

## ACCEPTABLE USE OF TECHNOLOGY, ELECTRONIC NETWORKS AND RELATED EQUIPMENT

### Purpose of Technology Use

Bloom Township School District 206 (“District”) provides access for students, staff and community to resources from around the world through an electronic communication system which includes internet and email access. These technologies are provided solely for the purpose of enhancing learning and communication in the District. Therefore, access to the District’s electronic network(s) must be for educational purposes only.

### The Opportunities and Risks of Technology Use

The Bloom Township School District 206 Board of Education (“Board”) believes that the value of information and interaction that technology offers outweighs the possible hazards of its use. Making network access available, however, carries with it the potential that some network users will encounter sources that may be controversial or inappropriate. Because information on networks is transitory and so diverse, the District cannot completely predict or control what users may or may not locate.

In accordance with the Children’s Internet Protection Act, the Keeping the Internet Devoid of Sexual Predators Act, and the Social Networking Prohibition Act the District installs and operates filtering software to limit users’ internet access to materials that are obscene, pornographic, harmful to children, or otherwise inappropriate, notwithstanding that such software may at certain times block access to other materials as well. At the same time the District cannot guarantee that filtering software will in all instances successfully block access to materials that are obscene, pornographic, harmful to children, or otherwise inappropriate. The use of filtering software does not negate or otherwise affect the obligations of users to abide by the terms of this policy and to refrain from accessing such inappropriate materials.

No technology is guaranteed to be error-free or totally dependable. Among other matters, the District is not liable or responsible for:

1. Any information that may be lost, damaged, or unavailable due to technical or other difficulties,
2. The accuracy or suitability of any information that is retrieved and/or produced through technology,
3. Breaches of confidentiality, or
4. Defamatory material.

In addition, the District will not be responsible for any unauthorized charges or fees resulting from access to the Internet/Telnet.

### Privileges and Responsibilities

The District’s Network is a part of a curriculum and is not a public forum for general use. Users may access technology only for educational purposes. Access to the District’s

Network and use of the District's technology related equipment is a privilege, not a right. The district will strive to provide equitable opportunities for the use of technology, and the administration will take reasonable measures to inform students and staff of the rules and regulations regarding network and equipment use in staff and student handbooks. This policy shall apply to all users (faculty, students, administrators, staff, Board of Education, community, etc.) of the District's technology.

Users of technology will:

- Use or access District technology only for educational or administrative purposes.
- Comply with copyright laws and software licensing agreements.
- Understand that email and network files are not private. Network administrators and other designated personnel have access to all email messages and may review files and communications to maintain integrity and monitor responsible use.
- Respect the privacy rights of others and maintain confidentiality of all personnel and student records stored or accessible by means of District technology.
- Be responsible at all times for the proper use of technology including the proper use of access privileges, complying with all system security identification codes, and not sharing any codes or passwords.
- Maintain the integrity of technological resources from potentially damaging messages, physical abuse, or viruses.
- Abide by the policies and procedures of networks and systems likened by technology.
- Respect the rights of others to use equipment.

Users of technology will not:

- Access, submit, post, publish, display or create any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially/religiously offensive, harassing, illegal or other material unsuitable in the educational setting or related to the District's educational program.
- Use the Network for, or in support of, any obscene or pornographic purposes including, but not limited to, the retrieving or viewing of any sexually explicit material. If a student inadvertently accesses such information he or she should immediately disclose the inadvertent access to a teacher or other school official. Other authorized users should report the incident to the Network Administrator. This will protect the user against accusations of violating this policy
- Solicit or distribute information with the intent to incite violence, cause personal harm or bodily injury, or to harass or "stalk" (cyberstalking) another individual.
- Interfere with, or disrupt Network use by others; create and/or propagate unsolicited advertising, political lobbying, chain letters, pyramid schemes, computer worms, viruses, or other acts of vandalism. Vandalism includes any attempt to harm or destroy data of another user, the Internet, the District's Network or any other network. This includes, but is not limited to, uploading, downloading, creation or knowing transmission of computer viruses. If a user is uncertain whether his or her conduct is permissible, he or she should contact the Network Administrator.

- Use another's account or password.
- Distribute user passwords, copyrighted or plagiarized material or material protected as a trade secret.
- Misrepresent themselves or others.
- Trespass in others' folders, work, or files, or gain unauthorized access to resources or entities.
- Use the District's networks to distribute or share files (including music and video files), images, applications, etc. with others unless the shared file is created by District technology staff.
- Post personal contact information or other private information about oneself, a student or staff member, or otherwise invade the privacy of individuals or violate the Illinois School Student Record Act or federal Right to Privacy Education Act.
- Use District technology for non-school purposes, personal financial gain (including gambling), or any other illegal purpose of activity.
- Forge or anonymously transmit email or other electronic materials.
- Attempt and/or breach security measures or remove hardware/software, networks, information, or communication devices from the District or other network.
- Represent personal views as those of the District or those that could be interpreted as such.
- Use the Network while access privileges are suspended or revoked.

### Security

In order to maintain the security of the District Network users are prohibited from:

- Using any unauthorized personal equipment to attach, connect to or install on the District Network.
- Intentionally disrupt the District Network by "hacking" of any kind, use of proxy or filter avoidance software or devices, and/or engaging in computer tampering of any kind.
- Downloading and/or installing and/or using unauthorized software, games, programs, files, electronic media, and/or stand-alone applications.

### Websites and Web pages

Authorized users may create web pages as part of a class activity. Material presented on a class website must meet the educational objectives of the class activity. The District has the right to exercise control over the content and/or style of the student web pages. All class web pages shall be posted through the school website.

Only those students whose parent(s) or guardian(s) have consented and signed a release may post their work or picture on student or school websites. Students whose work, likeness (as captured by photograph, video or other media) or voices are presented on a student website shall be identified by first name only and for confidentiality and safety purposes.

### Electronic Social Networking

While home-based web sites, message boards, blogs, forums, and other uses of home-based computers may be regarded as a benefit to a student's computer literacy, the student needs to be aware of the following:

Using a non-district computer such that it results in material and/or disruption of the educational process of the school will constitute grounds to investigate whether the use violates District policies and rules.

### Disciplinary Action

Violations of the policy, or any administrative regulations and/or guidelines governing the use of technology, may result in disciplinary action which could include the loss of network access, loss of technology use, suspension or expulsion (in the case of students), suspension with or without pay or termination (in the case of staff), or other appropriate disciplinary action. Violations of local, state, or federal law may subject staff and students to prosecution by appropriate law enforcement authorities.

Any expenses incurred by virtue of violation of this policy, including telephone long distance, per-minute or line charges, are the sole responsibility of the user.

### No Expectation of Privacy

The District retains control, custody and supervision of all computers and the Network. The District reserves the right to monitor all computer and network activity by students and staff. Users have no expectation of privacy concerning information transmitted or received via the Network or contained or stored on the District's computers. In addition, users must recognize that there is no assurance of confidentiality with respect to access to transmissions and files by persons outside, or from persons inside the District.

### Staff responsibilities to Students

Staff members utilizing the Network for instructional purposes with students are responsible for supervising such use. In selecting technology for teaching purposes, staff shall comply with the selection criteria for instructional materials and library-media center materials. Staff members are expected to be familiar with the District's policies and any administrative rules concerning student computer and Network use and then enforce them. When in the course of their duties staff members become aware of student violations, they are expected to stop the activity and/or inform the building Network Administrator or the building administration.

### Additional Rules/Actions

The Superintendent may establish procedures and guidelines and shall take appropriate action to implement this policy.

Approved: July 9, 2007