EAGLE MOUNTAIN-SAGINAW INDEPENDENT SCHOOL DISTRICT GUIDELINES FOR RESPONSIBLE USE OF TECHNOLOGY RESOURCES

Introduction and Purpose of this Document

Technology resources, including Internet access, will be used to promote innovation and educational excellence consistent with the Texas Essential Knowledge and Skills and the goals of the Eagle Mountain-Saginaw Independent School District (“EMS ISD” or “District.”) EMS ISD believes that the access to information resources and opportunities for collaboration, when used in a responsible manner, will provide educational benefit for students and employees. To foster a culture of excellence, Eagle Mountain-Saginaw ISD embraces what it means to be a future ready learner by engaging our students in safe, ethical practices in a digital environment. The Responsible Use Policy is based on the premise that future ready students need to learn how to be responsible users, make informed choices, and exercise accountability for their behavior. When using the System and technology devices, employee and student behavior should reflect the same responsible, ethical behavior as outlined in the Employee Handbook and/or Student Handbook. This document is intended to provide clarification on those expectations as they apply to technology usage and is consistent with district policy.

Annual Review

Users are required to review these guidelines at the beginning of each school year and agree to the terms in writing. The user is required to acknowledge receipt and understanding of the district’s Responsible Use Guidelines for Technology as part of their review of the Employee and/or Student Handbook.

Digital Citizens of Eagle Mountain-Saginaw ISD

Employees and students using technology resources should practice appropriate digital citizenship. All information transmitted digitally should be considered public and permanent. Appropriate digital citizenship includes:

- **Respecting Yourself and Others**
  Users will apply appropriate language/content in all online posts, as users continuously represent Eagle Mountain-Saginaw ISD and yourself whenever and wherever they use online communications. Users will not use technology resources to bully, harass or tease other people. Users will not make or share audio or video recordings of others without prior permission from the subject. User will not pose as a user other than him or herself when online. Users will not access, download, or modify accounts, files, or data belonging to others. Users will adhere to current copyright laws.

- **Protecting Yourself and Others**
  Users will not publish personally identifiable information or data for themselves or anyone else. Users are the custodian of their accounts and are responsible for all activity initiated by and/or performed under their accounts. It is the responsibility of each user to appropriately secure account credentials (user IDs/passwords) and to maintain and backup all data. If a user is uncertain whether a specific computer activity is permitted or appropriate, he/she should ask a teacher/administrator before engaging in the activity. (This includes passwords.) Users will help maintain a safe computing environment by notifying appropriate campus officials of inappropriate behavior, online bullying or harassment, vulnerabilities, risks, and breaches involving campus technology.

- **Respecting and Protecting Intellectual Property**
  Users will adequately cite websites, books, media, etc. used in creating presentations, student assignments, or other school projects. Users will respect all copyrights, requesting permission for the use of software, media, and the intellectual property of others.

Children’s Online Privacy Protection Act (COPPA)

For students under the age of 13, the Children’s Online Privacy Protection Act (COPPA) requires additional parental permission for educational software tools. Parents wishing to deny access to these educational tools must do so in writing to the campus principal indicating their child should be denied access to these tools. Examples of these tools are Microsoft Office 365, blogs, online presentation tools, and other digital resources.

Use of District Provided Internet Access

The district’s goal is to increase student access to digital tools and facilitate immediate access to technology-based information including textbooks, teacher built content, and other digital materials. The district will utilize a filtered, wireless network as defined by the federal Children’s Internet Protection Act (CIPA) through which all student devices will connect. Any attempt to disable or circumvent (aka proxy) the district filter is strictly prohibited. Students will be allowed to use the Internet between classes and in the cafeteria setting at the discretion of campus leadership. Causing network congestion through mass consumption of system resources is prohibited. Examples of this include extensive video or game streaming and mass email forwards.

Monitoring of Computer and Internet Usage

Users should have no expectation of privacy regarding their use of district property and technology resources. In general, communications or transmissions made through technology resources should never be considered private or confidential. The district reserves the right to monitor the use of its network and all technology resources as it deems necessary to ensure the safety and integrity of its network, diagnose problems, investigate reports of illegal or impermissible activity, and ensure user compliance with state and federal laws and the district’s policies. In addition, users should be aware that the district will comply with lawful orders of courts, such as subpoenas and search warrants. The district is also subject to the Texas Public Information Act, which may require disclosure of information transmitted through its technology resources, including e-mail communications.

Bring Your Own Device (BYOD)

EMS ISD permits students to bring their own device for use during the school day and connect to the guest network. This Internet access is filtered by the district on personal technology devices in the same manner as district-owned equipment. If network access is needed, connection to the filtered, wireless network provided by the district is required. BYOD devices are the sole responsibility of the student owner. The campus or district assumes no responsibility for personal technology devices if they are lost, loaned, damaged or stolen. Students are prohibited from trading or selling these items to other students on district property, including school buses. Each student is responsible for his/her own device: setup, maintenance, charging, and security. Campus administrators and staff members have the right to prohibit use of BYOD devices at certain times, during designated activities (i.e. campus presentations, theatrical performances, or guest speakers) or designated locations (restrooms and locker rooms) while students are on campus. An administrator may examine a student’s personal technology device and search its contents, in accordance with disciplinary guidelines.

Appropriate Behavior

Access to the district’s computer/network/Internet is a privilege, not a right. Campus and district Administrators are responsible for determining what is considered to be inappropriate use of the Eagle Mountain-Saginaw ISD computer network. They may request to disable a user’s account or network access at any time. Student discipline will be referred to campus administration, while staff behavior will be referred to the employee’s supervisor and Human Resources. All actions on a district issued device may be monitored at any time. Both district-issued, and personal technology devices, are subject to examination in accordance with disciplinary guidelines if there is reason to believe that the Responsible Use Guidelines have been violated.

Electronic Communication

A certified employee, licensed employee, or any other employee designated in writing by the Superintendent or a campus principal may use electronic communication, as this term is defined by law, with currently enrolled students only about matters within the scope of the employee's professional responsibilities. Unless an exception has been made in accordance with the employee handbook or other administrative regulations, an employee shall not use a personal electronic communication platform, application, or account to communicate with currently enrolled students.

Unless authorized above, all other employees are prohibited from using electronic communication directly with students who are currently enrolled in the District. The employee handbook or other administrative regulations shall further detail:

1. Exceptions for family and social relationships;
2. The circumstances under which an employee may use text messaging to communicate with individual students or student groups;
3. Hours of the day during which electronic communication is discouraged or prohibited; and
4. Other matters deemed appropriate by the Superintendent or designee.

In accordance with ethical standards applicable to all District employees, an employee shall be prohibited from using electronic communications in a manner that constitutes prohibited harassment or abuse of a District student; adversely affects the student's learning, mental health, or safety; includes threats of violence against the student; reveals confidential information about the student; or constitutes an inappropriate communication with a student, as described in the Educators' Code of Ethics.

An employee shall have no expectation of privacy in electronic communications with students. Each employee shall comply with the District's requirements for records retention and destruction to the extent those requirements apply to electronic communication.

Personal Use

All employees shall be held to the same professional standards in their public use of electronic communication as for any other public conduct. If an employee's use of electronic communication violates state or federal law or District policy, or interferes with the employee's ability to effectively perform his or her job duties, the employee is subject to disciplinary action, up to and including termination of employment.

Reporting Improper Communication

In accordance with administrative regulations, an employee shall notify his or her supervisor when a student engages in improper electronic communication with the employee.

Disclosing Personal Information

An employee shall not be required to disclose his or her personal email address or personal phone number to a student.

Physical Care of District-Provided Property

- Keep the device secure and damage free.
- Keep track of your device, charger, and cord.
- Bring your charged device to school each day.
- Make sure to store your device in a secure environment when not in use. Some examples of unsecure locations: car, unlocked athletic locker, bleachers, etc.
- Devices are not water resistant. Take precautions when dealing with liquids and food.
- Devices are not intended to have heavy weight placed on them. Do not stack things on top of the device.
- Safely transport your device in a weather resistant manner.
- When using campus devices (iPads, laptop carts, etc.), follow campus and district procedures and guidelines.

Security

The district strives to help students and employees make informed choices and exercise accountability when using digital content. In the unlikely situation that a user accesses inappropriate or harmful material, they must immediately discontinue use and report the incident to the supervising staff member. Any student or employee identified as a security risk or as having violated the Responsible Use Guidelines may be denied access to the district's system. Other consequences may also be assigned.

The use of smart speakers (Alexa, Echo, etc.) on the district network is strictly prohibited. An employee who knowingly brings prohibited materials into the school's electronic environment will be subject to suspension of access and/or revocation of privileges on the district's system and will be subject to disciplinary action in accordance with the Board-approved Employee Handbook.

Content/Third-Party Supplied Information

Employees with access to the district's systems should be aware that use of the systems may provide access to other electronic communication systems, such as chat rooms and social media. The global electronic network that may contain inaccurate and/or objectionable material. It is the employee's responsibility to make ethical decisions when interacting in an online environment. Be aware that it is the employee's responsibility to ensure the security of student data when using non-district approved digital resources.

Employees will not upload identifiable student information (first and last names, ID numbers, etc.) into web-based applications without express consent of a supervisor or district administrator.

Commercial and Political Use

Use of the system for any type of income-generating activity is prohibited. Advertising the sale of products, whether commercial or personal is prohibited. Marketing by non-EMS ISD organizations or the use of the system for promoting activities or events for individuals or organizations not directly affiliated with or sanctioned by the district is prohibited. Users may not use their accounts for non-school related activities including but not limited to: financial gain, personal advertising, promotion, non-government related fundraising, or public relations, political advertising, or religious proselytizing.

Email

District-provided email accounts are to be used for district business. This includes sharing work and communicating digitally with colleagues, teachers, students, and parents. Employees should keep personal and confidential information private. The district uses multiple email security systems to scan both inbound and outbound email for spam, viruses, appropriate content, attachments, and bulk marketing. This means the system blocks access to language and visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors.

Disclaimer

The district’s system is provided on an “as is, as available” basis. The district does not make any warranties, whether expressed or implied, with respect to any services provided by the system and any information or software contained therein. The district does not guarantee 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. Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not the district. The district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the district’s electronic communications system. The district makes every effort to limit access to objectionable material; however, controlling all such materials on the computer/network/Internet is impossible, even with filtering in place. With global access to computers and people, a risk exists that students may access material that may not be of educational value in the school setting.

Acknowledgment and Agreement

I have read and will abide by these Responsible Use Guidelines and understand use of technology resources is a privilege, not a right. I understand that if I fail to comply with these Guidelines, I will be subject to appropriate disciplinary consequences. My signature on the Acknowledgment in the EMS ISD Employee Handbook or EMS ISD Student Handbook confirms my receipt of these Guidelines and my agreement to follow them as a condition of access to district technology resources.