East Baton Rouge Parish School System

Internet and Network Usage Policy

The East Baton Rouge Parish School Board recognizes the role of educational technologies in stimulating innovative approaches to teaching and learning and shifting the manner in which 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 school system and school 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 technology monitoring and protection measures that monitor, block and/or filter Internet access to prevent access to Internet sites that fall under any of the definitions contained in *Section I: Definitions*. The technology protection measures that block and/or filter Internet access may be disabled by an authorized individual for bona fide research purposes with the permission of the superintendent, chief technology officer, or authorized designee(s). This disabling is permissible only for students 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 any and all 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 all records, messages and other information stored on district computers, file servers, and email and other data storage systems.

Specific guidelines for students and employees are outlined *in Section II: Student Policies and Guidelines; Section III: Employee Policies and Guidelines; Section IV: Acceptable Use of*

Information Technology Resources for District Enterprise Business applications, and *Section V: 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 and Sexual Conduct* -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

Student 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. Online Safety Instruction

All students will be educated about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyber-bullying awareness and response.

B. 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 shall:

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, bullying, cyber-bullying, or any form of terrorizing language which shall apply to all forms of electronic communications. The student and parent or guardian shall sign an EBR Internet and Network Usage Policy agreement prior to an email or network 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.

C. Network 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. All forms of cyber-bullying are strictly prohibited.
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 use, download and/or install any file sharing program or anonymous proxy programs or websites that bypass the district filtering systems.
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 EBR Internet and Network Usage Policy 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. Email 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 EBR Internet and Network Usage Policy 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 EBR 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 shall:

1. not communicate any indecent, vulgar, lewd, slanderous, abusive, threatening, sexually harassing, cyber-bullying, 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. Network and Internet Use

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. All forms of cyber bullying are strictly prohibited.
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 use, download and/or install any file sharing programs or anonymous proxy programs or websites that bypass the district filtering systems.
8. not use the network, email system, or district web sites for personal financial gain, political advertising, or issue advocacy.
9. not use the network, email system, or district web sites for fundraising purposes without prior written administrative approval.
10. not link to personal home pages, use the district sites 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 (Instructional Technology Department).
8. secure a parent or guardian signature on 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 (Communications Department).

IV. Acceptable Use of Information Technology Resources for District Enterprise Business applications

The purpose of this policy is not to impose restrictions that are contrary to the EBRPSS's established culture of openness, trust and integrity; but to outline acceptable and ethical use of information technology resources. Enforcing this policy is an integral part of the district's

commitment to protecting its employees, affiliates and itself from illegal, unethical or damaging actions by individuals, either knowingly or unknowingly. It is important that every enterprise business-system computer user know the guidelines of this policy, and to conduct their work accordingly.

A. General Guidelines Regarding Enterprise Business Application Systems:

1. Prior to gaining access to EBRPSS information technology resources; all employees, temporary staff, interns, contractors and affiliates must acknowledge receipt and acceptance of the EBRPSS Internet and Network Use Policy.
2. All data created on the EBRPSS's computer system remains the property of the EBRPSS. Users are responsible for exercising good judgment when using EBRPSS information technology resources.
3. Users should be aware that EBRPSS network, network traffic and devices may be monitored and audited for security and network maintenance purposes at any time by authorized individuals without prior notice.
4. All confidential and sensitive data must be encrypted and transported exclusively upon EBRPSS-owned devices.
5. EBRPSS employees should protect the technical resources under their control, such as passwords, computers and data.
6. EBRPSS employees are prohibited from sending official EBRPSS messages from a personal, non-EBRPSS email address.
7. EBRPSS employees will not configure personal e-mail to be delivered to an EBRPSS computer.

B. The following actions are prohibited on EBRPSS data networks:

1. Engaging in any illegal activity under local, state, federal or international law or in violation of EBRPSS policies
2. Sharing network user-accounts and passwords with others even on temporary basis
3. Storing EBRPSS sensitive/confidential data on personal computers or devices
4. Gaining unauthorized access or modifications to any district, department, or school network or information technology resource for any reason
5. Installing unauthorized or unlicensed hardware or software on any EBRPSS information technology device
6. Attaching personally owned devices to the EBRPSS network without an approved exclusion
7. Violating copyright laws including downloading music and non-work related video files
8. Installing personally owned digital music or movies on a district-owned computer
9. Setting up file sharing in which protected intellectual property is illegally shared such as music or videos
10. Using EBRPSS information technology resources for personal financial gain

11. Using an EBRPSS computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace policies or laws
12. Performing any form of harassment or cyber-bullying
13. Creating or forwarding chain letters
14. Port scanning or security scanning is prohibited unless prior notification to the EBRPSS's chief technology officer is made and authorization is granted.
15. Leaving your computer unlocked and unattended
16. Using instant messaging, voice over internet protocol, or video over internet protocol programs unless authorized for business use

C. Password requirements for EBRPSS enterprise business application systems:

Passwords keep information safe and to prevent potential security breaches. Each employee is assigned a password as a method to provide unique access to information technology resources and information. Passwords shall never be shared with others; unless a legitimate business reason exists (e.g. sharing a password with the EBRPSS Help Desk to solve a computer related problem). If an employee suspects their password has been compromised, it should be changed immediately and reported to the EBRPSS technology help desk or to the chief technology officer.

A poorly chosen password may result in the compromise of the EBRPSS network. A strong password:

1. Has both upper and lower case letters. (Required)
2. Has digits or punctuation characters as well as letters. (Required)
3. Is at least eight alphanumeric characters long. (Required)
4. Is easy to remember and hard to guess.
5. Can be typed quickly.
6. Is changed at least once every forty-five days. (Required)

Do not use:

1. The same password for multiple computer or network systems.
2. Personal information (pets, names, phone numbers, etc.) as passwords.
3. Easy to guess or identify passwords such as 1234 or QWERTY.
4. Your password on a computer you suspect may have viruses or malware.

It is important to note that the practice of writing down your passwords is discouraged, but allowed if it is stored in a secure location.

D. Virus/Malware/Spyware Prevention and Protection

1. To protect EBRPSS information technology resources, data standards or requirements for all computers and devices connected to the EBRPSS networks must be in place to ensure effective virus and malware detection and prevention.

2. All EBRPSS computers must have the standard supported EBRPSS antivirus program installed and scheduled to run at regular intervals.
3. The antivirus program and antivirus patterns (definitions) must be kept up-to date.
4. All EBRPSS computers must have antispyware program installed.
5. If you believe your computer is infected with a virus or performing abnormally, turn off your machine and contact the EBRPSS technology help desk immediately.
6. The use of non-standard programs or shareware is allowed only after approval of the EBRPSS chief technology officer.

E. Sensitive/Confidential Data Handling

The purpose of this policy is to establish awareness and provide guidance on the proper handling of confidential and sensitive information, including but not limited to Social Security Numbers (SSN), credit card numbers and Federal ID numbers maintained by the EBRPSS. Forms of communication include but are not limited to oral or written words, screen displays, electronic transmission (such as email and attachments), printed material, USB storage device, etc; whether it is a partial or full display of the number.

1. Do not use SSNs as the primary identifier for any person or entity in any system, unless it is a mandated necessity.
2. Confidential or sensitive data may not be copied without authorization from EBRPSS administrators.
3. Confidential information shall be encrypted before communicated via e-mail or transferring via portable storage devices.
4. Recipients of confidential or sensitive data shall not disclose the contents to any individual unless that person has a valid need and proper authorization from EBRPSS Management.
5. The principle of least privilege must be followed in giving access to data.
6. Access privileges must be reevaluated regularly; access rights should be revoked or changed accordingly to reflect an individual's role, responsibilities and employment status.
7. Any release, exposure or potential exposure of confidential information to an unauthorized third party or unauthorized access to EBRPSS's system must be reported immediately to district management.

V. 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 network file server.
3. All software installed on district computers must be related to the educational or business 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 and/or properly licensed.
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 video conferencing in schools must be approved by the appropriate site and district administrators prior to implementation and use. 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 EBR Internet and Network Usage Policy prior to an email account and/or access credentials 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 (Office of Coordinator of Grants).

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: Neither EBRPSS nor the Department of Technology Services will assume responsibility for maintaining, installing, operating, or repairing any technology installations initiated by outside agencies without prior written agreement approved by the superintendent, chief technology officer, and/or other authorized designee(s).

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.

*** Updated and Board-approved: June 2012

---------- NOTICE OF RECEIPT AND REVIEW----------

I have received and reviewed the Internet and Network Usage Policy of the East Baton Rouge Parish School System.

Employee Signature: _____

School/Department: _____

Date: _____