Milton Town School District

Procedure

F100P: STUDENT COMPUTER AND INTERNET USE PROCEDURE

These Procedures accompany Board policy on Student Computer and Internet Use. Each student is responsible for his/her actions and activities involving district's computers, networks and Internet services, and for his/her computer files, passwords and accounts. These procedures provide general guidance concerning the use of the District's computers and examples of prohibited uses. The procedures do not attempt to describe every possible prohibited activity by students. Students, parents and school staff who have questions about whether a particular activity is prohibited are encouraged to contact a building administrator or the Director of Technology.

A. Consequences for Violation of Computer Use Policy and Procedures

Student use of the **Milton Town School District** computers, networks and Internet services is a privilege, not a right. Compliance with the District's policies and procedures concerning computer use is mandatory. Students who violate these policies and procedures may have their computer 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.

B. Acceptable Use

The **Milton Town School District** computers, networks and Internet services are provided for educational purposes and research consistent with the school's educational mission, curriculum and instructional goals.

All Board policies, school procedures and expectations concerning student conduct and communications apply when students are using computers.

Students are also expected to comply with all specific instructions from teachers and other school staff or volunteers when using the school's computers.

C. Prohibited Uses

Examples of unacceptable uses of school unit computers that are expressly prohibited include, but are not limited to, the following:

1. **Accessing Inappropriate Materials -** Accessing, submitting, posting, publishing, forwarding, downloading, scanning or displaying defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing and/or illegal materials.

2. **Illegal Activities -** Using the school unit's computers, networks and Internet services for any illegal activity or in violation of any Board policy or school procedures. The District assumes no responsibility for illegal activities of students while using school computers.

3. **Violating Copyrights –** Copying, downloading or sharing any type of copyrighted materials (including music or video) without the owner's permission (see Board policy/procedure Copyright Compliance). The school unit assumes no responsibility for copyright violations by students.

4. **Copying/Installing Software –** Copying, installing or downloading software without the express authorization of the Director of Technology. Unauthorized copying of software is illegal and may subject the copier to substantial civil and criminal penalties. The school assumes no responsibility for illegal software copying by students.

5. **Plagiarism -** Representing as one's own work any materials obtained through any electronic means (such as term papers, articles, music, etc). When Internet sources are used in student work, the author, publisher and web site must be identified.

6. **Non-School-Related Uses -** Using the school's computers, networks and Internet services for non-school-related purposes such as private financial gain; commercial, advertising or solicitation purposes; or any other personal use not connected with the educational program or assignments.

7. **Misuse of Passwords/Unauthorized Access -** Sharing passwords, using other users' passwords, and accessing or using other users' accounts or allowing others to use your account.

8. **Malicious Use/Vandalism -** Any malicious use, disruption, physical tampering or harm to the school unit's computers, networks and Internet services, including but not limited to hacking activities and creation/uploading of computer viruses.

9. **Unauthorized Access to Chat Rooms -** Accessing chat rooms or news groups without specific authorization from the supervising teacher.

10. **Student Use of E-Mail -** Students may access their personal email accounts using the school district's electronic resources for limited personal use. Limited personal use of the district's electronic resources shall be permitted if the use:

    a) imposes no tangible cost to the District;
    b) does not unduly burden the District's electronic resources;
    c) occurs during non-instructional time and does not impede other students' access to electronic resources for academic use;

d) has no adverse effect on students' academic performance; and
e) is in strict compliance with the Acceptable Use Policy and Acceptable Use Procedures of the Milton Town School District.

11. Bypassing Filtering – all use of software, web sites or other means to bypass the district filtering system is strictly prohibited.

D. No Expectation of Privacy

The Milton Town School District's computers remain under the control, custody and supervision of the District at all times. Students have no expectation of privacy in their use of school computers, including e-mail, stored files and Internet access logs.

E. Compensation for Losses, Costs and/or Damages

The student and his/her parents are responsible for compensating the District for any losses, costs or damages incurred by the District for violations of Board policies and school procedures while the student is using school's computers, including the cost of investigating such violations. The District assumes no responsibility for any unauthorized charges or costs incurred by a student while using school's computers.

F. Student Security

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

G. System Security

The security of the District's computers, networks and Internet services is a high priority. Any student who identifies a security problem must notify his/her teacher immediately. The student 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 computer privileges limited, suspended or revoked.

H. Games

Students are not allowed to play games on the district's computers unless they are tied directly to an educational goal, aligned with curriculum that students are currently studying, and have been approved by the teacher who is implementing the curriculum.

I. Use of District Network

Student personal space on the district network (H Drive) is intended to house basic files (word processing, databases, spreadsheets, etc.) used in their classes/courses. Students shall not store music, video, executables or other large files in this space. Students, working through their teachers, may store appropriate music and video files in the designated space – I Drive for Middle and High School and J Drive for Elementary school.