TECHNOLOGY USE AND ELECTRONIC COMMUNICATIONS SYSTEM

The McMinnville School District recognizes that telecommunications systems and new technologies change the way information is accessed and used in society. Instruction, student learning, and business practices are transformed through the effective integration and use of technology. The District is committed to providing access to telecommunications, network services, and information system tools in support of the District's mission. All individuals accessing these resources through District systems or on District property are expected to use them in a professional manner aligned with the instructional and operational mission of the District and applicable policy and guidelines.

ADMINISTRATIVE REGULATION:

Definitions

1. "Technology protection measure", as defined by the Children's Internet Protection Act (CIPA), means a specific technology that blocks or filters Internet access to visual depictions that are:

    a. Obscene, as that term is defined in Section 1460 of Title 18, United States Code;
    b. Child pornography, as that term is defined in Section 2256 of Title 18, United States Code; or
    c. Harmful to minors.

2. "Harmful to minors", as defined by CIPA, means any picture, image, graphic image file or other visual depiction that:

    a. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion;
    b. Depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
    c. Taken as a whole, lacks serious literary, artistic, political or scientific value to minors.

3. "Sexual act; sexual contact", as defined by CIPA, have the meanings given such terms in Section 2246 of Title 18, United States Code.

4. "Minor", as defined by CIPA, means an individual who has not attained the age of 17. For the purposes of Board policy and the administrative regulation, minor will include all students enrolled in District schools.

5. "Inappropriate matter", as defined by the District, means material that is inconsistent with general public education purposes, the District's mission and goals.

6. User: An employee, student, authorized volunteer, authorized contractor, or other user accessing technology resources provided by the McMinnville School District.

7. Systems: All District technology systems including, but not limited to, telecommunications, network, storage, server, software, and information systems. This also includes all computing

devices such as, but not limited to, computers, laptops, mobile computing and telecommunications devices, and all related peripherals.

System Access

Access to District systems is provided to conduct business or research related to the operational or instructional needs of the District. To that end, access to the District's system is authorized to:

1. Board members and District employees who have signed a District user agreement.

2. Students in grades K-12 under the appropriate supervision of staff.

3. District volunteers, contractors, or other members of the public as authorized by the system coordinator, consistent with the District's mission and policies governing the use of District equipment and materials.

4. Students, Board members, volunteers, contractors, and other authorized users may use District technology, including e-mail and Internet, only to conduct District business. Personal use of said systems is strictly prohibited.

5. Staff must use District technology including, but not limited to, Internet access and e-mail, to conduct District business. Personal use of said systems by staff is restricted. Any personal use by staff is limited to such uses as deemed permissible under the Oregon Government Ethics Commission (OGEC) guidance. (e.g., occasional use to type a social letter to a family member) Such use is restricted to the employee's own time.

General Use Guidelines

Operation of District technology systems relies on appropriate use by all users. Students, staff, and others granted system access are responsible for being good digital citizens and adhering to the ethical, legal, and appropriate use guidelines. As digital citizens and users of District technology systems, users agree to the following when using District technology systems or when using any technology on District property:

1. Use District systems to conduct District business or research related to the instructional or operational needs of the District.

2. Keep their District account information and/or passwords private and not share them with anyone in any manner. Users agree to only use those accounts and/or passwords they have been issued by the District. Passwords are the property of the District.

3. Protect private information including that related to students and staff. The downloading of student or staff information to any personal device is prohibited unless approved by technology services.

4. Protect user safety by not posting user information, including private information, photos, video, or other information forms, to the web or other Internet-based systems not provided by the District unless approved by technology services.

5. Adhere to the same standards for communicating on-line that are expected in the classroom and consistent with Board policy and administrative regulations.

6. Use District systems to conduct all District business related to the instructional or operational needs of the District. All web sites and other related systems must be hosted on District servers unless approved by TECHNOLOGY SERVICES management.

7. Respect the privacy of others. Do not read the mail or files of others without their permission.

8. Report violations of the District's policy and/or administrative regulations, or security problems to the supervising teacher, system coordinator, or administrator as appropriate.

9. Practice good digital citizenship as explained in District training sessions and student handbook.

10. Use District approved software, computing devices, and systems in the conduct of District business supporting instruction and operation. MSD Staff members must follow the District's acceptable use of Educational Technology procedures as outlined in the MSD Acceptable Use Guidelines for Technology Document.

11. Abide by all copyright laws and license agreements.

The following are strictly prohibited:

1. Attempts to use the District's system for:
   a. Unauthorized solicitation of funds;
   b. Downloading, storage, use and/or distribution of chain letters, media, or other items not directly related to the conduct of District business;
   c. Unauthorized sale or purchase of merchandise and services;
   d. Collection of signatures;
   e. Membership drives;
   f. Transmission of any materials regarding political campaigns.

2. Attempts to upload, download, use, reproduce, or distribute information, data, software, music, videos, or other media or materials on the District's system in violation of copyright law or applicable provisions of use or license agreements.

3. Attempts to degrade, disrupt, or vandalize District systems, software, materials or data, or those of any other user of the District's system, or any of the agencies or other networks connected to the District's system directly or indirectly.

4. Attempts to evade, change, or exceed resource quotas or disk usage quotas.

5. Attempts to send, intentionally access, or download any material including, but not limited to, websites, text files, or media, or engage in any communication that includes material which may be interpreted as:
   a. Harmful to minors;
   b. Obscene or child pornography as defined by law; or indecent, vulgar, profane, or lewd as determined by the District;
   c. A product or service not permitted to minors by law;
   d. Harassment, intimidation, menacing, threatening; or constitutes insulting or fighting words, the very expression of which injures or harasses others;

e. A likelihood that, either because of its content or the manner of distribution, it will cause a material or substantial disruption of the proper and orderly operation of the school or school activity;

f. Defamatory, libelous, reckless, or maliciously false; potentially giving rise to civil liability; constituting or promoting discrimination; a criminal offense, or otherwise violates any law, rule, regulation, Board policy, and/or administrative regulation.

6. Access or attempts to gain unauthorized access to any service via the District's system. This prohibition includes services with or without cost and/or attempts to incur other types of costs without specific approval. The user accessing such services will be responsible for these costs.

7. Posting, publishing, or attempts to post or publish personally identifiable student or staff information, including photos or videos, to any web or other Internet-based system not provided by the District unless approved by the technology services director.

8. Attempts to use District names or information in external communication forums such as chat rooms, websites, or social media without prior District authorization.

9. Attempts to use another individual's account name or password, failure to provide the District with individual passwords, or to access restricted information, resources, or networks to which the user has not been given access.

General District Responsibilities

The District will:

1. Provide technology protection measures that protect against Internet access by both staff and students to visual depictions that are obscene, child pornography, or with respect to the use of computers by students and staff, harmful to minors. An administrator, supervisor, or other individual authorized by the Superintendent may disable the technology protection measures to enable access for bona fide research or other lawful purposes, as deemed appropriate;

2. Prohibit access by minors, as defined by CIPA and this regulation, to inappropriate matter on the Internet and World Wide Web;

3. Provide staff supervision to monitor the on-line activities of students to prevent unauthorized access, including "hacking" and other unlawful activities on-line, and ensure the safety and security of students when authorized to use E-mail, chat rooms and other forms of direct electronic communication.

4. Program its computers to display a message reinforcing key elements of the District's Electronic Communications policies and regulations when accessed for use;

5. The Technology Department administrator with advisement from the district technology committee will set parameters for internet filtering.

6. Notify the appropriate system users that:

    a. The District retains ownership and control of its computers, hardware, software and data at all times. All communications and stored information transmitted, received or

contained in the District's information system are the District's property and are to be used for authorized purpose only. Use of the District equipment or software for unauthorized purposes is strictly prohibited. To maintain system integrity, monitor network etiquette and ensure that those authorized to use the District's system are in compliance with Board policy, administrative regulations and law, school administrator may routinely review user files and communications.

b. Files and other information, including E-mail, sent or received, generated or stored on District servers are not private and may be subject to monitoring. By using the District's system, individuals consent to have that use monitored by authorized District personnel. The District reserves the right to access and disclose, as appropriate, all information and data contained on District computers and District-owned E-mail system;
c. The District may establish a retention schedule for the removal of E-mail;
d. E-mail sent or received by a Board member or employee in connection with the transaction of public business may be a public record and subject to state archivist rules for retention and destruction;
e. Information and data entered or stored on the District's computers and E-mail system may become discoverable evidence if a public records request is made or a lawsuit is filed against the District. "Deleted" or "purged" data from District computers or E-mail system may be retrieved for later public records disclosure or disciplinary purposes, as deemed necessary by the District;
f. Passwords used on the District's system are the property of the District and must be provided to their supervisor or designated district personnel, as appropriate. Passwords that have not been provided to the District are prohibited;
g. Transmission of any materials regarding political campaigns is prohibited.

Violations and Consequences

1. Students
    a. Students who violate general system user prohibitions shall be subject to discipline up to and including expulsion and/or revocation of District system access up to and including permanent loss of privileges.
    b. Violations of law will be reported to law enforcement officials.
    c. Disciplinary action may be appealed by parents, students and/or a representative in accordance with established District procedures.

2. Staff
    a. Staff who violated general system user prohibitions shall be subject to discipline up to and including dismissal in accordance with Board policy, collective bargaining agreements and applicable provisions of law.
    b. Violations of law will be reported to law enforcement officials.
    c. Violations of applicable Teacher Standards and Practices Commission (TSPC), Standards for Competent and Ethical Performance of Oregon Educators will be reported to TSPC as provided by OAR 584-020-004.
    d. Violations of ORS 244.040 will be reported to the Government Standards and Practices Commission (GSPC).

3. Others
    a. Other guest users who violate general system user prohibitions shall be subject to suspension of system access up to and including permanent revocation of privileges.
    b. Violations of law will be reported to law enforcement officials or other agencies, as appropriate.

Complaints

Complaints regarding use of the District's Electronic Communications System may be made to the teacher, principal, employee's supervisor, or system coordinator. The District's established complaint procedure will be used for complaints concerning violations of the District's Electronic Communications System policy and/or administrative regulation. See Board policy KL/KLD—Public Complaints and KL/KLD-AR—Public Complaint Procedure.

7/14/14, 3/13/2017