

Electronic Communications System

Definitions

“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.

“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.

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

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

“Inappropriate matter” as defined by the district means material that is inconsistent with general public education purposes, the district’s mission and goals. 1

General District Responsibilities

The district will:

- A. Designate staff as necessary to ensure coordination and maintenance of the district’s electronic communications system which includes all district computers, E-mail and Internet access;
- B. Provide staff training in the appropriate use of the district’s system including copies of district policy and administrative regulations. Staff will provide similar training to authorized system users;
- C. Cooperate fully with local, state or federal officials in any investigation relating to misuse of the district’s system;
- D. Use only properly licensed software, audio or video media purchased by the district or approved for use by the district. The district will comply with the requirements of law regarding the use,

- reproduction and distribution of copyrighted works and with applicable provisions of use or license agreements;
- E. Protect computers and systems by the use of desktop and/or server virus detection and removal software;
 - F. Provide technology protection measures that protect against Internet access by both adults and minors to visual depictions that are obscene, child pornography, or with respect to the use of computers by minors, 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;
 - G. Prohibit access by minors, as defined by CIPA and this regulation, to inappropriate matter on the Internet and World Wide Web;
 - H. 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 minors when authorized to use E-mail, chat rooms and other forms of direct electronic communication;
 - I. Provide student education about appropriate online behavior, including cyberbullying awareness and response, and how to interact with other individuals on social networking sites and in chat rooms;
 - J. Determine which users and sites accessible as part of the district’s system are most applicable to the curricular needs of the district and may restrict user access, accordingly;
 - K. Provide staff with access to the district’s e-mail system;
 - L. Program its computers to display a message reinforcing key elements of the district’s Electronic Communications System policy and regulation when accessed for use;
 - M. Notify appropriate system users that:
 - 1. 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 purposes only. Use of 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 administrators may routinely review user files and communications.
 - 2. 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;
 - 3. The district may establish a retention schedule for the removal of E-mail;
 - 4. 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;
 - 5. 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;

6. The district may set quotas for system disk usage. The district may allow system users to increase their quota by submitting a written request to the supervising teacher or system coordinator stating the need for the increase;
 7. Transmission of any materials regarding political campaigns is prohibited.
- N. Ensure all students, staff and non-school system users complete and sign an agreement to abide by the district's electronic communications policy and administrative regulations. All such agreements will be maintained on file in the school office or may be maintained electronically by the district.
- O. Notify users of known copyright infringing activities and deny access to or remove the material.

System Access

- A. Access to the district's system is authorized to:
1. Board members, district employees, students, with parent approval and when under the direct supervision of staff, and district volunteers, district contractors or other members of the public as authorized by the system coordinator or district administrators consistent with the district's policy governing use of district equipment and materials.
 2. Students, staff, Board members, volunteers, district contractors and other members of the public may be permitted to use the district's system for personal use, in addition to official district business, consistent with Board policy, general use prohibitions/guidelines/etiquette and other applicable provisions of this administrative regulation. Personal use of district-owned computers including Internet and E-mail access by employees is prohibited during the employee's work hours. Additionally, Board member and employee use of district-owned computers may be permitted only when such use does not violate the provisions of ORS 244.040 and use is under the same terms and conditions that access is provided to the general public under the district's policy governing use of district equipment and materials.
 3. Students, staff, Board members, volunteers, district contractors and other members of the public may be granted access for up to one academic year at a time. The district may renew access for students and staff at the start of each school year. System access agreements will be incorporated into student and staff handbooks.

General Use Prohibitions/Guidelines/Etiquette

Operation of the district's system relies upon the proper conduct and appropriate use of system users. Students, staff and others granted system access are responsible for reporting misuse and adhering to the following prohibitions and guidelines which require legal, ethical and efficient utilization of the district's system.

A. Prohibitions

The following conduct is strictly prohibited:

1. Attempts to use the district's system for:
 - (a) Unauthorized solicitation of funds;
 - (b) Distribution of chain letters;
 - (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 or software 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 the district's equipment, 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;
4. Attempts to evade, change or exceed resource quotas or disk usage quotas;
5. Attempts to send, intentionally access or download any text file or picture 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. Attempts to gain unauthorized access to any service via the district's system which has a cost involved or attempts to incur other types of costs without specific approval. The user accessing such services will be responsible for these costs;
7. Attempts to post or publish personal student contact information unless authorized by the system coordinator or teacher and consistent with applicable Board policy pertaining to student directory information and personally identifiable information. Personal contact information includes photograph, age, home, school, work or E-mail addresses or phone numbers or other unauthorized disclosure, use and dissemination of personal information regarding students;
8. Attempts to arrange student meetings with anyone on the district's system, unless authorized by the system coordinator or teacher and with prior parent approval;
9. Attempts to use the district's name in external communication forums such as chat rooms without prior district authorization;
10. Attempts to use another individual's account name or password, fail to provide the district with individual passwords or to access restricted information, resources or networks to which the user has not been given access.

B. Guidelines/Etiquette

Appropriate system use etiquette is expected of all users and is explained in district training sessions. The district may develop a refresher training schedule. The district may develop training and informational materials to be available for staff and students. New staff members will receive technology etiquette/guidelines training as part of their orientation.

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.

Violations/Consequences

A. Students

1. 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.
2. Violations of law will be reported to law enforcement officials.
3. Disciplinary action may be appealed by parents, students and/or a representative in accordance with established district procedures.

B. Staff

1. Staff who violate 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.
2. Violations of law will be reported to law enforcement officials.
3. 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 584-020-0041.
4. Violations of ORS 244.040 will be reported to OGEC (Oregon Government Ethics Commission).

C. Others

1. 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.
2. Violations of law will be reported to law enforcement officials or other agencies, as appropriate.

Telephone/Membership/Other Charges

- A. The district assumes no responsibility or liability for any membership or phone charges including, but not limited to, long distance charges, per minute (unit) surcharges and/or equipment or line costs incurred by any personal usage of the district's system.
- B. Any disputes or problems regarding phone services for home users of the district's system are strictly between the system user and his/her local phone company and/or long distance service provider.

Information Content/Third Party Supplied Information

- A. System users and parents of student system users are advised that use of the district's system may provide access to materials that may be considered objectionable and inconsistent with the district's mission and goals. Parents should be aware of the existence of such materials and monitor their student's home usage of the district's system accordingly.
- B. Opinions, advice, services and all other information expressed by system users, information providers, service providers or other third party individuals are those of the providers and not the district.
- C. The district does not warrant that the functions or services performed by or that the information or software contained on the system will meet the system user's requirements or that the system will be uninterrupted or error-free or that defects will be corrected. The district's system is provided on an "as is, as available" basis. The district does not make any warranties, whether express or implied including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein.

MILTON-FREEWATER UNIFIED SCHOOL DISTRICT NO. 7
District Electronic Communications System (DECS)

STUDENT NETWORK RESPONSIBILITY CONTRACT

Please read the following carefully before signing this document. This is a binding contract and must be signed before you will be given internet access.

DECS (District Electronic Communications System) is Milton-Freewater Unified School District's electronic network which accesses the Internet. The Internet is an electronic highway connecting thousands of computers all-over the world and millions of individual people. Students, teachers, support staff, parents and community members access to the DECS server have access to: 1) electronic mail (email) communication with people all over the world; 2) information and news from a variety of sources and research institutions; 3) public domain and shareware software of all types; 4) discussion groups on a wide variety of topics; 5) access to many university libraries, the Library of Congress, and more!

With access to computers and people all over the world also comes the availability of some material that may not be considered to be of educational value within the context of the school setting. The Milton-Freewater Unified School District (MFUSD) has taken every available precaution to restrict access to controversial materials.

However, on a global network it is impossible to control all materials. The users of DECS firmly believe that the valuable information and interaction available on this worldwide network far outweigh the possibility of users procuring material that is not consistent with the educational goals within each school.

Attached are guidelines provided to establish the responsibilities you are about acquire. If any user violates any of these provisions, his or her access to DECS will be terminated and all future access could possibly be denied. The signatures at the end of this document are binding and indicates the parties who signed have read the terms and conditions carefully and understands their significance.

DECS - Terms and Conditions:

- I. ACCEPTABLE USE:** The purpose of the Internet is to support research and education in and among academic institutions in the U.S. by providing access to unique resources and the opportunity for collaborative work. Your access must be in support of education and research and consistent with the educational objectives of the Milton-Freewater Unified School District. Use of other organization's networks or computing resources must comply with rules appropriate for that network. Transmission of any material in violation of any US or state organization is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secret. Use for commercial activities by for profit institutions is generally not acceptable. Use for product advertisement or political lobbying is also prohibited. (Initial)

- II. PRIVILEGES:** The use of DECS is a PRIVILEGE, not a right, and inappropriate use will result in a cancellation of those privileges. (Each student who receives access permission will be part of a discussion with a MFUSD faculty member pertaining to the proper use of the network.) The system administrator(s) will deem what is inappropriate use and the decision is final. Also, the system administrator(s) may ban access at any time as required. The administration, teachers and/or staff, of MFUSD may request the system administrator to deny, revoke, or suspend specific user access. (Initials)

- III. NETIQUETTE (NETWORK ETIQUETTE):** The use of an access on DECS requires that you abide by accepted rules of network etiquette. These include, but are not limited to, the following:
 1. **BE POLITE.** Do not send abusive messages to ANYONE.
 2. **USE APPROPRIATE LANGUAGE.** In all messages, do not swear, use vulgarities or any other inappropriate language. Anything pertaining to illegal activities is strictly forbidden.
 3. **PRIVACY.** Do not reveal the personal address or phone numbers of yourself, or any persons. All communications and information accessible via the network should be assumed private property.
 4. **CONNECTIVITY.** Do not use the network in such a way that would disrupt the use of the network by others.

- IV. SERVICES:** MFUSD will not be responsible for any damages you may suffer. This includes loss of data resulting from delays, non-deliveries, or service interruptions caused by our own negligence or your errors or omissions. Use of any information obtained via DECS is at your own risk. MFUSD specifically denies any responsibility for the accuracy or quality of information obtained through its services.
- V. SECURITY:** Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on DECS, you must notify a system administrator either in person or via the network. Attempts to login to DECS as a system administrator or as any other user will result in immediate cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to DECS.
- VI. VANDALISM:** Vandalism will result in cancellation of privileges. This includes, but is not limited to, the uploading or creation of computer viruses.
- VII. UPDATES:** MFUSD may occasionally require new registration and access information from you to continue providing services.

All Terms and Conditions as stated in this document are applicable to the Milton-Freewater School District in addition to DECS and all other Internet access networks. These Terms and Conditions reflect the entire agreement of the parties and supersedes all prior oral or written agreements and understandings of the parties. These terms and conditions shall be governed and interpreted in accordance with the laws of the State of Oregon, United States of America.

“I understand and will abide by the above Terms and Conditions for access privileges to the DECS server. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation my access privileges may be revoked, school disciplinary action may be taken and/or appropriate legal action.”

Student Printed Name: _____ Student Signature: _____

PARENT OR GUARDIAN NETWORK RESPONSIBILITY CONTRACT

*(**If user is under the age of 18, a parent or guardian must also read and sign this agreement)*

As the parent or guardian of this student I have read the Terms and Conditions for DECS. I understand that this access is designed for educational purposes and MFUSD has taken available precautions to eliminate controversial materials. However, I also recognize it is impossible for MFUSD to restrict access to all controversial materials and I will not hold them responsible for materials acquired on the network.

Further, I accept full responsibility for supervision if and when my child’s use is not in a school setting. I hereby give my permission to allow access privileges for my child and certify that the information contained on this form is correct.

Parent or Guardian (print) _____

Signature: _____ Date: ____/____/____