

East Baton Rouge Parish School System
Internet Safety and Network Use Policy
(Revised: June 2005)

The East Baton Rouge Parish School Board recognizes the role of educational technologies in stimulating innovative approaches to teaching and learning and shifting the way educators and students access and transmit information, share ideas, and contact others. In addition, technology is a key component in transacting the business of the system and board. The connection of schools and offices to the global online community brings new responsibilities as well as opportunities.

Network resources are provided for educational purposes and to carry out the legitimate business of the *East Baton Rouge Parish School System (EBRPSS)*. Appropriate uses include instruction, research, online collaborations, and the official work of the offices, departments, and schools. The Board expects all employees, students, and board members who use computing and network resources, including electronic mail and telecommunications tools, to apply them in appropriate ways to the performance of responsibilities associated with their positions and assignments. The Board directs the Superintendent or authorized designee(s) to specify those behaviors that are permitted and those that are not permitted as well as disseminate appropriate guidelines for the use of technology resources.

In compliance with the *Children's Internet Protection Act*, the EBRPSS shall use a technology protection measure that blocks and/or filters Internet access to prevent access to Internet sites that fall under any of the definitions contained in Section I: Definitions. The technology protection measure that blocks and/or filters Internet access may be disabled by an authorized individual for bona fide research purposes with the permission of the Superintendent or authorized designee(s). This disabling is permissible only for a student 17 years of age or older or an authorized employee for the purpose as stated.

The network and Internet user shall be held responsible for his/her actions and activities. Responsibilities include efficient, ethical and legal utilization of network resources.

As a matter of public law, any document pertaining to the public business on a publicly funded system is a public record, and this law applies to records stored on district computers.

Specific guidelines for students and employees are outlined in Section II: Student Policies and Guidelines; Section III: Employee Policies and Guidelines; and Section IV: General District Technology Policies.

I. DEFINITIONS

- A. CHILD PORNOGRAPHY** - The term "child pornography" has the meaning given such term in section 2256 of title 18, United States Code.

- B. HARMFUL TO MINORS** - The term “harmful to minors” means any picture, image, graphic image, file, or other visual depictions that
1. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
 2. depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
 3. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.
- C. MINOR** - The term “minor” means an individual who has not attained the age of 17.
- D. OBSCENE** - The term “obscene” has the meaning given such term in section 1460 of title 18, United States Code.
- E. SEXUAL ACT; SEXUAL CONTACT** - The Terms “sexual act” and “sexual contact” have the meanings given such terms in section 2246 of title 18, United States Code.

II. STUDENT POLICIES AND GUIDELINES

Use of network resources and the Internet is for educational purposes. Adherence to policies and guidelines is required for continued access to technological resources.

A. EMAIL AND TELECOMMUNICATIONS

In general, any student use of networks and telecommunication resources must be for educational purposes. School system rules for student communication also apply in the online environment. Students must respect and adhere to policies in the *Student Rights and Responsibilities Handbook* as well as any other applicable policy, and local, state, and Federal law.

Students must

1. login and use network resources only with their student account.
2. logoff and close applications immediately after completing work to prevent unauthorized use of the user ID.
3. not use email, chat rooms, net meeting rooms, and other forms of direct electronic communication including instant messaging systems unless authorized by the district and directly supervised by a teacher. School system rules prohibiting indecent, vulgar, lewd, slanderous, abusive, threatening, sexually harassing, or terrorizing language apply to all forms of electronic communications. The student and parent or guardian shall sign an *Acceptable Use of Networks and Telecommunications Agreement* prior to an email account being issued.
4. not distribute private information about themselves or others.

5. not send spam, chain letters, or other mass unsolicited mailings.
6. not view, use, or copy passwords to which they are not authorized.

B. NETWORKS AND INTERNET USE

Students shall

1. use Internet search engines and/or other Internet tools only under the direction and supervision of teachers.
2. observe copyright laws, citing the source of information accessed over the Internet using a standard system as directed by the teacher and/or librarian.
3. not intentionally access, transmit, copy, or create material that is illegal, such as obscenity, stolen materials, or illegal copies of copyrighted works, including, but not limited to, music, games, and movies.
4. not intentionally access, transmit, copy, or create any materials or visual depictions on school or district networks or the Internet that are indecent, vulgar, lewd, slanderous, abusive, threatening, harassing, terrorizing, or harmful to minors.
5. not attempt to gain unauthorized access, including so-called “hacking” or otherwise compromise any computer or network security or engage in any illegal activities on the Internet, including willfully introducing a computer virus, worm, or other harmful program to the network.
6. not download and install any file sharing program that bypasses the district filtering device.
7. not use technology resources to further other acts that are criminal or violate the school or district code of conduct.
8. not make any purchase on the Internet while using school equipment or Internet service.

Students who may inadvertently access a site that is pornographic, obscene, or harmful to minors shall immediately disconnect from the site and inform the teacher. The Board does not condone any illegal or inappropriate activities and will not be responsible for such use by students. The Board does not guarantee the right to use the Internet and reserves the right to suspend or terminate the privilege of any individual at its sole discretion without notice, cause, or reason.

Any violation of this policy may result in the loss of access to the Internet through the EBRPSS network. Additional disciplinary action for students will be determined in accordance with existing rules and procedures, both administrative and as stipulated in East Baton Rouge Parish policy, and including applicable law enforcement agencies when necessary.

III. EMPLOYEE POLICIES AND GUIDELINES

Use of network resources and the Internet is for educational and research purposes or to conduct legitimate business of the School Board. All employees desiring to use school district computers, including the Internet and email systems, must sign the *East Baton Rouge Parish Employee Internet Safety and Network Use Agreement* and

agree to abide by all district regulations. The Board does not condone any illegal or inappropriate activities and will not be responsible for such use by staff. The Board does not guarantee the right to use the Internet and reserves the right to suspend or terminate the privilege of any individual at its sole discretion without notice, cause, or reason. Failure to adhere to these regulations may result in the loss of computer privileges, access to the Internet and electronic mail account and may result in further disciplinary action up to and including termination. Furthermore, any activity that may be in violation of local, state, or federal laws will be reported to the appropriate law enforcement agency.

A. E-MAIL AND TELECOMMUNICATIONS

Employees must use assigned email accounts in support of educational purposes and conducting district business. All employees desiring to use telecommunications tools signify by their acceptance of an email account and their signature on the *East Baton Rouge Parish Employee Internet Safety and Network Use Agreement* their willingness to adhere to School Board policy. This policy also applies to the use of private e-mail accounts when access is attained using School Board equipment or networks and to access attained through any authorized personal digital device while on School Board property.

Communication over networks is not private. Network supervision and maintenance may require review and inspection of directories or messages. Messages may sometimes be diverted accidentally to a destination other than the one intended. The school system reserves the right to access stored records in cases where there is reasonable cause to suspect wrongdoing or misuse of the system. Courts have ruled that old messages may be subpoenaed, and network supervisors may examine communications in order to ascertain compliance with network guidelines and acceptable use policies.

In general, employees are expected to communicate in a professional manner consistent with state laws and local policies governing the behavior of school employees and with federal laws governing copyright. Electronic mail and telecommunications are not to be utilized for unauthorized disclosure, use and dissemination of personal identification or confidential information regarding any student or employee.

Employees must

1. not communicate any indecent, vulgar, lewd, slanderous, abusive, threatening, sexually harassing, or terrorizing e-mail or other messages or materials on school or district networks or the Internet.
2. not send spam, chain letters, or other mass unsolicited mailings.
3. not view, use, or copy passwords to which they are not authorized.
4. not use technology resources to further other acts that are criminal or violate the school or district code of conduct or rules.
5. not disclose, use, or disseminate personal information regarding minors

6. not use the email system for commercial, political, personal activities, or religious purposes.

B. NETWORKS AND INTERNET

All employees are responsible for knowing and adhering to school system policies regarding networks and the Internet. Employee policies and regulations apply to all EBRPSS employees, including classified and unclassified staff and board members.

Employees shall

1. login and use their network account only for their own use.
2. logoff and close applications when leaving the computer unattended to prevent unauthorized access to sensitive, protected, or prohibited information.
3. not intentionally access, transmit, copy, or create material that is illegal, such as obscenity, stolen materials, or illegal copies of copyrighted works, including, but not limited to, music, games, and movies.
4. not intentionally access, transmit, copy, or create any materials or visual depictions on school or district networks or the Internet that are indecent, vulgar, lewd, slanderous, abusive, threatening, harassing, terrorizing, or harmful to minors.
5. not attempt to gain unauthorized access, including so-called "hacking" or engage in any other unlawful conduct online, including willfully introducing a computer virus, worm, or other harmful program to the network.
6. not download non-work related files or access or download files from sites delivering streaming audio or video except for educational use in direct instruction of students, for professional development, or to conduct district business. Any use of streaming audio or video in schools must comply with district procedures.
7. not download and install any file sharing program that bypasses the district filtering device.
8. not use the website for personal financial gain, political advertising, or issue advocacy.
9. not use the web site for fundraising purposes without prior written administrative approval.
10. not link to personal home pages, use the district site for personal web pages, or use the district site for links to sites of personal interest.
11. not make any personal purchase on the Internet while using EBRPSS equipment or Internet service.

C. TEACHERS RESPONSIBILITY FOR STUDENT USE OF NETWORKS AND THE INTERNET

Teachers shall

1. not allow students to use their teacher network account.
2. require students to login to the network with their student account.
3. ensure that the use of Internet resources is consistent with curriculum objectives of the school system.

4. preview and evaluate learning resources including Internet sites prior to recommending them for student use.
5. direct and supervise student access to Internet resources identified through tools such as age-appropriate search engines, directories, resource lists, and news groups, and provide appropriate guidance and instruction to students in the use of those sites that have not been evaluated by the teacher.
6. limit electronic distribution of assignments, classroom materials, grades, parental advisories, and any other information to systems the district provides for that purpose, in accordance with the *EBRPSS Web Publishing Policy and Guide*.
7. submit a *Distance Learning* approval form to the appropriate site and district administrators prior to participating in online educational projects or courses requiring student email access.
8. secure a parent or guardian signature a district *Media Release* form and keep on file at the school, prior to publishing student pictures or work on the Internet, to protect student privacy.

IV. GENERAL DISTRICT TECHNOLOGY POLICIES

A. INSTALLATION AND MAINTENANCE OF HARDWARE AND SOFTWARE

Installation and maintenance of hardware and software in EBRPSS schools and offices shall be directed and performed by the appropriate district technology staff. The following guidelines shall be observed:

1. Computers and other network devices shall be installed and maintained only by authorized staff. The Board has an obligation to ensure that software on its computers is being used legally according to the software license and to ensure that any software installed does not create problems on that computer or the district network.
2. A multiple license must be in effect for any software installed on a file server.
3. All software installed on district computers must be related to the educational purposes of the EBRPSS School System.
4. “Migrating” to an upgraded computer does not carry with it the right to “migrate” software unless the software is removed from the original machine.
5. “Migrating” to upgraded servers or network operating systems does not carry with it the right to continue use of older software designed for older operating systems.
6. District technical staff has the right and obligation to remove unauthorized and harmful software from computers and will report the incident to the appropriate site and district administration.
7. Any computer that does not meet the requirements for the District network will no longer be maintained or repaired by the District.
8. Any computer accessing the Internet without network login and authentication must maintain current anti-virus software.
9. *School Technology Facilitators* at each school site are designated to enter work orders for hardware or software installation and maintenance and related issues into the district online system for reporting, maintaining and tracking documentation on repairs and service calls.

B. DISTANCE LEARNING

Use of videoconferencing in schools must be approved by the appropriate site and district administrators prior to implementation. Appropriate uses include online courses (distance education/virtual schools), online collaborations, and/or virtual field trips to enhance the comprehensive curriculum, and other approved educational activities, including professional development. Principals or an authorized designee must submit a *Distance Learning Request Form* for any course or activity requiring student email access. The student and parent or guardian shall sign an *Acceptable Use of Networks and Telecommunications Agreement* prior to an email account being issued.

C. GRANTS

Any employee applying for a grant with a technology component must follow *EBR Grant Procedures* and utilize the appropriate *Grant Technology Planning Form*.

D. OUTSIDE AGENCIES AND ORGANIZATIONS

Any project in an EBRPSS school or facility that is initiated and funded by non-EBRPSS agencies or organizations must be planned in conjunction with the *Department of Technology Services* to insure that appropriate standards and procedures are followed.

Disclaimer: EBRPSS will not assume responsibility for maintaining, installing, operating, or repairing any technology installations initiated by outside agencies without prior written agreement approved by the Superintendent or authorized designee(s).

The Board recognizes that changes in technologies and local, state, and federal laws may from time to time require adjustments to policies and guidelines governing technology usage in the District and hereby authorizes the Superintendent or designee(s) to make such adjustments as necessary.

The Board expects all employees and students to cooperate in good faith with established policies and rules in order to preserve the integrity of network resources and Internet access for all users.

Adopted: July 17, 1997

Amended: July 23, 1998

Revised: February 21, 2002

Revised: June 16, 2005