

2103 Acceptable Use Policy

Purpose

Maeser offers students and employees access to electronic and network resources for appropriate educational use.

The Internet provides students access to massive amounts of educationally useful information. Some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate, obscene, or offensive. However, Maeser provides Internet access to further its legitimate educational goals.

Maeser uses filtering software to limit student exposure to inappropriate materials; in addition, teachers monitor classroom use of the Internet to the best of their ability. However, no filtering and monitoring system is capable of blocking 100% of the inappropriate material available on the Internet.

1. Definitions

- a. "Electronic device" means a device that is used for audio, video, or text communication or any other type of computer or computer-like instrument including but not limited to:
 - i. A smart phone;
 - ii. A smart or electronic watch
 - iii. A tablet; or
 - iv. A virtual reality device.
- b. "Guest" means an individual:
 - i. Who is not a student, employee, or designated volunteer of a public school; and
 - ii. Who is on school property or at the site of a school-sponsored activity or event.
- c. "Inappropriate matter" means pornographic or indecent material as defined in Subsection 76-10-1253(1)(a).
- d. "Maeser-owned electronic device" means a device that is used for audio, video, text communication, or other type of computer or computer-like instrument that is identified as being owned, provided, issues or lent by Maeser to a student or employee.
- e. "Privately-owned electronic device" means a device, including an electronic device that is used for audio, video, text communication, or other type of computer or computer-like instrument that is not owned or issued by Maeser to a student, or employee.

Source: Utah Admin. Code r. 277-495 (2019).

2. Guidelines for Social Media Use

- a. Be aware of the permanency of the Internet and think before posting.
- b. Act responsibly since everything online may be accessible to the public.

- c. Treat others with respect, protect confidential information, and obey copyright law.
 - d. Post positive, meaningful, and thoughtful comments.
 - e. Disagree courteously, without disparaging comments.
 - f. If something you are about to post makes you uncomfortable, take a minute to consult with others.
 - g. Do not bully others online.
 - h. Be open offline about what you experience online. Report inappropriate online behavior.
 - i. Only comment on things about which you are well informed.
 - j. Do not violate privacy, confidentiality, or legal guidelines.
 - k. Ask permission before posting pictures or videos of others.
3. Prohibitions
- a. Students and/or employees are subject to the school discipline policy if they use electronic devices and/or network resources to
 - i. bully, humiliate, harass, or intimidate school-related individuals, including students, employees, and guests, consistent with Utah Admin. Code r. 277-609 and r. 277-613; or
 - ii. Violate local, state, or federal law
 - iii. Access inappropriate matter on the Internet and World Wide Web while using Maeser equipment, services, or connectivity whether on or off school property.
 - b. Unauthorized access
 - i. Any attempt to bypass school security or content filters using web proxy sites, VPN, alternate search engines or other methods is forbidden. Attempting to disable safe search functionality is forbidden. Unauthorized intrusion (AKA "hacking") of servers, workstations, or network devices is forbidden.
 - c. Unauthorized disclosure, use and dissemination of personal student information
 - d. Unauthorized use that would cause invasions of reasonable expectations of student and employee privacy
 - e. Students are prohibited from using privately-owned electronic devices during standardized assessments.
 - f. Connecting unauthorized computers or other electronic equipment to the network
 - g. Assuming network identities, credentials, and access that have not been given to you
 - h. Downloading or using unapproved apps, extensions or plugins on school computers
 - i. Changing or attempting to change administrative settings on school computers
 - j. Creating or sharing Internet connections

- k. Sharing your Maeser username and password with others
 - l. Sending, storing, or displaying offensive messages, pictures, or other content
 - m. Using obscene language
 - n. Giving personal information, such as complete name, phone number, address, or identifiable photo, without family permission
 - o. Cyber bullying, hate mail, harassment, insults, personal attacks, discriminatory jokes and remarks
 - p. Invasion of privacy through the unauthorized creation of sound recordings, videos, or images;
 - q. Damaging or modifying computers, computer systems, or computer networks; downloading, installing, or using games, audio files, video files, or other applications without permission to do so
 - r. Attempting to bypass network security, filtering and monitoring
 - s. Violating copyright laws
 - t. Trespassing in others' folders, work, or files
 - u. Intentionally wasting resources
 - v. Posting, sending, or storing information that could endanger others or is illegal, including pornography
 - w. Employing the school computers, network, or Internet resources for non-academic, personal, commercial, political, financially gainful, or fraudulent purposes
4. Students have no expectation of privacy in their use of Maeser-owned devices or Maeser network resources, including stored files and email. Maeser reserves the right to monitor student use of electronic resources to the fullest extent authorized by law.
5. Violations of this policy may result in confiscation of Maeser-owned electronic devices or restriction of access on the Maeser's network.
6. Students
- a. Maeser allows students to possess their privately-owned electronic devices while on campus. However, the use of privately-owned electronic devices while on campus is a privilege, and not a right, and is subject to Maeser policies and discipline.
 - b. Privately-Owned Electronic Devices
 - i. Students may possess and use their privately-owned electronic device(s) before and after school, during passing periods, and at lunch.
 - ii. Students may not use their privately-owned electronic devices in class, unless given explicit approval by the teacher.
 - 1. Privately-owned electronic devices should be kept out of sight and turned off during instructional time.
 - iii. Students who use privately-owned devices in class without explicit teacher approval may have their device confiscated. The school is

not responsible for any damages or loss that may occur to confiscated devices.

- iv. Consequences for unauthorized use of personal electronic devices.
 1. 1st violation: Confiscation of device until the end of the class period.
 2. 2nd violation: Device turned in to Administration, and it will be returned at the end of the school day.
 3. 3rd violation: Administration will return the device to a parent/guardian.
 4. 4th violation: Loss of privately-owned electronic device privileges on campus.
 - a. If a student who has lost the privilege to possess a privately-owned electronic device on campus continues to bring it to campus, that student will be subject to disciplinary action, up to and including suspension from school.
- v. Exceptions
 1. Exceptions to this section of the policy may be granted at the sole discretion of Maeser Administration in certain circumstances, including but not limited to:
 - a. Medical needs
 - b. Emergency situations
 - c. Special educational circumstances (e.g., as part of a 504 or IEP)
 2. Parents seeking an exception for any reason must contact Maeser Administration.
- vi. Confiscated Devices
 1. School employees may confiscate a privately-owned electronic device.
 2. School employees may not search or review material or numbers stored on student electronic devices except under compelling circumstances.
 - a. School employees may search an electronic device if the device is found by the employee for the limited purpose of determining the device's owner.
 - b. Maeser Administration may search a privately-owned electronic device in accordance with the provisions of the Discipline Policy.
 3. Maeser will do its best to guard and protect confiscated electronic devices, but are not responsible for loss, damage, theft.
 4. Maeser will make a good faith effort to notify parent(s) or designated individuals that the confiscated, privately-owned

electronic device is in Maeser's possession. Time and resources permitting, Maeser will hold onto the electronic device until the parent(s) or designated individuals are able to pick up the electronic device. However, Maeser will only hold onto the electronic device for a reasonable amount of time, typically until the end of the school year. Prior to disposing of electronic devices that have not been picked up, Maeser will make reasonable attempts to return devices. Maeser may also, at its own discretion, make reasonable attempts to clear them of personal data before disposing of electronic devices that have not been picked up.

- c. Students are personally responsible for devices assigned or provided to them by Maeser, both for loss or damage of electronic devices and use of electronic devices consistent with Maeser's directives.
 - i. Students who misuse, mistreat, or otherwise abuse electronic devices assigned or provided to them by Maeser may have their access to electronic devices and the network restricted or revoked.
 - 1. Students who break or otherwise render inoperative an electronic device that has been assigned to them by Maeser may be held financially liable for the replacement cost of the device.
- d. Misuse of Maeser-owned electronic devices at any time, including outside of school hours, may result in revocation of the ability to use Maeser-owned electronic devices, as well as additional discipline in accordance with the Maeser Discipline Policy.
- e. Misuse of privately-owned electronic devices during school hours or during a school-sponsored activity may result in confiscation of the device and/or additional disciplinary action in accordance with the Maeser Discipline Policy.
 - i. Teachers may confiscate privately-owned electronic devices if a student is using it in violation of classroom or school rules or policies. See Maeser Discipline Policy for additional information.
- f. Should a student's parent or guardian wish to establish more restrictive boundaries for that student's use of Maeser's electronic resources, they must submit a written request to Maeser Administration setting forth their proposed criteria. Maeser will make reasonable efforts to comply with such requests, subject to its own resource constraints and the educational mission of the school.

7. Employees

- a. Employees who use electronic devices to access inappropriate material on Maeser-owned electronic devices, or privately-owned electronic devices on school property, at school-sponsored events or using school

- connectivity may have criminal, employment or student disciplinary consequences, and if appropriate, may be reported to law enforcement.
- b. Employees are responsible for Maeser-issued electronic devices at all times and misuse of an electronic device may have employment consequences, regardless of the user.
 - c. Employees have responsibilities in educating students on appropriate online activities (as required by Utah Code Ann. § 53G-7-1202), and in supervising such activities.
8. Reporting misuse
 - a. Students may report misuse of electronic devices to a teacher, counselor, or school administrator, who may then conduct an investigation.
 - b. Teachers may report misuse of electronic devices to their department chair or a member of the Administration.
 9. The school computer and network resources are provided for students to conduct research, complete assignments, and communicate with others in connection with their Maeser-related academic and extracurricular activities. Access to these resources and services is only available with the permission of a parent or guardian. Network access will only be granted to a student if the student and their parent/guardian complete, sign, and return a copy of the Network Access Permission form. Note: students that do not have permission to access network resources may not be able to participate in some classes.

Reviewed & Approved 8 October 2019