

**MSAD #28 POLICY****STUDENT COMPUTING DEVICE and INTERNET USE RULES**

These rules implement Board policy IJNDB (Student Computing Device and Internet Use). Each student is responsible for his/her actions and activities involving school district computing devices, networks and Internet services, and for his/her computing device files, passwords and accounts.

The rules are intended to provide general guidelines and examples of prohibited uses, but do not attempt to state all required or prohibited activities by users. Failure to comply with Board policy IJNDB and these rules may result in loss of computing devices and Internet access privileges, disciplinary action and/or legal action. Students, parents and school staff who have questions about whether a particular activity is prohibited are encouraged to contact a building administrator or the Technology Director. These rules apply to all school computing devices and all school-provided devices wherever used, and all uses of school servers, Internet access and networks regardless of how they are accessed.

**A. Acceptable Use**

Student access to MSAD #28's computing devices, networks and Internet services are provided for educational purposes, research, and incidental personal use consistent with MSAD #28's educational mission, curriculum and instructional goals, as long as personal use of school computing devices does not interfere with student performance, with system operations or with other system users.

All Board policies, school rules and expectations concerning student conduct and communications apply when students are using school computing devices, whether on or off school property.

Students are further expected to comply with these rules and all specific instructions from the teacher or other supervisory staff member/volunteer when accessing MSAD #28's computing devices, networks, and Internet services.

**B. Consequences for Violation of Computing Device Use Policy and Rules**

Student use of MSAD #28 computing devices, networks, and Internet services is a privilege, not a right. Compliance with the school district's policies and rules concerning computing devices use is mandatory. Students who violate these policies and rules may have their computing devices privileges limited, suspended, or revoked. Such violations may also result in disciplinary action, referral to law enforcement, and/or legal action.

The building principal shall have the final authority to decide whether a student's privileges will be limited, suspended or revoked based upon the circumstances of the particular case, the student's prior disciplinary record, and any other pertinent

factors.

### C. **Prohibited Use**

The user is responsible for his/her actions and activities involving MSAD #28's computing devices, networks and Internet services and for his/ computing device files, passwords, and accounts. Examples of unacceptable uses that are expressly prohibited include, but are not limited to, the following:

1. **Accessing or Communicating Inappropriate Materials** -Accessing, submitting, posting, publishing, forwarding, downloading, scanning, or displaying materials or messages that are defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing, bullying, and/or illegal.
2. **Illegal Activities** -Using MSAD #28's computing devices, networks, and Internet services for any illegal activity or activity in violation of any other Board policies, procedures and/or school rules. The District assumes no responsibility for illegal activities of students while using school computing devices.
3. **Violating Copyrights** - Copying, downloading or sharing any type of copyrighted materials (including music or films) without the owner's permission (see Board policy/procedure EGAD - Copyright Compliance). The school district assumes no responsibility for copyright violations by students.
4. **Copying Software** - Copying or downloading/installing software without the express authorization of the Technology Coordinator. Unauthorized copying of software is illegal and may subject the copier to substantial civil and criminal penalties. The District assumes no responsibility for illegal software copying by students.
5. **Plagiarism**- Representing as one's own work any materials obtained on the Internet (such as term papers, articles, music, etc.). When Internet sources are used in student work, the author, publisher, and website must be identified.
6. **Misuse of Passwords/Unauthorized Access** -Sharing passwords, using other users' passwords without permission and/or accessing other users' accounts.
7. **Malicious Use/Vandalism** -Any malicious use, disruption or harm to MSAD #28's computing devices, networks, and Internet services, including, but not limited to, hacking activities and creation/uploading of computing devices viruses. Students are prohibited from modifying the hardware configuration of any computing device. Students may not install or run any software not owned and/or authorized by the District.
8. **Avoiding School Filters** - Students may not attempt to or use any software, utilities, or other means to access Internet sites or content blocked by the school filters.
9. **Unauthorized Access to Blogs/Social Networking Sites, Etc.** - Accessing blogs, social networking sites, etc. to which student access is prohibited.

### D. **No Expectation of Privacy**

MSAD #28 retains control and supervision of all computing devices, networks and

Internet services owned or leased by MSAD #28. MSAD #28 reserves the right to monitor all computing devices and Internet activity by students. Students have no expectations of privacy in their use of school computing devices, including e-mail and stored files and Internet access logs.

**E. Compensation for Losses, Costs and/or Damages**

The student and/or the student's parent/guardian shall be responsible for compensating MSAD #28 for any losses, costs, or damages incurred by MSAD #28 related to violations of policy IJNDB and/or these rules, including investigation of violations. The District assumes no responsibility for any unauthorized charges or costs incurred by a student while using District computing devices.

**F. Student Security**

A student should not reveal his/her full name, address or telephone number, social security number, or other personal information on the Internet. Students should never agree to meet people they have contacted through the Internet without parental permission. Students should inform their supervising teacher or parent if they access information or messages that are dangerous, inappropriate, or make them uncomfortable in any way.

**G. System Security**

The security of MSAD #28's computing devices, networks, and Internet services is a high priority. Any user who identifies a security problem must notify the Building Administrator or the Technology Director. The user shall not demonstrate the problem to others or access unauthorized material. Any user who attempts to breach system security, causes a breach of system security, or fails to report a system security problem shall be subject to disciplinary and/or legal action in addition to having his/her computing device privileges limited, suspended, or revoked.

**H. Additional Rules for Use of Privately-Owned Computing Devices by Students**

1. A student who wishes to use a privately-owned computing device in school must complete a Student Request to Use Privately-Owned Computing Device form. The form must be signed by the student, his/her parent, a sponsoring teacher, the building administrator, and the Technology Coordinator. There must be an educational basis for any request.
2. The Technology Coordinator will determine whether a student's privately-owned computing devices meets MSAD #28's network requirements.
3. Requests may be denied if it is determined that there is not a suitable educational basis for the request and/or if the demands on the District's network or staff would be unreasonable.
4. The student is responsible for proper care of his/her privately-owned computing device, including any costs of repair, replacement or any modifications needed to use the computing device at school.

5. The District is not responsible for damage, loss or theft of any privately-owned computing device.
6. Students are required to comply with all Board policies, administrative procedures, and school rules while using privately-owned computing devices at school.
7. Students have no expectation of privacy in their use of a privately-owned computing devices while at school. The District reserves the right to search a student's privately-owned computing devices if there is a reasonable suspicion that the student has violated Board policies, administrative procedures, or school rules, or engaged in other misconduct while using the computing device.
8. Violation of any Board policies, administrative procedures, or school rules involving a student's privately-owned computing device may result in the revocation of the privilege of using the computing device at school and/or disciplinary action.
9. The District may confiscate any privately-owned computing device used by a student in school without authorization as required by these rules. The contents of the computing device may be searched in accordance with applicable laws and policies.

Legal Reference:

- 47 USC § 254 (h) (5) (Children's Internet Protection Action)

Cross Reference:

- GCSA - Employee Computer and Internet Use
- IJNDB - Student Computing Devices and Internet Use Rules
- IJNDB-L - School Provided Device Use
- IJNDB-P – School Provided Device Use – Procedure
- EGAD - Copyright Compliance
- JIC - Student Code of Conduct

History:

Adopted: 01/12/00, 12/14/05, 01/20/10, 06/19/13

Reviewed: November 20, 2021