

COMPUTER NETWORK FOR EDUCATION REGULATIONS

I. Administration

A. SUPERINTENDENT OF SCHOOLS. The Superintendent of Schools of the Berlin Central School District shall oversee the District's computer network. At her/his discretion, the Superintendent may delegate some or all such responsibilities to District personnel.

B. COMPUTER OVERSIGHT RESPONSIBILITIES. The Superintendent or her/his designee shall have the following computer network oversight responsibilities:

1. Monitor and examine all network activities, as she/he deems appropriate, in order to ensure proper use of the system;
2. Disseminate and interpret at the building level District policy and regulations governing use of the District's network to all staff who are actual or potential users of the system;
3. Provide or see to the provision of employee training in the proper use of the network;
4. Provide or see to the provision of employee training for those supervising students, so that students who use or will use the network then receive training in the proper use of the network; and
5. Ensure that all disks and software loaded into the computer network have been previously scanned for computer viruses.

II. Persons with Access to the System

The following individuals may be designated as members with access to the computer network system:

- A. Elementary, middle, and high school students who have been granted an account;
- B. Teachers, who may apply for a class account;
- C. Other District employees, as may be deemed necessary by the Superintendent of Schools or her/his designee; and
- D. Community members, as deemed necessary by the Superintendent of Schools or her/his designee.

III. Procedures for Proper Use of the District's Computer Network System

- A. APPROPRIATE USE OF SYSTEM. The District's computer network shall be used only for educational purposes that are consistent with the policies, mission and goals of the District.
- B. ACCOUNT RESPONSIBILITY. The person in whose name an account is issued, whether that person is a staff member, a student, or some other person, shall be responsible at all times for the proper use of that account.
- C. USERNAME AND PASSWORD. Each network user shall be issued a "login" (user) name and a password. Each user's password is to be changed every 30 days.
- D. OFF-SITE USE. In order to access the District's system from off- site (e.g., from the user's home), prior written permission from the building principal or the Superintendent or her/his designee shall be necessary.
- E. PROCEDURE FOR HANDLING COMPUTER SECURITY PROBLEMS. Any network user who identifies a security problem on the District's system shall immediately notify the Superintendent or her/his designee, or a building administrator, sponsoring teacher, or other teacher. The network user who discovers the problem shall not demonstrate that problem to any person except those just named, or an individual whom someone just named has designated.
- F. STUDENT ACCOUNT INFORMATION IS STUDENT RECORD. Student account information shall be deemed a student record. It shall therefore be maintained in accordance with statutory rules governing access and retention of student records, and with applicable District policy and regulations.
- G. COPYRIGHTED MATERIAL.
1. Copyrighted Material. Copyrighted material may not be placed on any computer connected to the District's network without appropriate legal authorization to do so. Only staff who are specifically authorized by the Superintendent or the Superintendent or her/his designee may load copyrighted material into the network.
 2. "Fair Use" Restrictions in Effect. Network users may download copyrighted material for their own use. Copyrighted material shall be used in accordance with the "fair use" doctrine of U.S. copyright law, and with District policy and regulations.

H. DENIAL OF ACCESS. Any network user whom the District identifies as a security risk, or who is discovered to have violated the District's computer use rules and guidelines in the past, may be denied access to the District's network. Such determination to deny access shall be made by the Superintendent, by the principal of the building that the user attends or works in, or by the staff member's supervisor.

IV. Prohibitions

What follows is a list of prohibited activities when using the District's computer network. Violation of any of these prohibitions may result in discipline or another appropriate penalty, including suspension or revocation of a user's access to the network and restitution for damages.

A. PASSWORD SHARING. There shall be no sharing of passwords without prior written permission from the supervising or sponsoring teacher, the building administrator, or the Superintendent or her/his designee, as appropriate.

B. INTERFERENCE WITH E-MAIL. It is prohibited to read, delete, modify, or copy the electronic mail of another system user, or to attempt to any of these things. Such activities shall be deemed deliberate interference with the ability of another system user to send or receive electronic mail. In addition, forgery or attempted forgery of electronic mail messages is prohibited.

C. USE OF PERSONAL SOFTWARE. Use of personal software or any software that is not licensed to the District is strictly prohibited.

D. USE OF ANOTHER'S NAME TO LOG ON. No student shall attempt to log on to the District's system in the name of another individual, with or without that individual's password.

E. PROMOTION OF ILLICIT ACTIVITIES OR USE FOR OTHER IMPROPER PURPOSES. System users shall not use the system to promote or encourage the use of tobacco, alcohol, or any illegal or controlled substance; to transmit or receive pornographic or indecent materials; to promote any other activity prohibited by District policy, or by state or federal law; or for any other purpose or activity unrelated to the instructional, administrative, support, or extra- or co-curricular activities of the District.

F. ACCESS TO SECURE AREAS OF THE SYSTEM. Use of computer access to data and access to secure areas of the system other than for educational purposes is prohibited.

- G. EXCEEDING DISK QUOTA. System users shall not evade, change, or exceed resource quotas as set by the administration. A user who continues to violate disk space quotas after seven calendar days of notification that she/he has done so may have her/his file removed from the system by the Superintendent or her/his designee. Such quotas may be exceeded only with prior approval, upon the user's request, of the Superintendent or her/his designee that disk quotas be increased. Such request shall state the reason for the need to increase the disk quota.
- H. TRANSMISSIONS IN VIOLATION OF POLICY OR LAW. It is prohibited to transmit material, information, or software in violation of any District policy, or any state or federal law.
- I. VANDALISM. Vandalism is prohibited, and shall result in cancellation of the vandal's system use privileges. By "vandalism" is meant a malicious attempt to harm or destroy District equipment, or materials or data of another user of the District's system or any of the agencies or the other networks connected to the Internet. Vandalism shall include, but is not limited to, the loading or creating of computer viruses.
- J. TAMPERING, MISUSE, OR OTHER POLICY VIOLATION. Tampering with or misuse of the computer system, or taking any other action inconsistent with this policy or regulation, shall be viewed as a security violation, and is prohibited.