PERMISSIBLE USE OF DISTRICT TECHNOLOGY

Electronic networks, including the internet, are a part of the District's instructional program. Use of the District's electronic network allows students and staff potential access to electronic mail communication and other forms of electronic communication; to information via the World-Wide Web and other information networks; and to various research sources. The District's network is part of the District 87 curriculum and is not a public forum for general use. Employees shall not load onto the District's electronic network or Internet any student work by which the student may reasonably be identified or District 87 work product (as defined in administrative procedures) without prior approval of the originator, his/her designee, or a school administrator.

The term *electronic networks* includes all technology resources provided by the District, which may include but are not limited to:

1. The District's local-area and wide-area networks, including wireless networks (Wi-Fi), District-issued Wi-Fi hotspots, and any District servers or other networking infrastructure;

2. Access to the Internet or other online resources via the District's networks or to any District-issued online account from any computer or device, regardless of location;

3. District-owned or District-issued computers, laptops, tablets, phones, or similar devices.

The Board of Education denies any responsibility for any information, including its accuracy or quality, obtained or transmitted through use of the District's electronic network. Further, the Board denies responsibility for any information or data that may be lost, damaged, altered or unavailable when using District technology or the District's electronic network. Employees and students shall be solely responsible for any unauthorized charges or fees resulting from their access to the Internet.

Authorized use of the School District's electronic network and the Internet shall be governed by administrative procedures developed by the Superintendent.

A. General

1. Authorized personnel may use District-owned or leased technology (e.g., computers, laptops, tablets, smartphones, and other similar electronic devices) to access the District's electronic network and the Internet for activities related to the school curriculum and co-curricular activities sponsored by the District, for research consistent with the District's educational objectives, and for other administrative tasks. Students may use District technology for activities related to the school curriculum, co-curricular activities sponsored by the District, and for research consistent with the District's educational objectives.

2. Personnel shall not load onto the District's electronic network or Internet District 87 work product without prior approval from the originator, his/her designee, or a school administrator. Students shall not load District 87 work product onto the District's electronic network or Internet without prior approval from a teacher or school administrator. Examples of materials constituting District 87 work product include, but are not limited to: District 87 curriculum, District 87 test or examination materials, Department Guidelines and/or Procedures, Parent/Student Handbooks, Personnel Handbooks, District 87 publications and brochures, school newspaper, school yearbook, District 87 policies and administrative regulations/procedures, and information published on the District's Web site.

3. Personnel shall at all times maintain the confidentiality of student information regardless of how the information is transmitted or received. Additionally, confidential student information should not be loaded onto the District's electronic network where unauthorized access to

such information may be obtained. Student work by which the student may reasonably be identified shall not be loaded into the District's electronic network or "published" on the Internet without prior written consent from the originator, his/her designee, or a school administrator.

4. As a condition of being allowed access to the Internet and the District's electronic communications through use of District technology, personnel and students shall consent to monitoring and inspection by school administration of personnel and students use of District technology including any and all electronic communications made or attempted to be made or received by personnel or students and all materials accessed, uploaded, installed, downloaded or transmitted by personnel and students.

5. Students and staff should have no expectation that any information transmitted on the District's electronic network or stored on District 87 technology is or will remain private.

6. Personnel and students shall not install, upload, or download software without school authorization.

7. Personnel and students shall not use District technology for any illegal activities, including, but not limited to "hacking", copyright and license violations, and unauthorized access to or unauthorized use of databases.

8. Because it is impractical for the District to monitor its electronic network or District's technology for improper or illegal activity at all times, employees and students shall be solely responsible for any improper or illegal activity and/or transaction resulting from their use of same. The School District does not condone, authorize, or approve of use of its electronic network or District technology for any activity which is not related to the school curriculum or co-curricular activities sponsored by the District.

9. Personnel and students shall not use the District's electronic network or District technology for personal financial or commercial gain.

10. Use of the District's electronic communication systems, network, and access to and use of the Internet on District technology is a privilege, not a right. Staff members and students who abuse the privilege by engaging in the conduct prohibited in these procedures may lose the privilege and may be denied access to the network, Internet, and/or the District's electronic mail communication.

B. Internet Safety and Appropriate Online Behavior

1. 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.

2. Technology and the Internet is constantly changing and evolving. Due to the complexities of technology and the Internet, it is impossible to control access to all content, and a user may encounter inappropriate material. The District shall use its best efforts to ensure that technology protection measures are in place for District technology that connects to the District's electronic network. This includes but is not limited to device(s) that block or filter Internet access to visual depictions that are obscene, pornographic, child pornography, or 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 device(s). The Superintendent or designee shall include measures in this policy's implementation plan to address the following:

   a. Staff supervision of student access to online electronic networks,
   b. Student access to inappropriate matter as well as restricting access to harmful materials,

c. Student and staff privacy, safety, and security when using electronic communications,
d. Unauthorized access, including "hacking" and other unlawful activities, and
e. Unauthorized disclosure, use, and dissemination of personal identification information, such as, names and addresses.

C. Use of Electronic Communication

1. The District's electronic network and electronic communication systems shall be used for educational or work purposes only. Personnel and students shall not be allowed to use the District's electronic network or electronic communication systems for anonymous messages or communications unrelated to the school program. Personnel and students shall not use the District's electronic network or electronic communication systems to create, communicate, repeat, or otherwise convey any message or information which is illegal, indecent, obscene, harmful to minors, defamatory, likely to constitute harassment of another staff member, student, or any other individual, likely to cause disruption in the schools, or is otherwise inconsistent with the District's curriculum and educational mission.

2. Staff members and students shall respect the privacy rights of others and shall not attempt to access any electronic communications not directed to them or intended to be received by them.

D. Consequences of Improper or Prohibited Use of District Electronic Network or District Technology

1. Improper or prohibited use of the District's electronic network or District technology by District personnel will result in discipline up to and including dismissal. Criminal conduct will be referred to law enforcement authorities.

2. Improper or prohibited use of the District's electronic network or District technology by students will result in discipline up to and including expulsion. Criminal conduct will be referred to law enforcement authorities.

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 135/0.01

Policy Adopted: 06/25/01
Policy Revised and Number Changed: 09/26/11
Policy Revised: 12/17/12
Policy Revised: 05/18/15
Policy Revised: 07/26/21