regulations.

13. Internet Safety – Internet access is limited to only those "acceptable uses," as detailed in these procedures.

    a. Staff members shall supervise students while students are using District Internet access, computers, hardware/software and or any other technology equipment, to insure that the students abide by the Terms and Conditions contained in these procedures
    b. Each District computer with Internet access has a filtering device that blocks entry to sites that depict, describe, promote, or involve:

(1)Gambling; (2)Criminal Skills; (3)Violence; (4)Hacking; (5)Adult and Sexually Explicit materials; (6)Glamour and Intimate Apparel; (7)Personals and Dating; (8)Remote Proxies; (9)Games; (10)Chat; (11)Streaming Media; or harmful or inappropriate as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee.

c. The system administrator or district administrators shall monitor user Internet access.

Adoption Date:	First Reading:	October 2012	
	Second Reading:	November 2012	Adopted