Instruction

Computer and Network Use Policy

Computers and electronic networks, including the Internet, are a part of the District's instructional program and serve to promote excellence by facilitating resource sharing, innovation, and communication. The District's electronic network is part of the curriculum and is not a public forum for general use.

Full disclosure and understanding in the partnership between parents, students, staff, and volunteers with regard to District technology and its use are essential. This Computer and Network Use Policy is created to ensure that all parties understand their responsibilities. Unless otherwise specified, the following policies apply equally to all District computer and network users, including, but not limited to staff, students, School Board Members, guests, and volunteers.

Each staff member must sign the District's *Computer and Network Use Agreement* as a condition for using the District's computers and network, including the Internet. Each student and his or her parent(s)/guardian(s) must sign the District's *Computer and Network Use Agreement* before the student is granted access. Use of the District's computers and network is a privilege, not a right, and this privilege may be revoked at any time for conduct that violates this Policy.

All individuals with access to District technology and computer networks will:

- Respect the rights and property of others.
- Observe District Board Policies.
- Utilize the computers, network, Internet, and other technologies for purposes supporting the District's educational goals and legitimate District business.
- Take reasonable precautions to prevent loss or damage to equipment and data.
- Install and use software and hardware on the District's computers and network only in accordance with this policy and related procedures.

Interpretation and application of this Policy are within the sole discretion of the District Administration. Any questions or issues regarding this Policy should be directed to the Building or District Administration or the Technology Directors.

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 resource 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) cyberbullying awareness and response. Staff members may, consistent with the Superintendent's implementation plan, use the Internet throughout the curriculum.

User Privacy

No user of the District computer equipment or network has a reasonable expectation of privacy in such use. District Administration or Technology Department personnel may audit, monitor, or review the use of the equipment and network periodically or for a specific cause. Technology Department personnel may see e-mail messages and files during operational procedures or troubleshooting. All

works created or viewed by a user on the District's computers, network, or storage devices are subject to the monitoring and scrutiny of Technology Department personnel and District Administration.

Computer and Network Use Rules

All District policies and rules pertaining to behavior and communication apply to computer and network use. District computer users are expected to act in a responsible, ethical, and legal manner, in accordance with the missions and purposes of the District and the laws of the State of Illinois and the United States.

The following conduct is prohibited on District computers and the District network:

- Any illegal activity, including violation of copyright.
- Deliberate use of malicious code, such as viruses or malware.
- Vandalism or any attempt to harm or destroy data of another user, the Internet, or any other network, including uploading or creating computer viruses.
- Hacking or gaining unauthorized access to files, resources, or entities.
- Use for financial or commercial gain, including the development of Intellectual Property owned by the user.
- Attempting to circumvent any security, content filtering, or traffic management measures implemented by the District.
- Use while access privileges are revoked or suspended.
- Using an account owned by another user without authorization.
- Invading the privacy of any individual or organization.
- Misappropriating or plagiarizing data.
- Intentionally wasting finite resources or degrading or disrupting system performance.
- Unauthorized downloading of software.
- Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material.
- Deliberately attempting to access obscene or inappropriate materials.
- Posting or forwarding personal communications without the author's consent.
- Posting anonymous messages.
- Using abusive or otherwise objectionable language in either public or private messages.
- Harassing, threatening, or intimidating another person.
- Sending chain letters to lists or individuals.
- Unauthorized access to or alteration of any school document.

Network Etiquette and Conscientious Use Guidelines

- Be polite. Do not use abusive, vulgar, or inappropriate language in your messages or posts.
- Exercise caution with personally identifiable information.
- Do not reveal the personal information of others including students or colleagues.
- Student records may not be disclosed to third parties unless disclosure is in accordance with the Illinois School Students Records Act.
- Any student receiving unsolicited requests for personal information should immediately report the request to the supervising teacher. The teacher will report the incident to the appropriate building administrator.
- Do not share your user account information with other individuals or leave your computer logged in unattended.
- Exercise caution with messages or files received from unknown or suspicious senders.

- When bringing in data from outside the District, ensure media is free from viruses. District virus protection software should be used to examine these media before they are used in a District computer.
- Information accessible via the network and Internet should be assumed to be private property and copyrighted unless otherwise stated.
- Broadcast messages must be work-related.

Acceptable Electronic Mail Usage

The District's electronic mail system and its constituent software, hardware, and data files are owned and controlled by the District. The District provides e-mail as an educational tool to aid students and staff members in fulfilling their duties and responsibilities.

- The District reserves the right to access the contents of any account on its system, without prior notice or permission from the account user. Messages relating to or in support of illegal activities may be reported to law enforcement authorities.
- Unauthorized access by any student or staff member to an e-mail account is strictly prohibited.
- Use the same degree of care in drafting an e-mail message as would be used writing a memorandum or letter. Nothing should be transmitted in an e-mail message that would be inappropriate in a letter or memorandum.
- E-mails transmitted via the District's Internet gateway carry an identification of the user's Internet domain, which identifies the author as being with the District. Use care in composing e-mail and consider how the message will reflect on the name and reputation of the District. Users will be held personally responsible for the content of any and all e-mail messages they prepare or send.
- Any message received from an unknown sender should be immediately deleted or forwarded to the Technology Directors. Downloading any file is prohibited unless the user is certain of the nature and authenticity of the file.
- Use of the District's e-mail system constitutes consent to these regulations.

Controlled Access to the Internet

Internet access is provided strictly for use consistent with the District's educational goals. All staff will receive yearly training on the appropriate use of Internet resources. Students will be educated annually about appropriate online behavior, including but not limited to interacting with other individuals on social networking websites and in chat rooms, and cyber-bullying awareness and response.

In accordance with the Children's Internet Protection Act, District monitors Internet access and e-mail use and uses mechanisms such as content filters and firewalls to protect staff and students from obscene, pornographic, and other inappropriate material available on the Internet. Students are not allowed to access the Internet or e-mail without staff supervision and are required to connect to the web through a content filter. Despite these efforts, users may encounter information on the Internet that is controversial or potentially harmful. Some Internet material may contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal content. The District does not condone the use of such materials and does not knowingly permit the use of such materials. Deliberate attempts to access obscene or inappropriate materials by any user will result in disciplinary action by the District Administration.

The Superintendent or the Superintendent's designee shall include measures in this policy's implementation plan to address the following:

- Ensure staff supervision of student access to online electronic networks.
- Restrict student access to inappropriate matter and harmful materials.

- Ensure student and staff privacy, safety, and security when using electronic communications.
- Restrict unauthorized access, including “hacking” and other unlawful activities.
- Restrict unauthorized disclosure, use, and dissemination of personal identification information, such as names and addresses, unless disclosure is required by law.

Security
Network security is a high priority. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the District's computers and network. Any user who feels that he or she can identify a security problem or data breach on the network must immediately notify an Administrator and not demonstrate the problem to others.

Users should always log out of a computer when leaving their work area for extended periods of time and especially at the end of the day. Logging out will prevent others from using your account. Keep your account and password confidential.

Intellectual Property
All works of any kind that an employee or student of the District creates on the District's computers or network shall be deemed “work for hire” (as defined in 17 U.S.C. § 1001(1)) and thus the intellectual property of the District.

For each re-publication of a graphic or text file that was produced externally, the user must provide a notice at the bottom of the page crediting the original producer and noting how and when permission to republish was granted.

Warranties/ Indemnification
The District makes no warranties of any kind, express or implied, in connection with its provision of access to and use of its computers and network. The 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. 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. Users are responsible for backing up their data. 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 on the Internet.

The user agrees to indemnify, defend, and hold harmless 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 and its procedures.

Enforcement
Violation of the rules set forth by this Computer and Network Use Policy may result in disciplinary action by District Administration or the Board of Education. District Administration may suspend some or all privileges associated with computer and network use in cases of misuse. Additional disciplinary action for misuse by students may include, but is not limited to, suspension or expulsion from school, removal from classes requiring computer use, and, if appropriate, criminal prosecution. Additional disciplinary action for misuse by employees and other users may include, but is not limited to, formal reprimand, probation, termination, and, if appropriate, criminal prosecution.

Before any permanent action is taken against a user, the user will be advised of the basis for the proposed action and given an opportunity to respond. The specific disciplinary action for each case will be at the discretion of the District Administration or the Board of Education and may vary depending on the severity of the infraction. Any formal discipline of students or staff shall comport

with existing District policy and procedure. The District will rigorously uphold laws governing the use of the District's computers and network.

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.

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 (Restrictions on Publications)

ADMIN PROC.: 6:235-AP1 (Administrative Procedure – Hardware Procedures), 6:235-AP2 (Administrative Procedure – Software Procedures), 6:235-AP3 (District Website Publishing Guidelines)

Adopted: May 28, 1996

Amended: March 26, 2001
March 26, 2007
June 22, 2009
June 25, 2012
October 22, 2012

■