Administrative Procedure - Acceptable Use of Electronic Networks

Introduction ~ Each staff member, teacher, administrator, Board member, and other designated individuals granted access to District electronic networks must sign the *Authorization for Electronic Networks Access (5.165-E1)* as a condition for using the District's electronic network resources. These resources include, but are not limited to, voice mail, email, the Internet, computers, and other network files or accounts.

All use of the Internet shall be consistent with the District's goal to provide current technology in communications and electronic services to employees and those granted access, in order to promote education, work place efficiency, information sharing, and a cooperative and innovative environment. This *Acceptable Use of Electronic Networks* procedure does not attempt to state all required or proscribed behavior by users; however, some specific examples are provided.

Users who access, transmit, or store inappropriate material or who fail to follow the terms of this procedure and the *Authorization for Electronic Networks Access* are subject to loss of privileges, disciplinary action, and/or legal action.

Scope ~ The smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines, rules and regulations. Internet access is coordinated through a complex association of government agencies as well as regional and state networks. Worldwide access to computers and people may involve the availability of materials considered to be inappropriate, illegal, or of no professional or educational value. On a global network it is virtually impossible to control all materials. However, through a filtering and monitoring system, the District has taken precautions to restrict access to inappropriate materials and protect its users.

Terms and Conditions ~ The reading and acknowledgement of this procedure through the signing of the *Authorization for Electronic Networks Access* is legally binding and indicates that the user has carefully read, understands, and agrees to the terms and conditions given within this procedure.

Privileges ~ The use of electronic information resources is a privilege, not a right. Inappropriate use of these resources may result in disciplinary and/or referral to legal authorities by school administrators. The system administrator(s) will make all decisions regarding whether or not a user has violated the terms of access privileges and may deny, revoke, or suspend access at any time. Incidents of inappropriate use that involve the revocation or suspension of access will be reviewed by the Superintendent and/or designee.

Security ~ Network security is a high priority. If you can identify a security problem on the Internet, you must notify the system administrator(s) or building principal. Do not demonstrate the problem to other users. Keep your account and password confidential. 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.

Network Etiquette ~ District employees and other designated individuals have the responsibility to assure all shared information meets the standards set forth in this *Acceptable Use of Electronics Networks* procedure. Each account holder and user is expected to abide by the generally accepted rules of user etiquette. These include, but are not limited to, the following:

- Be polite. Do not become abusive in your messages to others.

- Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
- Recognize that electronic mail (email) is not private. People who operate the system have access to all mail.
- Consider all communications and information accessible via the network to be private property.

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

Unacceptable Use ~ The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:

- Promoting, or supporting political functions or agenda's in any way, both internally and externally;
- 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;
- Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused;
- Downloading of copyrighted material for other than personal use;
- Using the network in any way that would disrupt its use by other users;
- Intentionally wasting or wastefully using resources, such as file space;
- Engaging in practices that threaten the network (e.g., loading files that may introduce a virus);
- Hacking or gaining unauthorized access to folders, documents, files, resources or entities;
- Invading the privacy of individuals, that includes the unauthorized disclosure, dissemination, and/or use of information about anyone that is of a personal nature including a photograph;
- Sharing confidential information on students or employees unless authorized by District Administrators;
- Revealing personal information, including the addresses or telephone numbers, of students or colleagues;
- Using another user's account or password;
- Posting material authored or created by another without his/her consent;
- Posting anonymous messages;
- Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, pornographic, threatening, racially offensive, harassing, or illegal material;
- Using the network while access privileges are suspended or revoked;
- Advertising products or services not directly related to District functions;
- Using the network for private advertising or financial or commercial gain;
- Promoting, supporting or celebrating religion or religious institutions; and
- Transmission or intentional receipt of any inappropriate material or material in violation of law or District policy.

Vandalism ~ Vandalism is defined as any malicious attempt to harm or destroy property of the user, another user, or of any other agencies or networks that are connected to the network as well as the Internet system. Vandalism also includes, but is not limited to overloading of data on the server as well as the uploading, downloading or creation of computer viruses in an intentional manner. Vandalism is considered a violation of the *Acceptable Use of Electronics Networks*

procedure and as such is subject to disciplinary and/or legal action as deemed appropriate by the administration.

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.

Indemnification ~ The user agrees to indemnify 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 procedure or the *Authorization for Electronic Networks Access*.

Service Disclaimer ~ 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. These damages may include but are not limited to loss of data resulting from delays, non-deliveries, mis-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 users own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Web Publishing Rules ~ Any employee who "publishes" on the District web server must abide by the District's *Web Publishing Guidelines* (5.165-AP2). Illegal or inappropriate publishing activities or uses of any kind that do not conform to the rules, regulations and policies of the District are forbidden.

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.

- 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.
- Students and staff engaged in publishing Web pages that embed or use copyrighted material must provide the district webmaster an email or hard copy permissions before the Web pages are published. Printed evidence of the status of "public domain" documents must be provided.
- 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.
- The "fair use" rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.
- Student work may only be published if there is written permission from both the parent/guardian and student.

Use of Electronic Mail ~ Email accounts provided to the staff, teachers, administrators, Board members, and designated individuals of the District are primarily for internal and external business communications to be used for fulfilling their duties and responsibilities; and as an education tool. Email addresses are not, except upon request, considered private and should be available to the public as deemed appropriate by the administration. Personal use of the District email is allowed, but should not interfere with the day-to-day duties of staff, nor violate Board policies and procedures. It must be the student and staffs' understanding that District provided email is not private or protected. Email correspondence should follow proper network etiquette guidelines found in this procedure.

Spam is defined as email that is sent to multiple individuals in an uninvited manner for purposes of furthering a private and/or political agenda, the transmission of questionable material, or as a means of solicitation. Engaging in internal or external email activities that are regarded as Spam or mass emailing is not permitted, unless for information purposes as approved by District administrators. When suspicion of a violation of this procedure pertaining to inappropriate material or usage exists, either through discovery as part of regular maintenance or by staff complaint, the District reserves the right to review data and files found on email clients and servers during the course of investigation. Any information gained through this review may be used as evidence in disciplinary or legal action should a violation of this procedure exist.

The District's email system, and its constituent software, hardware, and data files, are owned and controlled by the District.

- 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 email account is strictly prohibited.
- Each person should use the same degree of care in drafting an email message as would be put into a written memorandum or document. Nothing should be transmitted in an email message that would be inappropriate in a letter or memorandum.
- 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 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 the District. Users will be held personally responsible for the content of any and all email messages transmitted to external recipients.
- Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrators. 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.
- When suspicion of a violation of the *Acceptable Use of Electronics Networks* procedure pertaining to inappropriate material or usage exists, either through discovery as part of regular maintenance or by staff complaint, the District reserves the right to review data and files found on email clients and servers during the course of investigation. Any information gained through this review may be used as evidence in disciplinary and/or legal action should a violation of this procedure exist.

Use of the District's email system constitutes consent to these regulations.

Internet ~ Any employee who "publishes" on the District web server must abide by the *Web Publishing Guidelines* procedure. Illegal or inappropriate publishing activities or uses of any kind that do not conform to the rules, regulations and policies of the District are forbidden. It is advised to not reveal personal information, such as: home address, phone numbers, password, credit card numbers or social security number; this also applies to others' personal information or that of organizations. Additionally, it is understood that staff who publish personal web pages for educational or curricular use in the classroom outside the District that may be accessed or linked by the District computers must also abide by the same standards of appropriate content that all District hosted web pages must maintain. Sites found to be in violation of this will be blocked administratively and appropriate action taken to ensure the removal of dangerous or libelous content hosted by outside web resource providers. In addition, the administration reserves the right for further and appropriate action in situations where staff personal web pages and/or sites exist that violate the spirit of this procedure.

Internet Safety ~ 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". Each user is responsible for this provision when using the District electronic information resources.

Security on any computer system is a high priority because of multiple users. Do not use another individual's account or log on to the system as the system administrator. Any security concern, as well as changes to user account information must be reported to the principal/supervisor or system administrator(s) at once. Information stored on the network is not to be considered permanent or private. As such, the District retains the right to review and remove as needed data or files found on the network that violates this *Acceptable Use of Electronics Networks* procedure or that are not in direct support of education or business. In addition, regular maintenance activities can result in the deletion of information deemed not compliant with this procedure. When suspicion of a violation of this procedure pertaining to inappropriate material or usage exists, the District reserves the right to review data and files found on the network during the course of investigation. Any information gained through this review may be used as evidence in disciplinary or legal action should a violation of this *Acceptable Use of Electronics Networks* procedure exist.

Filtering, Monitoring, and Review ~ The District, in order to comply with local, state, and federal laws and standards, filters Internet content on systems to which employees or students may have access. This filtering removes access to websites and Internet servers that have been deemed to have inappropriate content not of an educational value. Report any errors found regarding what sites being or not being filtered, immediately to a building administrator or the system administrator(s). The District retains the right to monitor network, email, computer, and telephone use without warning or notice. Information stored, transmitted, or communicated on the District's equipment is not to be considered private. Information gained through monitoring may be used as evidence in disciplinary or legal action, at the administration's discretion. The District retains the right to review current and back-up copies of electronic systems, files, data, communications, and email. Reviews are done without notice, and information gained through review may be used as evidence in disciplinary and/or legal action should a violation of the *Acceptable Use of Electronics Networks* procedure be discovered.

Computer Resources ~ The District provides desktops and/or laptops to staff members and designated individuals on an as needed basis. District provided computers are not to be modified in any way, including the addition or removal of hardware or software, without prior permission from the system administrator(s). District provided computers, other than certified or operationally assigned laptops, may not be removed from District property without prior approval. Removal of District owned equipment is in violation of this procedure and disciplinary or legal action may result. Use of District provided computers or systems to gain personal income or monies is expressly forbidden, unless it is for fundraising activities associated with school and has prior approval from an administrator. This activity is considered a violation of this procedure and subject to disciplinary or legal action as deemed appropriate by District administrators.

■

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).
Enhances Education Through Technology Act of 2001, 20 U.S.C. §6751 et seq.
Harassing and Obscene Communications Act, 720 ILCS 135/0.01.
CROSS REF.: 5.100, 5.170, 6.40, 6.210, 6.230, 6.235, 6.260, 7.310
ADMIN. PROC.: 5.165-AP2, 5.165-E1, 5.165-E2

Adopted: January 26, 2011
Reviewed: June 2011
Amended: July 13, 2011