INTERNET SAFETY AND NETWORK USE

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 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, chief technology officer, or authorized designee(s). This disabling is permissible only for a student seventeen (17) years of age or older or an authorized employee for the purpose as stated.

The network, internet and EBR device user shall be held responsible for his/her actions and activities using disciplinary actions summarized in the EBRPSS Rights & Responsibilities Handbook. Responsibilities include efficient, ethical and legal utilization of network resources, including appropriate use of all websites, applications, extensions, platforms, etc. District provided resources are managed by designees of the EBRPSS utilizing knowledge of classroom instructional practices and a standardized system for approving access to network resources per request via the Technology Helpdesk.

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, 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*. All policies and guidelines apply when using an EBR Device or when accessing the internet using EBR credentials or network connection, which

include an EBR sponsored hot spot or EBR SIM enabled device.

1. 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 seventeen (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 Contact – The terms *sexual act* and *sexual contact* have the meanings given such terms in section 2246 of title 18, United States Code.

   F. Artificial Intelligence - According to 15 U.S. Code § 9401 artificial intelligence is defined as “a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments.” The notes in 10 U.S. Code § 2358 define artificial intelligence as:

      1. “Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
      2. An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.
      3. An artificial system designed to think or act like a human, including cognitive architectures and neural networks.

4. A set of techniques, including machine learning, that is designed to approximate a cognitive task.
5. An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting."

2. 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. The following policies and guidelines apply to students when using an EBR Device or when accessing the internet using EBR credentials or network connection, which include an EBR sponsored hot spot or EBR SIM enabled device.

A. Online Safety Instruction

Prior to gaining access to the EBR network, all students will be educated about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, cybersecurity and cyber safety, cyber-bullying awareness and response.

B. E-Mail and Digital Telecommunications

In general, any student use of email and digital 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 and regulations in the *Student Rights and Responsibilities Handbook* as well as any other applicable policy, and local, state, and Federal law. The student and parent or guardian shall sign an East Baton Rouge Parish School Board *Internet and Network Usage Policy Agreement* prior to email account access being granted.

Students shall:

1. login and use email and digital telecommunications only with their student account.
2. not use e-mail chat rooms, net meeting rooms, and other forms of direct electronic communication including instant messaging systems unless authorized by the district. School system rules prohibiting indecent, vulgar, lewd, slanderous, abusive, threatening, sexually harassing, bullying, cyber-bullying or any form of terrorizing language apply to all forms of electronic communications.
3. not distribute private information about themselves or others.
4. not send spam, chain letters, or other mass unsolicited mailings.

5. not view, use, copy or distribute passwords to which they are not authorized.
6. directly with other students unless authorized by the district and directly supervised by a teacher or EBR staff. Not use any EBR technology resources or devices to communicate

C. Networks and Internet Use

In general, any student use of networks and the Internet must be for educational purposes. Students must respect and adhere to policies and regulations in the *Student Rights and Responsibilities Handbook* as well as any other applicable policy, and local, state, and Federal law. The student and parent or guardian shall sign an East Baton Rouge Parish School Board *Internet and Network Usage Policy Agreement* prior to access to the EBR network being granted.

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 their user ID.
3. use Internet search engines, approved Artificial Intelligence (AI), and/or other approved Internet tools only education purposes.
4. observe copyright laws, citing the source of information accessed over the Internet and/or accessed via Artificial Intelligence (AI) tools, using a standard system as directed by the school site leadership, teacher and/or librarian.
5. 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.
6. 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.
7. 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.
8. not use, download and install any file sharing program or anonymous proxy programs or websites that bypass the district filtering device.
9. not use technology resources to further other acts that are criminal or violate the school or district code of conduct.
10. not make any purchase on the Internet while using school equipment or Internet service.

11. not use online tools such as Artificial Intelligence (AI) or internet bots to commit criminal acts or violate the school or district code of conduct.
12. not intentionally connect any unapproved device to the EBR network (i.e., a WIFI router, etc.). Any such devices are subject to removal by the Division of Technology staff.
13. not utilize any form of personal hotspot or VPN service while at an EBR site.

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 shall 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 shall be determined in accordance with existing rules and procedures, both administrative and as stipulated in East Baton Rouge Parish School Board policy and including applicable law enforcement agencies when necessary.

D. Device Use

In general, any student use of EBR devices must be for educational purposes. Students must respect and adhere to policies and regulations in the *Student Rights and Responsibilities Handbook* as well as any other applicable policy, and local, state, and Federal law. The student and parent or guardian shall sign an East Baton Rouge Parish School Board *Internet and Network Usage Policy Agreement* prior to being granted access to an EBR device.

Students shall:

1. login and use EBR devices only with their student account and district assigned or approved device(s), close applications and logoff immediately after completing work to prevent unauthorized use their user ID.
2. not intentionally access, download, transmit, copy or create any materials or visual depictions on school or district that are indecent, vulgar, lewd, slanderous, abusive, threatening, harassing, terrorizing, or harmful to minors. All forms of cyber-bullying are strictly prohibited.
3. be responsible for the care and preservation of any EBR device assigned to them.

4. be responsible for intentional and incidental damage caused by the student to any EBR device.
5. not intentionally access or use developer tools on an EBR device to manipulate the device in any way.
6. not intentionally unenroll any EBR device from enterprise systems.
7. not use an EBR device assigned to another party unless authorized by the district and directly supervised by a teacher or EBR staff.
8. not use any EBR device to take unauthorized photos and/or videos of students or employees of the EBRPSS.

3. Employee Policies and Guidelines

Use of network resources, the Internet, and EBR devices 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 e-mail systems, must sign the East Baton Rouge Parish School Board *Internet and Network Usage Policy Agreement* and agree to abide by all district policies and regulations. Employees of EBRPSS will be able to access district accounts (i.e., district provided email and district enterprise systems such as Google Workspace) from an external network using a multifactor authentication process. The Board does not condone any illegal or inappropriate activities and shall 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 shall be reported to the appropriate law enforcement agency. The following policies and guidelines apply to all employees when using an EBR Device or when accessing the internet using EBR credentials or network connection, which include an EBR sponsored hot spot or EBR SIM enabled device. All information sent or stored on EBRPSS servers is property of the EBRPSS and may be subject to review and public records request.

A. Online Safety Instruction and Guidance

Prior to gaining access to the EBR network, all employees 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. Employees are required to annually receive training provided by the EBRPSS related to current trends in cybersecurity and cyber safety best practices.

B. E-Mail and Digital Telecommunications

Employees must use assigned e-mail accounts in support of educational purposes and conducting district business. All employees desiring to use digital telecommunications tools signify by their acceptance of an e-mail account and their signature on the East Baton Rouge Parish Board *Internet and Network Usage Policy 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~~ when access is attained through any authorized personal digital device while on School Board property.

Communication over East Baton Rouge Parish School Board 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 Board 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 use e-mail chat rooms, net meeting rooms, and other forms of direct electronic communication including instant messaging systems unless a method authorized by the district.
2. 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.
3. not send spam, chain letters, or other mass unsolicited mailings.
4. not view, use, or copy passwords to which they are not authorized.
5. not use technology resources to further other acts that are criminal or violate the school or district code of conduct or rules.
6. not disclose, use, or disseminate personal information regarding minors.
7. not use the e-mail system for commercial, political, personal activities or religious purposes.

8. not use any EBR technology resources or devices to communicate directly with students unless via a method authorized by the district.

9. not distribute students' private information**.**

10. not distribute other employees' private information.

C. Network and Internet Use

In general, any employee use of networks and the Internet must be for educational purposes. Employees must respect and adhere to the *Internet and Network Usage Policy* as well as any other applicable policy, and local, state, and Federal law.

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 certified and classified staff and Board members. Policy guidance related to Cybersecurity and Artificial Intelligence tools will be provided annually to mitigate risks to personal and private information.

Employees shall:

1. login and use their network account for only their own use.
2. 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.
3. 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.
4. not attempt to gain unauthorized access to modify or configure EBRPSS Technology resources or infrastructure**,** including so-called "hacking" or engage in any other unlawful conduct online, including willfully introducing malware or other harmful programs to the network.
5. not download non-work related files or access downloadable 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 policy and the respective streaming service's Terms of Use.
6. not download, ~~and~~ install and use any file sharing program, any proxy programs, servers or websites that bypass~~es~~ the district filtering device.
7. not use the network, email system, or district websites for personal financial gain, political advertising, or issue advocacy.

8. not use the network, email system, or district websites for fundraising purposes without prior written administrative approval.
9. 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.
10. not make any personal purchase on the Internet while using EBRPSS equipment or Internet service.

11. use only district provided or approved resources and programs (i.e. do not download non-approved PDF editors, etc.).
12. not intentionally connect any unapproved device to the EBR network (i.e., a WIFI router, etc.). Any such devices are subject to removal by the Division of Technology staff.
13. not use online tools such as Artificial Intelligence (AI) or internet bots to commit criminal acts or violate the school or district code of conduct.

14. not utilize any form of **unsecured** personal hotspot at an EBR site or unauthorized VPN service ***while connected*** to the EBR network**.**

15. use only the district approved web browsers unless directly authorized by the Department of Technology Services.

D. Device Use

All employees are responsible for knowing and adhering to school system policies regarding EBR devices. Employee policies and regulations apply to all EBRPSS employees, including certified and classified staff and Board members.

Employees shall:

1. login and use EBR devices only with their employee account and only use district assigned or approved device(s) unless authorized by the Division of Technology.
2. logoff and close applications or lock the device when leaving the computer unattended to prevent unauthorized access to sensitive, protected, or prohibited information.
3. not intentionally access, transmit, copy, or create any materials or visual depictions on school or district devices that are indecent, vulgar, lewd, slanderous, abusive, threatening, harassing, terrorizing, or harmful to minors. All forms of cyber-bullying are strictly prohibited.
4. not download, install and use any file sharing program, anonymous proxy programs, servers or websites that bypass~~es~~ the district filtering device.
5. be responsible for the care and preservation of any EBR device assigned to them.

6. be responsible for intentional and incidental damage caused by the employee to any EBR device.
7. not intentionally destroy, delete, or alter any district software or data collection/storage on an EBR device unless authorized by the Division of Technology.
8. not use developer tools, software removal tools, or third-party uninstallers unless directly authorized by the Division of Technology.
9. not intentionally unenroll any EBR device from enterprise systems unless authorized by the Division of Technology.
10. not use an EBR device assigned to another party unless authorized by the district.
11. use only district provided or approved technology resources and programs (i.e. do not download non-approved PDF editors, etc.)
12. return, to the designated person on their campus, any device(s) assigned to them if they resign, retire, relocate schools, get terminated, or are promoted.

E. Teachers Responsibility for Student Use of Networks, the Internet and EBR Devices

Teachers shall:

1. not allow students to use their teacher assigned device(s) or network account.
2. require students to login to the network with their district 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. seek and gain approval by their immediate supervisor before participating in online educational projects or courses requiring the input of any student technology data (i.e. student emails, etc.)
7. confirm the status of consent via a *Student Media Consent and Release* or 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).

4. 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 art of the district's commitment to protect 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 upon EBRPSS-owned devices.
5. EBRPSS employees should protect the technical resources under their control, such as passwords, devices 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. Port scanning or security scanning is prohibited unless prior notification to the EBRPSS's Division of Technology is made, and authorization is granted.
14. Leaving a computer unlocked and unattended.
15. Using instant messaging, voice over internet protocol, or video over internet protocol programs unless authorized for business use.
16. Using a personal streaming service account in a manner that violates the respective streaming service's Terms of Use.
17. Accessing anonymous proxy programs, servers or websites that bypass~~es~~ the district filtering device.

C. Password requirements for EBRPSS enterprise business application systems:

Passwords keep information safe and to prevent potential security breaches. Each employee is required to maintain 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 utilizing https://pass.ebrschools.org and reported to the EBRPSS technology help desk. 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 the district required interval. (Required)

The following should not be used:

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. A password on a computer suspected of having viruses or malware.

It is important to note that the practice of writing down passwords is discouraged.

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 computers connected to the EBRPSS network must have an approved 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 connected to the EBRPSS network must have antispyware program installed.
5. If it is believed a computer is infected with a virus or performing abnormally, the machine shall be turned off and the EBRPSS technology help desk shall be contacted immediately.
6. The use of non-standard programs or open-sourced programs is allowed only after approval of the is granted by the Division of Technology.

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, cloud-based storage, etc; whether it is a partial or full display of the number.

1. SSNs shall not be used 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.

5. General District Technology Guidelines

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.
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. District technical staff has the right and obligation to remove unauthorized and harmful hardware from EBR sites and will report the incident to the appropriate site and district administration.
8. Any computer that does not meet the requirements for the district network will no longer be maintained or repaired by the district.
9. Any computer accessing the Internet without network login and authentication must maintain current anti-virus software.

10. Site 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. 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. The student and parent or guardian shall sign an East Baton Rouge Parish Board *Internet and Network Usage Policy Agreement* prior to an e-mail account or access credentials being issued.

C. Grants

Any employee applying for a grant with a technology component must follow East Baton Rouge Parish School Board *DFF*, *Grants* policy and utilize the appropriate *Grant Technology Planning* form (Office of Coordinator of Grants).

D. Purchasing of Technology

1. EBRPSS Divisions and Departments

Any purchase of technology for an EBRPSS school or facility that is initiated and funded by any EBRPSS Division or Department must be planned in conjunction with the Department of Technology Services to ensure 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 any EBRPSS Division or Department if the technology was purchased without prior written agreement approved by the Superintendent, chief technology officer, or authorized designee(s).*

2. Outside Agencies and Organizations

Any purchase of technology for 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 ensure 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 if the technology was purchased ~~any~~ without prior written agreement approved by the Superintendent, chief technology officer, or 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.

Adopted: July 17, 1997
Amended: July 23, 1998
Revised: February 21, 2002
Revised: June, 2005
Revised: December, 2008
Revised: June 21, 2012
Revised: November 21, 2021

Ref: 47 USC 254(h), *Children's Internet Protection Act* (CIPA); La. Rev. Stat. Ann. §§17:81, 17:100.7, 17:280; Board minutes, 7-17-97, 7-23-98, 6-16-05, 6-21-12, 11-21-24.