Madeira City Schools
Administrative Guidelines

7540.03 - STUDENT EDUCATION TECHNOLOGY ACCEPTABLE USE AND SAFETY

Students are authorized to use the Board's computers, laptops, tablets, personal communication devices (as defined by Policy **5136**), network, and Internet connection and online educational services ("Education Technology" or "Ed-Tech") for educational purposes. Use of the Education Technology is a privilege, not a right. When using the Ed-Tech, students must conduct themselves in a responsible, efficient, ethical, and legal manner. Unauthorized or inappropriate use of the Ed-Tech, including any violation of these guidelines, may result in cancellation of the privilege, disciplinary action consistent with the Student Handbook, and/or civil or criminal liability. Prior to accessing the Education Technology students and parents of minor students must sign the Student Education Technology Acceptable Use and Safety Agreement. Parents are encouraged to discuss their values with their children and encourage students to make decisions regarding their use of the Ed-Tech that is in accord with their personal and family values, in addition to the Board's standards. Students must complete a mandatory training session/program before being permitted to access the Education Technology and/or being assigned a school e-mail address.

Smooth operation of the Board's Education Technology relies upon users adhering to the following guidelines. The guidelines outlined below are not exhaustive, but are provided so that users are aware of their general responsibilities.

A. Students are responsible for their behavior and communication using the Education Technology. All use of the Education Technology must be consistent with the educational mission and goals of the District.

B. Students may only access and use the Education Technology by using their assigned account and may only send school-related electronic communications using their District-assigned email addresses. Use of another person's account/email address/password is prohibited. Students may not allow other users to utilize their account/email address/password. Students may not go beyond their authorized access. Students are responsible for taking steps to prevent unauthorized access to their accounts by logging off or "locking" their computers/laptops/tablets/personal communication devices when leaving them unattended.

C. Students may not intentionally seek information on, obtain copies of, or modify files, data or passwords belonging to other users, or misrepresent other users on the District's Network. Students may not intentionally disable any security features of the Education Technology.

D. Students may not use the Education Technology to engage in "hacking" or other illegal activities (e.g., software pirating; intellectual property violations; engaging in slander, libel, or harassment; threatening the life or safety of another; stalking; transmission of obscene materials or child pornography; including sexting; fraud; sale of illegal substances and goods).

1. Slander and libel are terms defined specifically in law. Generally, slander is "oral communication of false statements injurious to a person's reputation," and libel is "a false publication in writing, printing, or typewriting or in signs or pictures that maliciously damages a person's reputation or the act or an instance of presenting such a statement to the public." (The American Heritage Dictionary of the English Language. Third Edition is licensed from Houghton Mifflin Company. Copyright © 1992 by Houghton Mifflin Company. All rights reserved.) Students shall not knowingly or recklessly post false or defamatory information about a person or organization. Students are reminded that material distributed over the Internet is "public" to a degree no other school publication or utterance is. As such, any remark may be seen by literally millions of people and harmful and false statements will be viewed in that light.

2. Students shall not use the Education Technology to transmit material that is threatening, obscene,

disruptive, or sexually explicit or that can be construed as harassment or disparagement of others based upon their race, national origin, sex, sexual orientation or transgender identity, age, disability, religion, or political beliefs. Sending, sharing, viewing or possessing pictures, text messages, e-mails or other materials of a sexual nature (i.e. sexting) in electronic or any other form, including the contents of a personal communication device or other electronic equipment is grounds for discipline. Such actions will be reported to local law enforcement and child services as required by law.

E. Transmission of any material in violation of any State or Federal law or regulation, or Board policy is prohibited.

F. Any use of the Education Technology for commercial purposes (e.g., purchasing or offering for sale personal products or services by students), advertising, or political lobbying is prohibited. This provision shall not limit the use of the Education Technology by students for the purpose of communicating with elected representatives or expressing views on political issues.

G. Use of the Education Technology to engage in cyberbullying is prohibited. ""Cyberbullying" is defined as the use of information and communication technologies such as e-mail, cell phone and pager text messages, instant messaging (IM), defamatory personal Web sites, and defamatory online personal polling Web sites, to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm others." [Bill Belsey (http//www.cyberbullying.ca)]

Cyberbullying includes, but is not limited to the following:

1. posting slurs or rumors or other disparaging remarks about a student on a web site or on weblog;

2. sending e-mail or instant messages that are mean or threatening, or so numerous as to drive up the victim's cell phone bill;

3. using a camera phone to take and send embarrassing and/or sexually explicit photographs/recordings of students;

4. posting misleading or fake photographs of students on web sites.

H. Students are expected to abide by the following generally-accepted rules of online etiquette:

1. Be polite, courteous, and respectful in your messages to others. Use language appropriate to school situations in any communications made through the Education Technology. Do not use obscene, profane, lewd, vulgar, rude, inflammatory, sexually explicit, defamatory, threatening, abusive or disrespectful language in communications through the Education Technology (including, but not limited to, public messages, private messages, and material posted on web pages).

2. Do not engage in personal attacks, including prejudicial or discriminatory attacks.

3. Do not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a student is told by a person to stop sending him/her messages, the student must stop.

4. Do not post information that, if acted upon, could cause damage or a danger of disruption.

5. Never reveal names, addresses, phone numbers, or passwords of yourself or other students, family members, teachers, administrators, or other staff members while communicating on the Internet. This prohibition includes, but is not limited to, disclosing personal identification information on commercial

web sites.

6. Do not transmit pictures or other information that could be used to establish your identity without prior approval of a teacher.

7. Never agree to get together with someone you "meet" on-line without parent approval and participation.

8. Check e-mail frequently, and delete e-mail promptly to avoid excessive use of the electronic mail disk space.

9. Students should promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable, especially any e-mail that contains sexually explicit content (e.g. pornography). Students should not delete such messages until instructed to do so by a staff member.

I. Use of the Education Technology to access, process, distribute, display or print child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors is prohibited. If a student inadvertently accesses material that is prohibited by this paragraph, s/he should immediately disclose the inadvertent access to the teacher or building principal.

J. Malicious use of the Education Technology to develop programs that harass other users or infiltrate a computer/laptop/tablet or computer system and/or damage the software components of a computer or computing system is prohibited. Students may not engage in vandalism or use the Education Technology in such a way that would disrupt its use by others. Vandalism is defined as any malicious or intentional attempt to harm, steal or destroy data of another user, school networks, or technology hardware. This includes but is not limited to uploading or creation of computer viruses, installing unapproved software, changing equipment configurations, deliberately destroying or stealing hardware and its components, or seeking to circumvent or bypass Network security and/or the Board's technology protection measures. Students also must avoid intentionally wasting limited resources. Students must immediately notify the teacher or building principal if they identify a possible security problem. Students should not go looking for security problems, because this may be construed as an unlawful attempt to gain access.

K. All communications and information accessible via the Internet should be assumed to be private property (i.e. copyrighted and/or trademarked). All copyright issues regarding software, information, and attributions/acknowledgement of authorship must be respected. Rules against plagiarism will be enforced.

L. Downloading of information onto school-owned equipment or contracted online educational services is prohibited, without prior approval from the Network Manager. If a student transfers files from information services and electronic bulletin board services, the student must check the file with a virus-detection program before opening the file for use. Only public domain software may be downloaded. If a student transfers a file or installs a software program that infects the District's Education Technology with a virus and causes damage, the student will be liable for any and all repair costs to make the Education Technology once again fully operational.

M. Students may use real-time electronic communication, such as chat or instant messaging, only under the direct supervision of a teacher or in moderated environments that have been established to support educational activities and have been approved by the Board, Superintendent or building principal. Students may only use their school-assigned accounts/email addresses when accessing, using or participating in real-time electronic communications for education purposes.

N. Users have no right or expectation of privacy when using Education Technology. This District reserves the right to access and inspect any facet of the Education Technology, including, but not limited to, computers, laptops. Tablets, personal communication devices, networks, or internet connections or online educational

services, e-mail or other messaging or communication systems or any other electronic media within its technology systems or that otherwise constitutes its property and any data, information, e-mail, communication, transmission, upload, download, message or material of any nature or medium that may be contained therein. A student's use of the Ed-Tech constitutes his/her waiver of any right to privacy in anything s/he creates, stores, sends, transmits, uploads, downloads or receives on or through the Ed-Tech and related storage medium and equipment. Routine maintenance and monitoring, utilizing both technical monitoring systems and staff monitoring, may lead to discovery that a user has violated Board policy and/or the law. An individual search will be conducted if there is reasonable suspicion that a user has violated Board policy and/or law, or if requested by local, State or Federal law enforcement officials. Students' parents have the right to request to see the contents of their children's files, e-mails and records.

O. Use of the Internet and any information procured from the Internet is at the student's own risk. The Board makes no warranties of any kind, either express or implied, that the functions or the services provided by or through the Education Technology will be error-free or without defect. The Board is not responsible for any damage a user may suffer, including, but not limited to, loss of data, service interruptions, or exposure to inappropriate material or people. The Board is not responsible for the accuracy or quality of information obtained through the Internet. Information (including text, graphics, audio, video, etc.) from Internet sources used in student papers, reports, and projects must be cited the same as references to printed materials. The Board will not be responsible for financial obligations arising through the unauthorized use of the Education Technology. Students or parents of students will indemnify and hold the Board harmless from any losses sustained as the result of misuse of the Education Technology by the student.

P. Disclosure, use and/or dissemination of personally identifiable information of minors via the Internet is prohibited, except as expressly authorized by the minor student's parent/guardian on the "Student Education Technology Acceptable Use and Safety Agreement Form."

Q. Proprietary rights in the design of web sites hosted on Board–owned or leased servers remains at all times with the Board.

R. File-sharing is strictly prohibited. Students are prohibited from downloading and/or installing file-sharing software or programs on the Education Technology.

S. Since there is no central authority on the Internet, each site is responsible for its own users. Complaints received from other sites regarding any of the District's users will be fully investigated and disciplinary action will be taken as appropriate.

T. Preservation of Resources and Priorities of Use: Computer resources are limited. Because space on disk drives and bandwidth across the lines which connect the District's Ed-Tech (both internally and externally) are limited, neither programs nor information may be stored on the system without the permission of the network manager. Each student is permitted reasonable space to store e-mail, web, and personal files. The Board reserves the right to require the purging of files in order to regain disk space. Students who require access to the Education Technology for class- or instruction-related activities have priority over other users. Students not using the Education Technology for class-related activities may be "bumped" by any student requiring access for class- or instruction-related purpose.

P.L. 106-554, Children's Internet Protection Act of 2000
47 U.S.C. 254(h), (1), Communications Act of 1934, as amended (2003)
20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)
18 U.S.C. 1460
18 U.S.C. 2246
18 U.S.C. 2256
20 U.S.C. 6777, 9134 (2003)

Revised 12/09
Revised 11/17/14