Mapleton Public Schools

GBEE

Staff Use of the Internet and Electronic Communications

Mapleton Public Schools supports the use of the internet and electronic communications by staff to improve teaching and learning through interpersonal communication, access to information, research, training and collaboration and dissemination of successful educational practices, methods and materials.

Staff members shall take responsibility for their own use of School District computers and computer systems to avoid contact with or create material or information that violates this policy. At all times, the District reserves the right to remove, without advance notice or permission, any and all comments on the District's electronic technologies network which violate applicable laws, regulations and policies, Federal, state and local.

Mapleton Public Schools does not discriminate against employees who use these media for lawful personal interests and affiliations or other lawful purposes. Employees cannot use blogs or social networking sites to harass, threaten, discriminate or disparage District officials, students, employees or anyone associated with or doing business with the District. Any copyrighted information where written reprint information has not been obtained in advance must be properly cited in order to give appropriate recognition to the original creator. Bloggers and commenters are personally responsible for their commentary on social networking sites.

Blocking or Filtering Obscene, Pornographic and Harmful Information
To protect students from material and information that is obscene, including child pornography and any other materials otherwise harmful to minors, as defined by the District, network monitoring and firewall software is being utilized at the District level to block or filter such material and information from computers having internet or electronic communications access.

No Expectation of Privacy
Mapleton Public Schools' computers and computer systems are owned by the District and are intended for educational purposes and official business at all times. Staff members shall have no expectation of privacy when using the internet or electronic communications. The District reserves the right to monitor, inspect, copy, review and store (at any time and without prior notice) all usage of District computers and computer systems, including all internet and electronic communications access and transmission/receipt of materials and information. All material and information accessed/received through District computers and computer systems shall remain the property of the Mapleton Public Schools.

Confidentiality
Staff members shall not access, receive, transmit or retransmit material regarding students, parents/guardians or District employees that is protected by confidentiality laws unless

such access, receipt or transmittal is in accordance with their assigned job responsibilities, applicable law and District policy. Staff members shall handle all employee, student and district records in accordance with District policies GBJ, Personnel Records and Files; and JRA/JRC, Student Records/Release of Information on Students.

Disclosure of confidential student records, including disclosure via electronic mail or other telecommunication systems, is governed by state and federal law, including the Family Educational Rights and Privacy Act (FERPA).

Public records
Electronic messages sent or received by the Board of Education, District employees or students, including electronic mail on District-owned equipment, as well as other documents generated through use of the District's system may be considered a public record subject to disclosure or inspection under the Colorado Open Records Act.

Unauthorized and Unacceptable Uses
Staff members shall use District computers and computer systems in a responsible, efficient, ethical and legal manner. Employees are expected to protect personal login and password information, and should never share access with anyone, including a co-worker, student, parents/guardian or volunteer. Employees are responsible for exercising good judgment when utilizing district resources. A staff member identified as a security risk or having a history of problems with computer systems may be denied access to the District's network. Staff members also are held responsible and liable for any or all damages to school equipment assigned to them. Therefore, examples of unacceptable uses include, but are not limited to, the following. No staff member shall access, create, transmit, retransmit or forward material or information that:

- Promotes violence or advocates destruction of property including, but not limited to, access to information concerning the manufacturing or purchasing of destructive devices or weapons;
- Is not related to District education objectives except as provided in other District policies, or adversely affects the reputation or image of this organization;
- Contains pornographic, obscene or other sexually oriented materials, either as pictures or writings, which are intended to stimulate erotic feelings or appeal to interests in nudity, sex or excretion;
- Harasses, threatens, demeans, or promotes violence or hatred against another person or group of persons with regard to race, color, sex, sexual orientation, religion, national origin, age, marital status, disability or handicap. Sexual orientation is a person's orientation toward heterosexuality, homosexuality, bisexuality, or transgender status or perception of the individual's sexual orientation;
- Is for personal profit, financial gain, advertising, commercial purposes or campaigning purposes;

- Is intended to solicit, proselytize, advocate, or communicate the views of a non-school sponsored organization, except as otherwise provided in agreements with recognized employee organizations;
- Plagiarizes the work of another;
- Uses inappropriate or profane language or depictions likely to be offensive to others in the school community;
- Violates any federal or state law, including but not limited to copyrighted material and material protected by trade secret that contains personal information about themselves or others, including information protected by confidentiality laws;
- Shares student or district staff home addresses, phone numbers, or other private information except as allowed in policy JRA/JRC.

The following activities are also prohibited:

- Using another individual's internet or electronic communications account;
- Unauthorized attempts to log in to any network as a system administrator;
- Any malicious attempt to harm or destroy District data, or data of another user;
- Downloading, installing, storing or using malicious software, viruses, "cracking," and keystroke monitoring software;
- Interfering with or disrupting another information technology user's work as well as the proper function of information processing and network services or equipment;
- The individual assigned a computer/security account is accountable for any and all transactions entered under that computer/security account login;
- Leaving an active system unattended, thereby allowing an unauthorized person to gain access to district resources through the user's login session;
- Using a computer for unlawful purposes, such as the illegal copying or installation of software, or violation of copyright laws;
- Causes network performance degradation due to excessive bandwidth use as a result of unauthorized download or streaming of video or music not directly related to curriculum;
- Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws. Staff members should consult with their supervisor prior to exporting any material in question;
- Taking home or altering technology equipment (hardware or software) without permission of the Information Technology Department;
- Using information services for personal use or gain;
- Using District electronic communication resources to participate in activities including, but not limited to, news groups, wikis, blog discussions, and social networking except for bona fide educational purposes.

Social, Collaborative, Interactive, and Responsive Technologies
Mapleton Public Schools supports the use of technologies such as blogs, wikis, podcasts, for educational purposes and communicating with the community. These technologies are considered an extension of the classroom and are used to convey information about District services; promote and raise awareness of Mapleton Public Schools; and communicate with employees, students, and community members. Social media networks may not be used for classroom instruction or school-sponsored activities without the prior authorization of a supervisor or School Director and submitted to the District Communications Office. Staff members must provide a plan to your supervisor or School Director to show how this use of technology will be monitored to prevent misuses or to prevent in appropriate contact. In addition, your staff shall provide their supervisor or School Director all access codes and login information. Parental consent for students under the age of 18's participation on social networks shall be on file with the student's records.

The District also acknowledges that employees may choose to utilize technologies such as Twitter, MySpace, and Facebook on their own time. Employees should exercise good judgment and common sense, while maintaining their professionalism as District employees and should address inappropriate behavior or activity on these networks, including requirements for mandated reporting. Employees must avoid posting any information or engaging in communications that violate state or federal laws or District policies.

A clear line between personal and professional usage must be defined by the following:

- Personal social networking sites should not be used to encourage inappropriate personal non-professional relationships with current or recent students. "Friending" or otherwise establishing personal relationships with students on social networking sites or through other interactive technologies may be inappropriate and can erode professional boundaries expected of employees.
- Confidential student, information may not be disclosed on personal social networking sites or through other interactive technologies. Disclosure of confidential student records, including disclosure via electronic mail or other telecommunication systems, is governed by state and federal law, including the Family Educational Rights and Privacy Act (FERPA).
- Staff members shall handle all employee, student and District records in accordance with District policies GBJ, Personnel Records and Files; and JRA/JRC, Student Records/Release of Information on Students.

All employees must identify themselves as employees of the District when posting official comments or responses on the social networking site. Schools are responsible for ensuring all blogging and social networking information complies with District policies and guidelines including but not limited to the following: Bullying Policy, Sexual Harassment Policy and Acceptable Computer/Internet Use Agreement Policy. School Directors are

authorized to remove any content that does not meet the rules and guidelines of this policy or that may be illegal or offensive, upon approval of the primary account administrator as designated by the Superintendent.

Use of District's name and logo
Staff using the District's electronic resources must abide by guidelines regarding the use of the District's official name, logo or branding. District branding may not be used without appropriate authorization from Communications. Users of District electronic resources shall not represent or otherwise make statements on behalf of Mapleton Public Schools unless appropriately authorized to do so.

Passwords
Accounts must be protected as follows:

- All accounts, including accounts within major applications, must have a password.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level passwords must conform to the following strong password requirements
  - A strong password contains a minimum of eight (8) to fourteen (14) characters in length.
  - Have at least one numeric or symbol
  - Be significantly different from prior passwords
  - Not contain your name or user name
  - Not be a common word or name
- Passwords should never be written down or stored online unless they are encrypted using a district-approved encryption method.
- Passwords must be changed at least every 90 days.
- Passwords must be changed immediately if guessed by a password cracker or seen by another person even partially and must not be given to anyone.

Security
Security and integrity of District computer systems and information is a high priority and requires participation of all staff members. Staff members who identify a security problem while using the internet or electronic communications should immediately notify the IT Service Desk and avoid demonstrating the problem to other users. Student or employee information stored in electronic format shall not be taken home on a laptop or transferred to an external device for home or outside use unless district data security and encryption procedures are followed.

Staff members shall not:

- Use another person's password or any other identifier

- Gain or attempt to gain unauthorized access to District computers or computer systems
- Read, alter, delete or copy, or attempt to do so, electronic communications of other system users

Unauthorized Software
Staff members are prohibited from using or possessing any software that has been downloaded or is otherwise in the user's possession without appropriate registration and payment of any fees owed to the software owner. Software will not be copied or duplicated or loaded on any system without the proper proof of legal use rights or number of licenses.

Staff Member Use is a Privilege
Staff member use of the internet and electronic communications is a privilege, not a right. Failure to follow the use procedures contained in this policy may result in the loss of the privilege to use these tools, as well as disciplinary action up to and including dismissal and/or legal action. The District may deny, revoke or suspend access to District technology or close accounts at any time.

Staff members shall be required to verify their acceptance of and compliance with the District's acceptable use agreement.

Alternative Workspace
When working at home or an alternative workplace, District computer system users must establish security standards at their alternate workplace sufficient to protect hardware, software, and information. This includes:

- Having only those resources employees really need and have authority to use.
- Establishing a thorough understanding and agreement with supervisors as to what employees' security responsibilities are.
- Using software according to licensing agreements.
- Ensuring any non-approved or pirated software is not installed on District property computers.
- Ensuring that any confidential or sensitive information that is downloaded is secure with District approved encryption methods.

School District Makes No Warranties
The District makes no warranties of any kind, whether expressed or implied, related to the use of district computers and computer systems, including access to the internet and electronic communications services. Providing access to these services does not imply endorsement by the District of the content, nor does the District make any guarantee as to the accuracy or quality of information received. The District shall not be responsible for any damages, losses or costs a staff member suffers in using the internet and electronic communications including, but not limited to, loss of data, service interruptions and loss of

data resulting from delays or service interruptions.

The District will not be responsible for the accuracy, nature, or quality of information stored on District diskettes, hard drives, or servers; nor for the accuracy, nature, or quality of information gathered through District-provided Internet access. The District will not be responsible for personal property used to access District computers or networks or for District-provided Internet access. The District will not be responsible for unauthorized financial obligations resulting from District-provided access to the Internet. Use of any information obtained via the internet and electronic communications is at the staff member's own risk.

Adopted December 11, 2012 by the Board of Education for Mapleton Public Schools.

LEGAL REFERENCES:

47 U.S.C.. 254(h) (*Children's Internet Protection Act of 2000*)

47 U.S.C.. 231 (*Child Online Protection Act of 1998*)

20 U.S.C.. 6801 et seq. (*Elementary and Secondary Education Act*)

CROSS REFERENCES:

GBJ: Personnel Records and Files

JRA/JRC: Student Records/Release of Information on Students