

District staff shall adhere to the laws, policies and rules governing computers including, but not limited to copyright laws, rights of software publishers, license agreements, rights of privacy as stated in federal and state law. The systems are the property of the Monticello central school district and will be monitored. The following specific activity shall be prohibited by staff users of the District Computer System (DCS):

- 1- Using the DCS to obtain, view, download, send, print, display or otherwise gain access to or to transmit materials that are unlawful, pornographic, or abusive.
- 2- Use of obscene or vulgar language.
- 3- Harassing, insulting or attacking others.
- 4- Remote access to machines (i.e. to home).
- 5- Damaging, disabling, or otherwise interfering with the operation of computer, computer systems, software or related equipment through physical action or by electronic means.
- 6- Loading and/or using unauthorized software on the DCS including but not limited to any e-mail software, CUC me, downloading of automated data content delivery programs or real-life reference services (i.e. waterbug, stock ticker, ESPN, Web shots, screensavers), downloading chats (AOL, instant messenger), music unless otherwise approved by the technology director.
- 7- Use of storage devices (i.e. floppy disks, USB, CDs) without scanning for viruses before opening any file. If you're not familiar with scanning do not use devices or ask technology department for assistance.
- 8- Use of laptops on network without inspection and authorization.
- 9- Adding additional screensavers that do not come with your system.
- 10- Changing, copying, renaming, deleting, reading or otherwise accessing files or software not created by the staff member or students under his/her supervision without permission from the district technology director.
- 11- Violating copyright laws.
- 12- Employing the DCS for personal use; the DCS is to be used for school related activities only. E-mail is to be used only for district business and that the designated recipient of e-mail shall only be those whose receipt of the e-mail is necessary because of their direct involvement in or with the content of the e-mail communication. The district's system is not to be used as a form for articulating workplace grievances or complaints, which grievances or complaints are to be processed employing means authorized under applicable collective bargaining agreements, district policy and law.
- 13- Employing the DCS for commercial purposes, product advertisement, or political lobbying.
- 14- Disclosing an individual password to others, sharing passwords, or using others' passwords except in the supervision of students.
- 15- All staff members need to log out of programs when leaving their workstations based on accessibility of workstation to other users (i.e. AS/400, e-mail). We are monitoring the system and inappropriate activity will be traced to your password.
- 16- Transmitting material, information, or software in violation of any district policy or regulation or state or federal code.
- 17- Revealing personal information about a student or another faculty member.
- 18- Joining organizations, subscribing to mail lists, submitting entries to contests or participating in chat rooms without the express consent of the district.

As in any other area of instruction it is expected that teachers will maintain proper supervision of students making use of instructional technology. Violations by students of district policy should be reported to the Building principal. Teachers are responsible to be acquainted with district policy and regulations related to student and of their own use of instructional technology.

**Policy 6000 1 of 2    Staff Use of Computerized Information Resources**

The Board of Education will provide staff with access to various computerized information resources to the district's system (DCS hereafter) consisting of software, hardware, computer networks and electronic communication systems. This may include access to electronic mail, so-called "online services" and the Internet. It may also include the opportunity for some staff to have independent access to the DCS from their home or other remote locations. All use of the DCS, including independent use of school premises, shall be subject to this policy and accompanying regulations.

The Board encourages staff to make use of the DCS to explore educational topics, conduct research and contact others in the educational world. The board anticipates that staff access to various computerized information resources will both expedite and enhance the performance of tasks associated with their positions and assignments. Toward that end, the Board directs the Superintendent or his/her designee provide staff with training in the proper and effective use of the DCS.

Staff use of the DCS is conditioned upon agreement by the staff member that use of the DCS will conform to the requirements of this policy (available upon request) and any regulations adopted to ensure acceptable use of the DCS. All such agreement shall be kept on file in the District Office.

Generally, the same standards of acceptable staff conduct which apply to any aspect of job performance shall apply to the use of the DCS. Employees are expected to communicate in a professional manner consistent with applicable District policies and regulations governing the behavior of school staff. Electronic mail and telecommunications are not to be utilized to share confidential information about students or other employees.

This policy does not attempt to articulate all required and/or acceptable uses of the DCS; nor is it the intention of this policy to define all inappropriate usage. Administrative regulations will further define general guidelines of appropriate staff conduct and use as well as prescribed behavior.

Districts that shall also adhere to the laws, policies and rules governing computers including, but not limited to, copyright laws, rights of software publishers, license agreements, and rights of privacy created by federal and state law.

Staff members who engage in unacceptable use may lose access to the DCS and may be subject to further discipline under the law and in accordance with acceptable collective bargaining agreements. Legal action may be initiated against the staff member who willfully, maliciously or unlawfully damages or destroys property of the district.

### **Privacy Rights**

Staff the data files and electronic storage areas shall remain District property, subject to District control and inspection. The Director of Technology may access all such files and communications to ensure system integrity and that users are complying with the requirements of this policy and accompanying regulations. Staff should not expect that information stored on the DCS will be private.

### **Implementation**

The Board of Education directs the Superintendent or his/her designee to develop administrative regulations to implement the terms of this policy, addressing general parameters for acceptable staff conduct as well as prohibited activities so as to provide appropriate guidelines for the employee use of the DCS.

## **Policy 7000 Student Use of Computerized Information Resources**

The Board of Education will provide access to various computerized information resources through the District's computer system (DCS hereafter) consisting of software, hardware, computer networks and electronic communications systems. This may include access to electronic mail, so-called online services and the Internet. It may include the opportunity for some students to have independent access to the DCS from their home or other remote locations. All use of the DCS, including independent use of school premises, shall be subject to this policy and accompanying regulations. Further, all such use must be in support of education and/or research and consistent with the goals and purposes of the School District.

One purpose of this policy is to provide notice to students and parents/legal guardians that, unlike most traditional instructional or library media materials, the DCS will allow student access to external computer networks not controlled by the School District where it is impossible for the District to screen or review all of the available materials. Some of the available materials may be deemed unsuitable by parents/legal guardians for student use or access. This policy is intended to establish general guidelines for acceptable student use. However, despite the existence of such District policy and accompanying guidelines and regulations, it will not be possible to completely prevent access to computerized information that is inappropriate for students. Parents/legal guardians of students must be willing to set and convey standards for appropriate and acceptable use to their children when using the DCS or any other electronic media or communications. The District respects the right of each family to decide whether or not to apply for independent computer access.

Student use of the DCS is conditional upon written agreement by students and their parents/legal guardians that student use of the DCS will conform to the requirements of this policy and any regulations adopted to insure acceptable use of the DCS. All such agreements shall be kept on file in the building in which the student is enrolled.

Generally, the same standards of acceptable student conduct which apply to any school activity shall apply to the use of the DCS. This policy does not attempt to articulate all required and/or acceptable uses of the DCS; nor is it the intention of this policy to find all inappropriate usage. Administrative regulations will further define general guidelines of appropriate student conduct and use as well as prescribed behavior.

District students shall also adhere to the laws, policies and rules governing computers including, but not limited to, copyright laws, rights of software publishers, license agreements, and student rights of privacy as stated in federal and state law.

Students who engage in unacceptable use may lose access to the DCS and may be subject to further discipline under the District's school conduct and discipline policy and the Student Discipline Code of Conduct. The District reserves the right to pursue legal action against the student who willfully, maliciously or unlawfully damages or destroys property of the District. Further, the District may bring suit in civil court against the parent/legal guardians of any student who willfully, maliciously or unlawfully damages or destroys District property pursuant to General Obligation Law section 3 -- 112.

Student data files and other electronic storage areas will be treated like school lockers. This means in such areas shall be considered to be School District property subject to control and inspection. The Computer Coordinator in each building or the District Director of Technology may access all such files and communications to ensure system integrity and that users are complying with the requirements of this policy and accompanying regulations. Students should not expect that information stored on the DCS will be private.

The Superintendent or his/her designee is authorized to establish regulations as necessary to implement the terms of this policy.

<b>Regulation 7000R 1 of 2 Student Use of Computerized Information Resources</b>
--

### Program Implementation

The school district recognizes that effective use of technology is important to our students and will be essential to them as adults. Consequently, the School System will provide access to various computerized information resources through the District's Computer System (DCS) consisting of software, hardware, networks, electronic communication systems. This may include electronic mail, so-called online services and the Internet. The district shall provide personnel support for such usage.

The DCS is for educational and/or research use only and must be consistent with the goals and purposes of the School District. The standards of acceptable use as well as prohibited conduct by students accessing the DCS, as outlined in District Policy and Regulation, are not intended to be all-inclusive. Students are responsible for good behavior on school computer networks just as they are in a classroom or a school hallway. In addition to the specific standards of student conduct delineated in this regulation, the general requirements of acceptable student behavior expected under the District's school conduct and discipline policy and the Student Discipline Code of Conduct also apply to student access to the DCS. General school rules for behavior and communication apply.

### Authorization

Students will not be permitted to use the DCS without specific authorization from the appropriate administrator and/or instructor. Furthermore, only those students who have signed an agreement form and provided written permission from parents/legal guardians may access the DCS, including potential student access to external computer networks not controlled by the School District. Permission is not transferable and may not be shared. All required forms must be kept on file in the school in which the student is enrolled.

### Standards of Conduct Governing Student Access to the DCS

Inappropriate use of the DCS may result in disciplinary action, including suspension or revocation of student access to the DCS. Each student who is granted access will be responsible for that usage. The DCS is provided for students in support of their education program and to conduct research and communicate with others. Student access to external computer networks not controlled by the District is provided to students who act in a considerate and responsible manner. Individual users of the District's computerized information resources are responsible for the behavior and communications over the District computer network and stand-alone machines. It is presumed that users will comply with District standards and will honor the agreements they have signed.

No student may upload or download any file, program, graphic, e-mail, or a message without prior approval of the supervising teacher or computer coordinator in each building. No student may use a personal disk without first obtaining permission from the supervising teacher or computer coordinator and submitting that disk to a virus check.

<b>Regulation 7000R 2 of 2 Student Use of Computerized Information Resources (continued)</b>
--

Student data files and other electronic storage areas will be treated like school lockers. This means that such areas shall be considered to be School District property and subject to control and inspection. The Computer Coordinator or Director of Technology may access all such files and communications to insure system integrity and that users are complying with the requirements of District policy and regulations regarding student access to the DCS. Students should **not** expect that information stored on the DCS will be private.

During school, teachers will guide students toward appropriate materials. Outside of school, parents/legal guardians bear responsibility for such guidance as they do for information sources such as television, telephones, movies, radio and other potentially offensive/controversial media.

Use of the DCS which violates any aspect of School District policy; the Student Discipline Code of Conduct; and federal, state or local laws or regulations is strictly prohibited and may result in disciplinary action in compliance with applicable District guidelines and/or federal, state, and local law including, but not limited to, suspension and/or revocation of access to the DCS. In addition to the District's general requirements governing student behavior, the following specific activities shall be prohibited by student users of the DCS:

1. Using the DCS to obtain, view, download, upload, print, display or otherwise gain access to or to transmit materials that are unlawful, obscene, pornographic or abusive.
2. Use of obscene or vulgar language.
3. Harassing, insulting or attacking others.
4. Damaging, disabling or otherwise interfering with the operation of computers, computer systems, software or related equipment through physical action or by electronic means.
5. Using unauthorized software on the DCS.
6. Changing, copying, renaming, deleting, reading or otherwise accessing files or software not created by the student without express permission from the Computer Coordinator, supervising teacher or District Director of Technology.
7. Violating copyright law.
8. Employing the DCS for commercial purposes, product advertisement or political lobbying.
9. Disclosing an individual password to others or using others' passwords.
10. Transmitting material, information or software in violation of any District policy or regulation, the school behavior code, and/or federal, state and local law or regulation.
11. Revealing personal information about oneself or of other students, faculty or staff members, including, but not limited to, disclosure of home address and/or telephone number.
12. Joining organizations, subscribing to mail lists, submitting entries to contests or participating in chat rooms without the expressed consent or permission of the supervising teacher or District Director of Technology.

### Sanctions

1. Violations may result in suspension and/or revocation of student access to the DCS.
2. Additional disciplinary action may be determined at the building level in accordance with existing practices and procedures regarding inappropriate behavior as well as federal, state and local law.

## **Security**

Users of the DCS identifying a security problem on the District's system must notify the teacher in charge. A student is not to demonstrate the problem to other users. Attempts to log onto the DCS as a user other than oneself unless specifically requested to do so by the student's teacher or District Director of Technology will result in cancellation of user access. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the DCS. Further, any violations regarding the use and application of the DCS shall be reported by the student to the teacher in charge.