MARATHON CITY SCHOOL DISTRICT

GUIDELINES CONCERNING THE USE OF DISTRICT COMPUTER NETWORKS

All computer and communication network services in the School District of Marathon are provided for the sole purpose of facilitating the educational goals of the District. Users of the network should assume that any documents they store or any email messages they send or receive are not private. School District of Marathon reserves the right to access, review, monitor, copy, disclose, and/or download any stored information, communications, files or other materials created or maintained by any person, including coded, encrypted, or password protected material at any time. School District e-mail will be archived for a span of seven years. These services are provided as a privilege to the user and this Acceptable Use Policy provides an opportunity to educate the user on the school's expectations and the responsibilities of the user, in accordance with requirements of the Children's Internet Protection Act (CIPA) and the Neighborhood Children's Internet Protection Act (NCIPA).

Please keep the following information for future reference and sign, date and return the attached signature page to the building principal.

<u>User Rules</u>
1. Personal Safety
    a. Users shall not post contact information (e.g., address, phone number, images) about themselves or any other person.
    b. Students shall not agree to meet with someone they have met online without approval of their parent(s)/guardian(s). Any contact of this nature or the receipt of any message the student feels is inappropriate or makes the student feel uncomfortable should be reported to school authorities immediately.
    c. Security Software will be installed on all District computers. The District provides filtered Internet access. Filtering levels for all students are determined by federal law and Board policy.

2. Illegal Activities
    a. Users shall not use district computer networks to engage in any illegal act, such as arranging for a drug sale, engaging in criminal gang activity, threatening the safety of a person, transmitting material in violation of state or federal law (CIPA). Following CIPA guidelines, this includes but is not limited to cyber bullying, transmitting pornographic or erotic images, sexual innuendos/implications, racial slurs, derogatory gender-specific comments, or any comment that defames, slanders or libels another person.

3. Commercial Activities
    a. Users shall not use district computer networks for commercial purposes to offer or provide products or services that are not related to the School District of Marathon.

4. Political Activities
    a. Users shall not use district computer networks for political lobbying or assisting a campaign for election of any person to any office or the promotion of or opposition to any ballot proposition.

5. System Security
    a. If an individual account is provided, the user is responsible for that account and should take all reasonable precautions to prevent others from being able to use that account. Under no condition should a user give his/her or another user's login and/or password to another person.

b. Users shall immediately notify a teacher or the system administrator if they have identified a possible security problem. Users should not look for security problems – this may be construed as an illegal attempt to gain access.

c. Users shall avoid the inadvertent spread of computer viruses by following the district virus protection procedures when downloading files.

d. Users shall not attempt to gain unauthorized access to district computer networks or any other computer system or go beyond their authorized access by entering another person's account number or accessing another person's files.

e. Users shall not deliberately attempt to disrupt the computer network or destroy data by spreading computer viruses or by any other means.

f. Users shall not intentionally tamper with the hardware or software available for their use.

g. Users shall not use others' passwords.

h. Users shall not trespass in others' folders, documents or files.

i. Users shall not maliciously attempt to harm, modify or destroy data of another user.

6. Inappropriate Language

a. On any and all uses of the Internet, whether in application to public or private messages or material posted on web pages, including e-mail, users shall not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language or language that is inconsistent with community standards. Users shall not post information that could cause danger or disruption or engage in personal attacks, including prejudicial or discriminatory attacks. Users shall not harass another person by a persistent action that distresses or annoys another person and users must stop if asked to do so.

7. Network Etiquette

a. Students shall exhibit good behavior.

b. Staff shall follow general rules and standards for professional behavior when using district computer networks to communicate with others.

c. Users shall respect the privacy of others. Staff shall not use district computer networks to share confidential information about students or other employees.

d. Users shall not disrupt the use of the network by other users.

8. Respecting Resource Limits

a. Users shall use district computer networks only for educational purposes, including classroom activities, career development activities, limited high-quality self-discovery activities, research activities and for communication with others, that are consistent with the educational objectives of the Marathon City School District. Games or other programs of a personal nature may not be loaded from a floppy, CD or DVD drive.

b. Users shall not intentionally waste limited resources.

c. Students shall not download large files without the approval of a lab supervisor or teacher. The system administrator shall be notified when such files have been downloaded. These files will be deleted when no longer needed.

d. Staff shall not download large files without the approval of the system administrator.

e. Students shall subscribe only to high-quality discussion group mail lists that are approved by a teacher or the Librarian and Audio-Visual Coordinator and that meets specific curricular objectives that are consistent with published curriculum guides.

e. Staff shall subscribe only to high-quality discussion group mail lists that meet specific curricular objectives that are consistent with published curriculum guides.

9. Plagiarism and Copyright Infringement

a. Users shall not plagiarize works that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were their own.

b. Users shall respect the rights of copyright owners. Copyright infringement occurs when users inappropriately reproduce a work that is protected by copyright. If a work contains language that specifies appropriate use of that work, users should follow the expressed requirements. If users are unsure whether or not they can use a work, they should request

permission from the copyright owner. Any questions regarding copyright law should be directed to a teacher or the Librarian and Audio-Visual Coordinator as well consultation of the District Copyright Policy.

    c.   Users shall not attempt to alter or copy any licensed software found on a district computer network.

10.   Inappropriate Access to and Transmission of Material

    a.   Users shall not use district computer networks to access, send or display material, including messages and pictures, that is profane, obscene or sexually explicit (pornography) or that advocates illegal acts or violence or discrimination toward other people (hate literature). An exception may be made for hate literature if the access is for the purpose of planning or conducting research. Students may access hate literature only with the approval of their teacher and parent(s)/guardian(s).

    b.   Users shall not use district computer networks to access information on how to make explosives or other devices of destruction.

    c.   The district uses filtering software to attempt to limit access to profane, obscene or other inappropriate Internet sites. No filtering software is foolproof, however, and it is the responsibility of users to notify district personnel of sites that are profane, obscene, or violent in nature. If users mistakenly access inappropriate information, they should immediately tell a teacher or the system administrator. This will protect users against a claim of intentional violation of this policy.

    d.   A student's parent(s)/guardian(s) should instruct his/her child if there is additional material he/she thinks would be inappropriate for the student to access. The district fully expects that students will follow their parent's/guardian's instructions in this matter.

11.   Personal or Recreational Use of District Computer Networks

    a.   Users shall not use district computer networks for inappropriate recreational or personal use.

12.   Religion

    a.   Users shall not use district computer networks to promote, support or celebrate religion or religious institutions.

13.   Union Business

    a.   Staff shall not use district computer networks to conduct union business other than that which is approved under the negotiated agreement.

14.   Other Rules

    a.   Users shall not violate other established district or school rules while using district computer networks.

When users are using a computer system, it may feel like they can easily break a rule and not get caught. This is not true. Electronic footprints are imprinted on the system whenever an action is performed. Therefore, users are likely to be caught if they break the rules.

The district shall cooperate fully with local, state or federal officials in any investigation related to illegal activities conducted through a district computer network.

<u>Student Free Speech</u>
A student's right to free speech applies to the student's communication on the Internet. The Internet is considered a limited forum, similar to the school newspaper, and therefore the district may restrict a student's right to free speech for valid educational reasons. If student work is published on the Internet as part of a district or school web site, it shall be consistent with the goals of the curriculum and shall follow all district guidelines for web page development.

Privacy Issues

Users should not expect that their personal files and messages stored on district computer networks are private. The network administrator may review files and messages to maintain system integrity and to ensure that users are using the system responsibly. This review may lead to a discovery that a user has violated a rule or state or federal law. An individual search shall be conducted if there is reasonable suspicion that a user has violated a rule or law. The investigation shall be reasonable and related to the suspected violation. If the user is under age 18, the user's parent(s)/guardian(s) has the right at any time to see the contents of the user's network files and messages.

Violations

The building principal and system administrator shall determine if a user has violated a rule or state or federal law. In the event of a claim that a user has violated a rule or state or federal law, the user shall be given notice of the suspected violation and have an opportunity to present an explanation. Violations may result in payment for damages and repairs and/or disciplinary action including, but not limited to, loss of access privileges, suspension, expulsion or dismissal. When applicable, law enforcement agencies may be involved.

Waiver of Claims

The district makes no guarantee that the functions or the services provided by or through the district computer network system will be error-free or without defect. The district is not responsible for any damage students may suffer including, but not limited to, loss of data or interruptions of service. The district is not responsible for the accuracy or quality of the information attained through or stored on the system. The district is not responsible for financial obligations arising from unauthorized use of the system.

APPROVED: December 11, 1996

REVISED: May 10, 2000
                    February 10, 2010