MRUSD RESPONSIBLE COMPUTER, NETWORK & INTERNET USE

Purpose

The Maple Run Unified School District recognizes that information technology (IT) is integral to learning and educating today's children for success in the global community and fully supports the access of these electronic resources by students and staff. The purpose of this policy is to:

1. Create an environment that fosters the use of information technology in a manner that supports and enriches the curriculum, provides opportunities for collaboration and enhances staff professional development.
2. Ensure the district takes appropriate measures to maintain the safety of everyone that accesses the district's information technology devices, network, and web resources.
3. Comply with the requirements of applicable federal and state laws that regulate the provision of access to the internet and other electronic resources by school districts.

General DIgital Policy

It is the policy of the Maple Run Unified School District to provide students and staff access to a multitude of information technology (IT) resources including the Internet. These resources provide opportunities to enhance learning and improve communication within our community and with the global community beyond. However, with the privilege of access comes the responsibility of students, teachers, staff, and the public to exercise responsible use of these resources. The use by students, staff, or others of district IT resources is a privilege, not a right.

The same rules and expectations govern student use of IT resources as apply to other student conduct and communications, including but not limited to the district's harassment and bullying policies.

The district's computer and network resources are the property of the district. Users shall have no expectation of privacy in anything they create, store, send, receive, or display on or over the district's computers or network resources, including personal files and electronic communications.

The superintendent is responsible for establishing procedures governing the use of IT resources consistent with the provisions of this policy. These procedures must include:

1. An annual process for educating students about responsible digital citizenship. As defined in this policy, a responsible digital citizen is one who:
    - **Respects One's Self.** Users will maintain appropriate standards of language and behavior when sharing information and images on social networking websites and elsewhere online. Users refrain from distributing personally identifiable information about themselves and others.
    - **Respects Others.** Users refrain from using technologies to bully, tease, or harass other people. Users will report incidents of cyberbullying and harassment in accordance with the district's policies on bullying and harassment. Users will also refrain from using another person's system account or password or from presenting themselves as another person.
    - **Protects One's Self and Others.** Users protect themselves and others by reporting abuse and not forwarding inappropriate materials and communications. They are responsible at all times for the proper use of their account by not sharing their system account password.
    - **Respects Intellectual Property.** Users suitably cite any and all use of websites, books, media, etc.
    - **Protects Intellectual Property.** Users request to use the software and media others produce.

2. Provisions necessary to ensure that Internet service providers and other contractors comply with applicable restrictions on the collection and disclosure of student data and any other confidential information stored in district electronic resources.

3. Technology protection measures that provide for the monitoring and filtering of online activities by all users of district IT, including measures that protect against access to content that is obscene, child pornography, or harmful to minors.

4. Methods to address the following:
    - Control of access by minors to sites on the Internet that include inappropriate content, such as content that is:
        - Lewd, vulgar, or profane
        - Threatening
        - Harassing or discriminatory
        - Bullying
        - Terroristic
        - Obscene or pornographic

- The safety and security of minors when using electronic mail, social media sites, and other forms of direct electronic communications.
- Prevention of unauthorized online access by minors, including “hacking” and other unlawful activities.
- Unauthorized disclosure, use, dissemination of personal information regarding minors.
- Restriction of minors’ access to materials harmful to them.

5. A process whereby authorized persons may temporarily disable the district’s Internet filtering measures during use by an adult to enable access for bona fide research or other lawful purposes.

Policy Application

This policy applies to anyone who accesses the district’s network, collaboration and communication tools, and/or student information systems either on-site or via a remote location, and anyone who uses the district’s IT devices either on or off-site.

Limitation/Disclaimer of Liability

The District is not liable for unacceptable use or violations of copyright restrictions or other laws, user mistakes or negligence, and costs incurred by users. The District is not responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the District’s electronic resources network including the Internet. The District is not responsible for any damage experienced, including, but not limited to, loss of data or interruptions of service. The District is not responsible for the accuracy or quality of information obtained through or stored on the electronic resources system including the Internet, or for financial obligations arising through their unauthorized use.

Enforcement

The district reserves the right to revoke access privileges and/or administer appropriate disciplinary action for misuse of its IT resources. In the event there is an allegation that a user has violated this policy, the school district will handle the allegation consistent with the student disciplinary policy.

Allegations of staff member violations of this policy will be processed in accordance with contractual agreements and legal requirements.

Chromebook Care and Home Use guidelines for Families

- Use the device only on flat work surfaces like a kitchen table or desk, and never on the student's lap, the floor, or while laying down on a bed or sofa to prevent accidental damage.
- Have students use the device in public spaces in the home, and never in the student's bedroom with the door closed. This helps establish that parents can more easily monitor usage.
- Never have food or drinks near the device to avoid catastrophic liquid spill damage.
- Never place a device on a flat horizontal surface where people sit or stand like the floor or a chair to prevent accidental damage.
- Charge the device while it rests on a table or other safe flat surface, but not in its carrying case. Many carrying cases have padding for protection, but this acts like a blanket and can cause devices to overheat while charging.

BYOD Guidelines (Bring Your Own Device Guidelines)

For students who opt to use their own device instead of one provided by the school:

- Students who repeatedly use their BYOD in ways that violate the school technology 'Responsible Use Policy' could lose their ○ BYOD privileges and be assigned a school-issued Chromebook.
- Students must bring their BYOD device fully charged to school.
- Students must bring their chargers to school.
- A student's choice of BYOD device needs to be capable of supporting the student's learning requirements. Phones and tablets without external keyboards are not acceptable BYOD devices.
- School-owned software installed on student devices must be uninstalled by the Technology Department before students are cleared for check out at the end of the academic year or withdrawal from school.
- Virus and Malware protection and an up-to-date operating system are strongly recommended on BYOD devices.
- MRUSD does not provide technical support or repair for BYOD devices.
- MRUSD is NOT responsible for the theft or damage of a BYOD device. Students are fully responsible for their devices. In case of theft or damage in school, students are advised to contact an administrator or their teacher. Some devices have a device locator; it is recommended to enable this feature if possible.

Device Repair

- Devices provided by MRUSD which need repair should be brought to the Tech office. All repairs must be performed by authorized district technology staff.