INSTRUCTION

Access to Electronic Networks
Electronic networks, including the Internet, are a part of the District's instructional program and serve to promote educational excellence by facilitating resource sharing, innovation, and communication. The Superintendent shall develop an implementation plan for this policy and appoint system administrators.

The School District is not responsible for any information that may be lost or damaged, or become unavailable when using the network, or for any information that is retrieved via the Internet. Furthermore, the District will not be responsible for any unauthorized charges or fees resulting from access to the Internet.

Individual School Board members and administrative staff members shall be treated like teachers.

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-media center materials. As required by federal law and Board policy 6:60, Curriculum Content, students will be educated about appropriate online behavior, including but no 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 District's electronic networks throughout the curriculum.

The District's electronic network is part of the curriculum and is not a public forum for general use.

Acceptable Use
All use of the District's electronic network must be (1) in support of education and/or research, and be in furtherance of the goals stated herein, or (2) for a legitimate business purpose. Use is a privilege, not a right. Students and staff members have no expectation of privacy in any material that is stored, transmitted, or received via the District's electronic network or District computers. General rules for behavior and communications apply when using electronic networks. The District's administrative procedure, Acceptable Use of the District's Electronic Networks, contains the appropriate uses, ethics, and protocol. Electronic communications and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by school officials.

Internet Safety
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 [CIPA] 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 system administrator. The Superintendent or designee shall include measures in this policy's implementation plan to address the following:

1. Limiting student access to inappropriate matter as well as restricting access to harmful materials.
2. Student safety and security when using electronic communications to include but not limited to online behavior including interacting with other individuals on social networking websites and in chat rooms.
3. Limiting unauthorized access, including “hacking” and other unlawful activities.
4. Limiting unauthorized disclosure, use, and dissemination of personal identification information.
5. Cyberbullying awareness and response.
6. Adherence to the Children’s Internet Protection Act, the Neighborhood Children’s Protection Act, and the Protecting Children in the 21st Century Act [CIPA].
7. In addition to the above, the District Internet Safety program will include, but is not limited to the following:
INSTRUCTION

Access to Electronic Networks

a. Access by minors to inappropriate matter on the Internet and World Wide Web.
b. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.
c. Measures designed to restrict minors’ access to materials harmful to minors.
d. Compliance with the E-Rate requirements of the Children’s Internet Protection Act [CIPA].

Authorization for Electronic Network Access

Each staff member must sign the Authorization for Access to the District’s Electronic Network as a condition for using the District’s electronic network. Each student and his or her parent(s)/guardian(s) must sign the Authorization before being granted network access.

All users of the District’s computers and means of Network access 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 District’s administrative procedure, Acceptable Use of the District’s Electronic Networks, or this policy, will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

Personal Technology

Personal technology is defined as any device that is not owned or leased by the District or otherwise authorized for District use and (1) transmits sounds images, text messages videos, or electronic information; (2) electronically records, plays, or stores information; (3) accesses the Internet or private communications or information networks. This includes, but is not limited to smartphones, tablets, etc.

For all personal technology unassociated with the District provided network [including but not limited to any network technologies, i.e. 3G, 4G] the Board expressly claims no responsibility for imposing content filters, blocking lists, or monitoring of its students’ or employees’ personal technology.

Where personal technology has been approved for use during school or school-sponsored activities the student or employee will assume all risks associated with the use of personal technology and adhere to the standards set forth for appropriate behavior as stated and signed in the Acceptable Use Policy at all times, regardless if one is connected to the District network or to another unassociated network.

For employees of the District, use of personal technology and social media for personal purposes is permitted within the District only during non-work times or hours. Any duty-free use must occur during times and places that the use will not interfere with job duties or otherwise be disruptive to the school environment or its operation.

The district assumes no responsibility for a personal technology device that is lost, stolen, or damaged in any way.

The district will not expend any personnel or instructional time to support personal technology devices.

Internet /Electronic Mail Policy

Statement of Purpose

Macomb School District 185, being aware of the growing use of the electronic communications by employees and students, has developed guidelines for computer use. Electronic communication for purposes of this policy includes, but
INSTRUCTION

Access to Electronic Networks

is not limited to: Electronic mail, Internet services, voice mail, audio and video conferencing, and facsimile messages that are sent or received by administration, faculty, students or other authorized users of District 185 resources. The following policy is intended to supplement administrative and operational policies already in place. The purpose for the policy is to provide protection to the District, its Board, its employees, and students while using District-owned computer technology.

The growing issues of liability for misuse and failure to understand legal obligations in using the computer and Internet make the following policy necessary.

Of specific interest to the District are issues of copyright infringement, defamation, discrimination, and harassment. Courts have already upheld the legality of subpoenaing electronic documents including e-mail and historical logs. The District’s only protection against possible legal problems is a well-written policy regarding the use of the District’s computer system.

The policy has been developed through the cooperative work of the School Board, administration, and the Macomb Education Association. The cooperative nature of the policy reflects the importance that all involved parties place on having clear policies regulating and explaining the use of District 185 computers and related technologies.

Access to Electronic Networks and E-mail

Macomb School District 185 maintains both Internet and electronic mail systems to assist in the conduct of business within District 185. These systems, including the equipment and the data stored in the system, are and remain at all times the property of the District. Any and all computers or other devices (IE. PDAs or Cellular Phones) that are connected directly or wirelessly to the District’s network infrastructure are subject to inspection and monitoring at any time by the System Administrator. As such, all messages created, sent, received or stored in the system are and remain the property of the District.

Each District student, teacher, staff or Board member must sign the Authorization for Access to the District’s Electronic Networks as a condition for using the district’s electronic network. Each student and his or her parent(s)/guardian(s) must sign the Authorization before being granted unsupervised use. Failure of any of the previously listed to follow the terms of the District’s administrative procedure, Acceptable Use of the District’s Electronic Networks, or this policy, will result in the loss of privileges, and disciplinary action, and appropriate legal action.

Internet and e-mail use should be limited to the conduct of business for the District. The District allows employees to use the system on their own time for personal business as long as the personal use does not create a cost to the District. While the Board has no intention of monitoring computer use for either school or personal business, the District reserves the right to retrieve and review any message composed, sent, or received on its system. Please note that when a message is deleted or erased, it is still possible to recreate the message: therefore, ultimate privacy of message cannot be ensured for anyone. While the systems may accommodate the use of passwords for security, confidentiality cannot be guaranteed. Someone other than the intended recipient may review the message. Moreover, the District’s systems administrator can access anyone’s user area. Routine maintenance may require access to user files.

This policy is not intended in any way to restrict communications among employees and/or students. Macomb Education Association members may continue to use these systems following guidelines established between the Association and the District.

E-mail and Internet users are asked to take care in subscribing to list-serves, transmitting large messages and attachments, and sending multiple copies. Privacy in the use of District computers to access the Internet is not protected.

Messages, business or personal, may not contain content that may be considered offensive or disruptive to any employee or student. Offensive content would included, but would not be limited to, sexual comments or images, racial slurs,
INSTRUCTION

Access to Electronic Networks

gender specific comments or nay comments that would offend someone on the basis of his or her age, sexual orientation, religious or political beliefs, national origin, or disability. Use of the network must also comply with this principle.

An employee learning of any misuse of the computer systems or violations of this policy shall notify their building administrator. The District reserves the right to review user areas to include e-mail and historical data pertinent to the use of the Internet.

District Access

Cause Required for Access – the District reserves the right to access and disclose the contents of any communications created using District resources, but will do so only when it has a legitimate need. Existing rules, regulations and policies as agreed on between the District and MEA, existing or future law and regulations promulgated by state and/or federal legislation and/or court action shall govern such access.

Prohibited Uses

District resources shall not be used for
- commercial purposes;
- personal gain;
- non-school related political activity;
- non-school related fundraising;
- electronic communications to send copies of documents in violation of copyright;
- electronic communications to send messages, access to which is restricted by laws or regulations;
- intimidation of others or to interfere with the ability of others to conduct District business;
- “spoofing”, constructing electronic communication so it appears to be from someone else;
- “snooping”, obtaining access to files or communications of others for purpose of satisfying idle curiosity;
- Attempting unauthorized access to data or attempting to breach any security measures on any electronic communication systems, or attempting to intercept any electronic communication transmissions without proper authorization.

Records Retention

The District is to provide for efficient retention of e-mail communications. E-mail communications are considered public records and retention and disposition of public records is authorized by retention schedules in the Records Retention Act. Divisions may retain e-mail in hard copy, electronically, or by a combination of these two means. Building administrators are responsible for developing filing systems that include e-mail and are responsible for instructing employees on appropriate use of these systems.

When appropriate, e-mail messages may be filed with program records and assume the same retention as the records they are filed with. When e-mail records do not relate obviously or directly to a program, they may be filed as correspondence. When they are filed as correspondence, Records Retention Act will still govern retention. Any e-mail not affected by the Records Retention Act will be erased on a monthly basis as determined by the administration systems manager.

Sanctions for Violations

If an individual is accused of use of the system in ways that are judged excessive, wasteful, or unauthorized, the administration will follow established procedures to investigate those allegations. The individual found culpable might be subject to loss of access to computers. Depending on the abuse, the individual may also be subject to other appropriate
INSTRUCTION

Access to Electronic Networks

disciplinary action following procedures established by existing Board policies or the MEA contract. Appeal of decisions and procedures of appeals will follow established Board/Union agreements.

LEGAL REF.: No Child Left Behind Act, 20 U.S.C. §6777
Children’s Internet Protection Act, 42 U.S.C. §254(h) and (l).
7:20 ILCS 135/0.01

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


Adopted 9-16-97
Revised 12-14-98
Revised 5-21-01
Revised 6-18-01
Revised 12-17-01
Revised 7-15-02
Revised 03-19-07
Revised 11-19-07
Reviewed 03-19-12
Revised 06-18-12
Revised 12-17-12
Revised 11-18-13
Revised 10-17-16