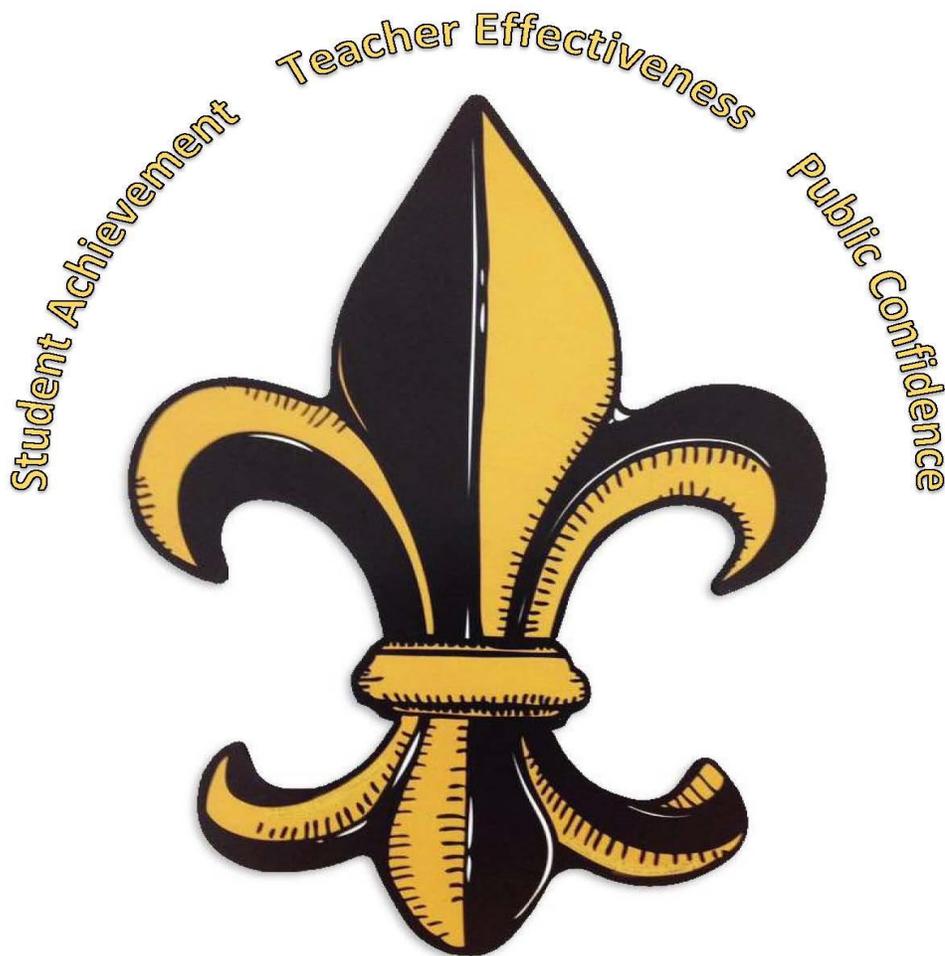


Bogalusa City Schools

Technology Handbook



Every Child, Every Day

TABLE OF CONTENTS

Mission, Vision, Motto, Why Technology	3
RESPONSIBLE USE PROCEDURES	4
Access to Network Information	6
Electronic Messaging Procedures	7
Internet Safety Procedures & Access	9
Network Connectivity	10
Home Internet	10
G Suite for Education	10
Social/Collaborative Content	10
Mobile Devices Procedures	10
Personally-Owned Devices Procedures	11
Security	11
Inspection	11
Procedure on Reloading Software	11
Netiquette	12
Plagiarism	12
Personal Safety	12
Cyberbullying	13
Responsible Use Expectations:	13
Examples of Irresponsible Use	14
Limitation of Liability	14
Violations of these Responsible Use Procedures	14
Distance Learning Plan	15
DEVICE POLICIES AND PROCEDURES	16
Taking Care of Your Device	17
Receiving Your Device	18
Device Check-In	18
Student Check-In Fines	18
Device Rules and Guidelines	18
Electronic Resource Policy and Device Usage Procedures	19
Copyright and Plagiarism	22
Technology Discipline	23
PERMISSIONS & AGREEMENTS	25
BCS Technology Acceptable Use Policy	26
BCS Technology Acceptable Use Policy Agreement Signature Sheet (All Grades)	27
BCS Technology Device Usage Policy	28
BCS Technology Device Usage Policy Agreement Signature Sheet (All Grades)	29

MISSION

The mission of Bogalusa City Schools is to be accountable to all stakeholders for providing a competitive education that empowers students to achieve academic and personal goals and to become college and career ready, productive, responsible citizens.

VISION

The vision of Bogalusa City Schools is to be a district of excellence preparing ALL students to live and compete successfully in the 21st Century.

MOTTO

Every Child, Every Day!

WE BELIEVE:

- Children have first priority on all of our resources.
- Education is the shared responsibility of the student, the parent/guardian, the school, and the community.
- Communication and understanding among all stakeholders of our community are essential to achieving the goals of education.
- Learning is a continuous process and most productive when the needs of each child are met through instruction provided by competent and caring teachers.
- A learning environment where everyone experiences security, care, dignity, and respect is essential.

WHY TECHNOLOGY:

- To empower learners to have the skills and resources necessary to be globally competitive.
- To ensure that our students are responsible users of technology and are Future Ready.
- To engage all learners and build their capacity as problem-solvers.

Responsible Use Procedures

Bogalusa City Schools (BCS) expects that all users will use technology, telecommunications and/or Internet tools in appropriate ways for the performance of tasks associated with their learning and assignments.

BCS recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st-century technology and communication skills. Toward that end, BCS staff will guide students in the proper, effective, and responsible use of telecommunications, electronic mail (messaging), Internet, and other technology usage.

These procedures apply to any use of technology within district property or at district sponsored events regardless of who owns the technology. These procedures do not attempt to state all required or prescribed behavior by users; however, some specific examples are provided.

Communication over networks and/or the Internet should not be considered private.

Network and/or Internet 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. Privacy in these communications is not guaranteed. The district reserves the right to access stored records in cases where there is reasonable cause to expect 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 for acceptable use.

BCS will specify those behaviors that are permitted and not permitted, as well as appropriate procedures to guide the users' use. In general, **users are expected to communicate in a respectful manner consistent with state laws governing the behavior of school users and with federal laws governing copyrights.**

Electronic messaging and telecommunications and/or Internet are not to be utilized to share confidential information about other users.

BCS encourages users to make use of telecommunications and/or the Internet

to explore educational topics, conduct research, and contact others in the educational world. BCS anticipates that new systems will expedite the sharing of effective practices and lessons across the district; and will help users stay on the leading edge of learning by forming partnerships with others across the nation and around the world.

Access to Networked Information Resources and/or Internet Procedures

The network and/or the Internet are provided for users to conduct research and communicate with others as directed and supervised by staff. Communications over the network and/or Internet are often public in nature, therefore general rules and standards for respectful behavior and communications will apply. Safety and security when using electronic messaging, chat rooms, and other forms of direct electronic communications are essential.

Electronic messaging, telecommunications and the Internet are not to be utilized by users to share confidential information about themselves or other users because messages are not entirely secure. **Unauthorized disclosure, use and dissemination of personal information regarding minors will not be permitted.**

Network administrators may review files and communications to maintain system integrity and to ensure that users are using the system responsibly. Users should not expect that files stored on district servers or any other storage device will be private, (i.e. CD ROM, hard drives, flash drives, backups, cloud storage, network storage, etc.).

The following behaviors are not permitted on district networks and/or the Internet:

- Sharing confidential information regarding users
- Sending or displaying offensive messages or pictures
- Assisting a campaign for election of any person to any office or for the promotion or opposition to any ballot proposition
- Using obscene language
- Harassing, insulting, or attacking others
- Engaging in practices that threaten the network (e.g. downloading files that may contain a virus)

- Unauthorized access to any network and/or network devices (e.g. hacking)
- Violating copyright laws
- Using others' passwords
- Trespassing in others' folders, documents or files
- Intentionally wasting limited resources
- Employing the network and/or Internet for commercial purposes
- Violating regulations prescribed by the network provider
- Promoting, supporting, or celebrating religion or religious institutions

The Technology department will report inappropriate behaviors to the staff's immediate supervisor or to the student's teacher who will take appropriate disciplinary action. Access to e-mail and other telecommunications and/or Internet is a privilege and violations of these procedures may result in a loss of access and/or disciplinary action up to and including expulsion. When applicable, law enforcement agencies may be involved.

Electronic Messaging, Internet Usage, and Other Technology Usage Procedures

In order to ensure compliance with local, state, and federal computer crime laws, copyright laws, and to prevent inappropriate and non-company related use of BCS Communication and Information Systems by BCS users and to protect BCS from being victimized by malicious acts of compromising organization assets, the following are BCS's regulations on the use of BCS Communication and Information Systems and/or Internet:

BCS Communication and Information Systems and/or the internet are not to be used as personal bulletin services. BCS Communication and Information Systems and/or Internet are not to be used in a way that may be disruptive, illegal, offensive to others, or harmful to morale, including unauthorized access and other unlawful activities. BCS maintains a process for monitoring user usage of BCS's Communication and Information Systems and/or Internet and will fully investigate suspected abuse. Users are responsible for preventing misuse of their technology devices and should take reasonable and appropriate precautions to protect BCS's systems, including securing their devices (logging off before leaving). BCS Communication and Information Systems and/or Internet are not to be used to transmit or knowingly receive vulgar, profane, insulting, or offensive messages, including racial, sexual slurs or jokes, harassing or threatening messages or pornography. BCS is required

to comply with all applicable federal laws and will report to authorities any individual accessing, transmitting, or knowingly receiving illegal information through the BCS Communication and Information Systems and/or Internet, either on a school owned or personal device, including child pornography and illegally obtained software or other media.

Users using BCS Communication and Information Systems and/or Internet are to use such services in a respectful manner so as not to damage the reputation of the organization. BCS Communication and Information Systems and/or Internet are to be used in compliance with the Student or Employee Handbook. BCS may choose to hold a user liable for any damage to BCS's reputation or systems as a result of a user's misuse or BCS's Communication and Information Systems and/or Internet.

The introduction of viruses, or malicious tampering with any computer system, is expressly prohibited. Questions on how to scan with virus detection software should be directed to the Technology Help Desk. All identified viruses must be reported to the Technology Help Desk.

Sensitive material transferred over the Internet may be at risk of detection by a third party without precautions. Users must exercise caution and care when transferring such material in any form. BCS' confidential information is not to be transmitted or forwarded to outside individuals or companies not authorized to receive the information or BCS users who do not have an approved educational need for the information. Alternate Internet Service Provider (ISP) connections to BCS' internal network are not permitted.

BCS reserves the right to restrict access to any materials that are inappropriate to minors and/or illegal materials. BCS also reserves the right to restrict access to and/or filter any type of direct communications (including electronic messaging and chat rooms) that are outside of the BCS Communication and Information Systems and/or Internet.

Vandalism is prohibited. Any malicious attempt to harm or destroy BCS equipment or materials, data of another user of the BCS' system, or any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to compromise, degrade, or disrupt system performance may be viewed as violations of BCS policies and administrative regulations and, possibly, as criminal activity under applicable state and federal laws. This

includes, but is not limited to, the uploading or creating of computer viruses.

BCS Communication and Information Systems and/or Internet are BCS property and are not private. Users do not have a personal privacy right in any material created, stored, received or sent in or through BCS Communication and Information Systems and/or Internet. By using BCS Communication and Information Systems and/or Internet, all users knowingly and voluntarily consent of their usage of these systems being monitored and acknowledge and agree to BCS' right to conduct such monitoring. BCS, in its sole discretion, reserves the right to access, monitor, copy, transcribe, forward, download, capture, and/or disclose all communications sent via any BCS Communication and Information System and/or Internet at any time, with or without prior notice. Violations of BCS' procedures on use of its Communications and Information Systems and/or Internet may result in disciplinary action up to and including expulsion or administrative leave.

Internet Safety Procedures and Access

BCS currently monitors and filters Internet traffic. Each year we evaluate whether to upgrade or purchase new or other products to give the organization and the services we provide the protection needed. Internet filtering blocks or filters Internet access, in accordance with the requirements of CIPA - Children's Internet Protection Act. Internet filtering protects against access by adults and minors to visual depictions that are obscene, child pornography, or - with respect to use of computers with Internet access by minors - harmful to minors. It may be disabled for adults engaged in legitimate, educational research or other lawful purposes. Filtering includes monitoring the online activities of minors.

BCS Internet filtering prevents access by minors to inappropriate content on the Internet and World Wide Web. It also has the right to monitor electronic messaging, chat rooms, and other forms of direct electronic communications and unauthorized accessing and other unlawful activities online. BCS is committed to the education of minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

Users are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web. If a site is blocked and

a user believes it shouldn't be, the user should follow district protocol to alert the Technology Department to submit the site for review. Unauthorized use of VPNs or proxy servers to bypass district content filter is prohibited.

Network Connectivity

Every effort will be made to have the network up and running each day, however BCS makes no guarantee that the network will be available 100% of the time. In the rare case that the network is down, the school will not be responsible for lost or missing data.

Home Internet Access

Users are allowed to set up access to home wireless networks on their devices. The user must provide home internet access. BCS may offer Internet service for home use where applicable.

G Suite for Education by Google

BCS will provide students with G Suite for Education accounts (Google accounts). Google accounts include free, web-based programs like email, document creation tools, shared calendars, and collaboration tools. This service is available through an agreement between Google and the State of Louisiana. This agreement ensures BCS Google student accounts are protected and not marketed for commercial purposes. G Suite runs on an Internet domain purchased and owned by the district and is intended for educational use. Your student's teachers will be using Google Apps within G Suite for lessons, assignments, and communication. Student Google accounts are also available at home, the library, or anywhere with Internet access. School staff will monitor student use of Apps when students are at school. Parents are responsible for monitoring their child's use of Apps when accessing programs from home. Students are responsible for their own behavior at all times. Google Account usage may be monitored and archived. G Suite is primarily for educational use.

Social/Collaborative Content

Recognizing the benefits collaboration brings to education, BCS may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users. Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users

should be careful not to share personally-identifying information online.

Mobile Devices Procedures

BCS may provide users with mobile computers or other devices to promote learning outside of the classroom. Users should abide by the same responsible use policies when using school devices not connected to the school network as when on the school network.

Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users should report any loss, damage, or malfunction to the Media Center immediately. Users may be financially accountable for any damage resulting from negligence or misuse. Use of school-issued mobile devices off the school network may be monitored.

If a student uses a telecommunication device without authorization during the school day, the device may be confiscated.

Personally-Owned Devices Procedures

Students should keep personally-owned devices (including laptops, tablets, smartphones/watches, and cell phones) turned off and put away during the class period-unless instructed by a teacher or staff for educational purposes.

Because of security concerns, when personally-owned mobile devices are used on campus, they should not be used over the school network without express permission from the building administrator.

The use of mobile telephones or any device capable of capturing images is strictly prohibited in locker rooms or restroom areas while at school or at school-related or school-sponsored events.

Security

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. **This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin.** If you believe a computer or mobile device you are using might be infected with a virus, please alert the Media Center. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

Inspection

Users may be selected at random to provide their device for inspection at any time.

Procedure on Reloading Software

If technical difficulties occur, the device will be restored from backup. The school does not accept the responsibility for the loss of any software or documents deleted due to a reformat and/or re-image.

Netiquette

Users should always use the Internet, network resources, and online sites in a courteous and respectful manner. Users should also recognize that among the valuable content available online is unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet. Users should also remember not to post anything online that they wouldn't want parents, teachers, or future colleges or employers to see. Once something is online, it's out there and can sometimes be shared and spread in ways you never intended.

Plagiarism

Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Unless otherwise noted, all software on the Internet should be considered copyrighted work. Therefore, users are prohibited from downloading software/apps and/or modifying any such files without approval.

Users are required to adhere to all licensing and copyright laws and cannot use electronic communications systems to send (upload) or receive (download) copyrighted materials including software.

Unauthorized users shall not place district, confidential or proprietary material (including but not limited to copyrighted software, internal correspondence, or e-mail) on any publicly accessible Internet device.

Personal Safety

Users should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without adult permission.

If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff if you're at school; parent if you're using the device at home) immediately.

Cyberbullying

Cyberbullying will not be tolerated. Examples include communications that seek to

- intimidate, control, manipulate
- put down or humiliate the recipient by
- harassing, dissing, flaming, denigrating, impersonating,
- outing, tricking, excluding, and cyberstalking.

Do not send emails or post comments in chat room discussion groups, on webpages or within instant messaging apps with the intent of scaring, hurting, or intimidating someone else.

Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges.

In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained.

Responsible Use Expectations:

I will:

- Bring my device to school each day.
- Use school technologies for instructional, classroom activities.
- Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- Treat school resources carefully, and alert staff if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher or other staff member if I see threatening, inappropriate, or harmful content (images, messages, and posts).
- Use school technologies at appropriate times, in approved places, for educational pursuits.
- Cite sources when using online sites and resources for research.

- Recognize that use of school technologies is a privilege and treat it as such.
- Be cautious to protect the safety of myself and others.
- Help to protect the security of school resources.
- The device battery must be charged and ready for school each day.
- Set up a charging station at your house and charge your device every night.
(highschool)

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies within a safe and responsible manner.

Examples of Irresponsible Use

I will not:

- Keep liquids in close proximity of the district issued device.
- Use school technologies in a way that could be personally or physically harmful.
- Attempt to find inappropriate images or content.
- Engage in cyberbullying, harassment, or disrespectful conduct toward others.
- Try to find ways to circumvent the school's safety measures and filtering tools.
- Use school technologies to send spam or chain mail.
- Plagiarize content I find online.
- Post personally-identifying information, about myself or others.
- Use language online that would be unacceptable in the classroom.
- Use school technologies for illegal activities or to pursue information on such activities.
- Attempt to hack or access sites, servers, or content that isn't intended for my use.
- Use my device in **inappropriate locations for example:** restrooms, locker rooms, cafeteria line

Limitation of Liability

BCS will not be responsible for damage or harm to persons, files, data, or hardware.

While BCS employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness. BCS will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network. Users are expected to follow the same rules for good behavior and respectful conduct online as offline. Misuse of school resources can result in disciplinary action.

Violations of these Responsible Use Procedures

Violations of these procedures may have disciplinary repercussions, including:

- Suspension of network, technology, or computer privileges
- Notification to parents

- Detention or suspension from school and school-related activities
- Legal action and/or prosecution

I have read and understood these Responsible Use Procedures and agree to abide by them. These Responsible Use Procedures outline the guidelines and behaviors that users are expected to follow when using school technologies or when using personally-owned devices on the school campus.

BCS provides Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more. As new technologies emerge, BCS will attempt to provide access to them (*See Distance Learning Plan - Communication Tools*). The policies outlined in this document are intended to cover all available technologies, not just those specifically listed. **All technologies provided by the district are intended for education purposes.** All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, respectful, and responsible; don't try to get around technological protection measures; use good common sense; and ask if you don't know.

Distance Learning Plan for BCS - Communication Tools

To support our Distance Learning Plan, BCS will employ our normal day-to-day platforms to communicate with parents, students and faculty/staff. All these systems are remotely accessible.

Channel	Audience	Description
Email	Faculty, Staff, Students, Parents	Email will be used for all major communications and announcements. Teachers will use email to communicate with students and use other platforms to interact with students for virtual learning.
Google G Suite	All students will have GSuite accounts	Google GSuite will continue to be the platform used by teachers (email, docs, Classroom, etc.)
Zoom	Students, Faculty/Staff	Zoom is an online video conferencing platform that allows for live group meetings, hosted by

		teachers.
D2L Brightspace	Faculty, Staff, Students, Parents	Learning Management System that contains online content for virtual learning.
Public Website	General Public	BCS will maintain up-to-date information about the District & Resources

Complete Parent and Student Acceptable Use Agreement - Signature Forms

DEVICE POLICIES & PROCEDURES

BCS views the use of the technology device as central to the delivery of its educational program and expects that all students will use these devices as an essential part of their learning experiences. It is the policy of BCS to maintain an environment that promotes ethical and responsible conduct in all electronic resource activities. With this privilege and extraordinary opportunity to explore technological devices come responsibilities for the parent and for the student.

When signing the Student/Parent Responsible Use Agreement, you are acknowledging that you understand and accept the information in this document.

Taking Care of Your Device

General Precautions

1. The device is school property and all users will follow these procedures and the Responsible Use Guidelines.
2. Only use a clean, soft cloth to clean the screen. No cleansers of any type.
3. Cords and cables must be inserted carefully into the device to prevent damage.
4. All BCS devices and cases must remain free of any personal writings, drawings, sticker, skins, or labels.
5. Devices must never be left in an unlocked room, unlocked car, or any unsupervised area.
6. Users must not remove any factory or BCS labels.
7. No food or drink is allowed near the electronic device.
8. Users are responsible for the general care of the device they have been issued. Devices that are broken or fail to work properly must be reported to the Technology department for an evaluation of the equipment.

Screen Care

The device screens can be damaged if subjected to rough treatment. The screens are particularly sensitive to damage from excessive pressure on the screen.

1. Do not lean on the top of the device
2. Do not place anything near the device that could put pressure on the screen.
3. Do not place anything heavy on top of the device.

4. Clean the screen with a soft, dry cloth, or anti-static cloth.
5. Do not “bump” the device against walls, car doors, floors, etc. as it will eventually break the screen.

Receiving Your Device

Devices will be distributed each school year with a schedule released by BCS administration. Users must sign and return the BCS Technology Handbook paperwork before the device can be issued.

Device Check-In

Student devices **MUST** be returned at the end of the school year so they can be checked for serviceability and summer storage. If a staff member or student transfers out of the BCS during the school year, the device and accessories **MUST** be returned at that time.

Student Check-In Fines

Devices and accessories must be returned to BCS at the end of each school year. That includes the device, case, charger, and charger cable. Students who graduate early, withdraw, are expelled, or terminate enrollment at BCS for any reason must return their device and accessories on the date of termination. If a student fails to return the device at the end of the school year or upon termination of enrollment, that student will be subject to criminal prosecution or civil liability. The student will also pay the replacement cost of the device at the fair market value. Failure to return the device will result in a theft report being filed with the local authorities.

Furthermore, the user will be responsible for any damage to the device and must return the device and accessories to the Technology Department in satisfactory condition. The user will be charged a fee for any needed repairs, not to exceed the replacement cost at the current fair market value of the device.

Device Rules and Guidelines

The rules and regulations are provided here so that students and parents/guardians are aware of the responsibilities students accept when using a district-owned device. In general, this requires efficient, ethical, and legal utilization of all technological devices. Violations of these rules and guidelines will result in disciplinary action. Please reference the materials

specific to each school or contact school directly for details. Students will receive device-related training at school on proper use and digital citizenship. Below you will find a review of the rules and guidelines.

Electronic Resource Policy and Device Usage Procedures

Devices are intended for use at school each day. In addition to teacher expectations for device use, student textbooks, learning management system, school messages, announcements, calendars, and schedules may be accessed using the device. Students are responsible for bringing their device fully charged to school each day.

Devices Left at Home

If students leave their device at home, they are responsible for getting the course work completed as if they had their device present. If a student repeatedly leaves their device at home, they will be required to have a meeting with the school administration to discuss the situation.

All Use of Technology Must:

- Support learning
- Follow local, state, and federal laws
- Be school appropriate

Security Reminders:

- Do not share logins or passwords unless asked to do so by a parent/guardian or school personnel
- Do not develop programs to harass others, hack, bring in viruses, or change others' files
- Follow Internet Safety guidelines

Storing the Device

When the device is not in use it should be stored in a safe place. Nothing should be placed on top of the device and the device should be locked. Devices should not be stored in a vehicle at any time.

Devices Left in Unsecured Areas

Under no circumstance should devices be left in unsecured areas. Unsecured areas include the school grounds and campus, the lunchroom, computer lab, locker rooms, library, unlocked classrooms, dressing rooms, and hallways. Any device left in these areas is in danger of being stolen. If a device is found in an unsecured area, it will be taken to the front office.

Saving to the Device

Storage space will be available, but it will NOT be backed up in case of re-imaging. The user is responsible for ensuring that work is not lost due to mechanical failure or accidental deletion. Device malfunctions are not an acceptable excuse for not submitting work.

Activities Requiring Teacher Permission During Instructional Time:

- Playing content-related games
- Sending email
- Using headphones in class, where related
- Use of camera for pictures or video
- Any activities per teacher/staff discretion

Activities PROHIBITED on School Property:

- Instant-messaging (e.g. FaceTime, SnapChat, KIK, WhatApp, etc.)
- Playing non-educational games
- Downloading programs, music, games, and/or videos (e.g. TikTok)
- Using a Hot Spot with a district-owned device (unless given permission)
- Any activities hindering the educative process per teacher/staff discretion

Inappropriate Content- All files must be school appropriate. Inappropriate materials include explicit or implicit references to:

- Alcohol, tobacco, or drugs
- Gangs
- Obscene language or nudity
- Bullying or harassment
- Discriminatory or prejudicial behavior
- Illegal activities

Email for Students' Purpose

All BCS students are issued an email account. Email allows students to safely and effectively communicate and collaborate with BCS staff and classmates, giving them an authentic purpose for writing. The effective use of email is:

- A 21st Century communication tool.
- Used in careers and higher education settings.

- A way to meet the International Society for Technology in Education (ISTE).

Guidelines and Reminders

- Email should be used for educational purposes only.
- Email transmissions may be monitored by the school at any time to ensure appropriate use. This means that any school personnel may check students' email.
- All email and its contents are the property of the district.
- Email should only be used by the authorized owner of the account.
- Students need to protect their passwords.

Unacceptable Email Use Examples

- Non-education related forwards (e.g. jokes, chain letters, images, etc.)
- Harassment, profanity, obscenity, racist terms
- Cyber-bullying, hate mail, discriminatory remarks
- Email for individual profit or gain, advertisement, political activities, or illegal activities

Webcams Purpose

Each student device is equipped with a webcam. This equipment offers students an extraordinary opportunity to experience a 21st Century tool and to develop 21st Century communication skills.

Examples of Use

Webcams are to be used for educational purposes only, under the direction of a teacher. Examples include:

- Recording videos or taking pictures to include in a project
- Recording a student giving a speech and playing it back for rehearsal and improvement
- Activating camera tools to actively engage in virtual lessons conducted and/or approved by your teacher

Important Note

BCS retains the rights concerning any recording and/or publishing of any student or staff member's work or image. Students must obtain permission to record, take, or publish a photograph or video of any person. **Unauthorized recordings are subject to disciplinary action in accordance with School Board Policy.** Additionally, parent(s) and/or guardian(s) must sign the **Media Release** form ensuring compliance with approved use of student images/likeness.

Media

- Listening to music on your device is not allowed during school hours without permission, from the teacher. Use your headphones.
- Watching movies on your device is not allowed during school hours without permission from the teacher. Permission will be given only for media used to complete a school assignment.

Gaming

- Online gaming is not allowed during school hours unless you have been given permission by a teacher. Any games must be in support of education.

Printing

- Any documents that require printing should be submitted to your teacher.

Wallpaper and other potentially damaging decor

- Any images set as the wallpaper must be in line with the Acceptable Use of Technology Resources Policy. Inappropriate media may not be used as wallpaper. Presence of guns, weapons, pornographic material, inappropriate language, alcohol, drugs, or gang-related symbols will result in disciplinary action.
- It is highly recommended to set the background lockscreen with your contact information to help expedite the return of your Device in the event it is lost/stolen.
- Only labels or stickers approved by BCS may be applied to the device.
- Keep the device free from magnets.

Copyright and Plagiarism

Students are expected to follow all copyright laws. Duplication and/or distribution of materials of educational purposes is permitted when such duplication and/or distribution would fall within the Fair Use Doctrine of the United States Copyright Law.

Technology Discipline

Behaviors and Discipline Related to Student Device Use

As a BCS community, we will continue to role model appropriate behaviors regardless of the location. The following behaviors will be treated as corresponding "traditional" behaviors and appropriate consequences will be assessed by the building administrators.

Refer to your grade level Code of Conduct for the corresponding disciplinary actions.

TECH-RELATED BEHAVIOR	EQUIVALENT "TRADITIONAL" BEHAVIORS
Email, instant-messaging, Internet surfing, games, or any other off-task behavior	Classroom Disruption
Removing keys/Damaging or Defacing Device	Defacing School Property
Cutting/Pasting without Citing Sources	Plagiarism
Cyber-bullying	Bullying/Harassment
Accessing digital pornographic material or inappropriate files	Bringing pornographic/inappropriate material to school
Accessing digital files potentially dangerous to network	Vandalism/Technology Policy Violation
Using electronic account authorized for another person without permission	Breaking into another student's locker/bookbag

The following behaviors could result in the possible loss of device or loss of access to district's network.

TECHNOLOGY VIOLATIONS CONTINUED Examples of potential behaviors unique to digital environment without "traditional" behavior equivalent
Chronic, tech-related behavior violations (see above)
Making use of electronic resources in a manner that serves to disrupt use of network by others
Unauthorized downloading or installing software
Attempts to defeat or bypass the district's Internet filter
Modification to district browser setting or any other techniques, designed to avoid being blocked from inappropriate content or to conceal Internet activity

School-Based Discipline

The discipline policies at each school encompass the one-to-one environment. Please reference the Code of Conduct specific to each school or contact school directly for details.

BCS may remove a user's access to the network without notice at any time if the user is engaged in any type of unauthorized activity.

Administration Consequences for Students

Campus Administration will address the inappropriate use of district or personal technology. **Administration Consequences for Staff**

District Administration will address the inappropriate use of district or personal technology.

PERMISSIONS & AGREEMENTS

Bogalusa City Schools - Technology Acceptable Use Policy

Bogalusa City Schools (BCS) views the use of the technology device as central to the delivery of its educational program and expects that all students will use these devices as an essential part of their learning experiences. It is the policy of BCS to maintain an environment that promotes ethical and responsible conduct in all electronic resource activities. With this privilege and extraordinary opportunity to explore technological devices come responsibilities for the parent and for the student.

When signing the **Student/Parent Responsible Use Agreement, you are acknowledging that you understand and accept the information in this document.**

Limitation of Liability

Bogalusa City Schools will not be responsible for damage or harm to persons, files, data, or hardware. While BCS employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

BCS will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Violations of these Acceptable Use Procedures

Violations of these procedures may have disciplinary repercussions, including:

- Suspension of network, technology, or computer privileges
- Notification to parents
- Detention or suspension from school and school-related activities
- Legal action and/or prosecution

This Chromebook and network are the property of Bogalusa City Schools and is for authorized use only.

The use of this Chromebook or any device connected to the network is governed by this Acceptable Use Agreement.

Using this Chromebook or connecting to the school system network in any way constitutes your acceptance of this agreement and willingness to adhere to all of the guidelines contained within it.

Users of this computer system or associated network (authorized or unauthorized) have no explicit or implicit expectation of privacy. Any or all uses of this system and all data stored or transmitted over the network may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized personnel and law enforcement.

Failure to comply with the Acceptable Use Agreement and all applicable laws will result in disciplinary actions, up to and including expulsion from school and criminal prosecution.

I have read and understood the Technology Acceptable Use Policy and Agree to abide by them.

Student Name _____ Grade _____

School _____

Parent or Guardian Section

I have read the District's Technology Acceptable Use Policies, also available online at:
<https://bogschools.org/Bogalusa%20City%20Schools%20-%20Technology%20Acceptable%20Use%20Policy.pdf>

I hereby release the district, its personnel, and any institutions with which it is affiliated, from any and all claims and damages of any nature arising from my child's use of, or inability to use, the district system, including, but not limited to, claims that may arise from the unauthorized use of the system to purchase products or services. **I understand that I can be held liable for damages caused by my child's intentional misuse of the system.**

I will instruct my child regarding restrictions against accessing material that are in addition to the restrictions set forth in the Technology Acceptable Use Policy. I also will emphasize to my child the importance of following the rules for personal safety.

I give permission for my child to access only those portions of the local and wide area network connections that are approved by the Bogalusa County Schools, and to use personal electronic devices/issued devices and services only as approved by the district.

Parent or Guardian Signature _____ Date _____

Parent or Guardian Name Printed _____

Phone _____ E-Mail _____

Student Section

I have read the district's Technology Acceptable Use Policy (site address above). I agree to follow the rules contained in this policy. I understand that if I violate the rules my account can be terminated and I may face other disciplinary measures.

Student Signature _____ Date _____

Please return this completed form to your child's school office.

Bogalusa City Schools - Device Usage Policy

The educational program at Bogalusa City Schools - grades PreK through 12th, includes a Chromebook that will be issued to your child for their use at school and at home.

Utilizing the Chromebook in BCS' learning environment gives students

- access to learn anywhere, anytime - both in classrooms and at home,
- narrows the digital divide between students, and
- promotes responsible use of today's ever changing technologies

Like textbooks, team uniforms and other school property issued to your child, there is a responsibility to take appropriate care of these valuable resources. The Chromebook is no different, but it does represent an increased cost to the district and liability to students and parents.

Our experience with mobile technology has shown students take great care of these tools. But we know that loss and accidents will happen. With Chromebooks, the cost of loss or damage can be significant.

To respond to this concern, the district has developed the **Device Usage Policy for Chromebooks** as a way for families to minimize and **reduce the financial risk** if a Chromebook is damaged or lost. Please review, provide signature where required.

Device Usage Policy Works as Follows:

ACCIDENTAL DAMAGE			INTENTIONAL DAMAGE		
In the event a Chromebook is accidentally damaged (ex. cracked screen, broken keys or unit, etc.), the repair cost to parents will be as follows:			In the event a Chromebook is intentionally damaged or destroyed the family is responsible for the full replacement cost.		
Incident	% of Parent Responsibility	Accidental Damage	Incident Type	Incident	% of Parent Responsibility
First	50%	Based upon repair cost	Stolen Device	All incidents	100% Responsible for Replacement Cost
Second*	100%	Based upon repair cost	A Stolen Device requires 1. a police report filed within 24 hrs 2. submit a copy of the police report to school.		
*Each subsequent incident will result in parent being 100% Responsible for Repair Cost			Lost Device	All incidents	100% Responsible for Full Replacement value.
BCS will be responsible for normal maintenance of the Chromebook including normal wear or malfunction due to manufacturing.			Lost Charger	All incidents	100% Responsible for Full Replacement value.
Each Chromebook issued contains a corresponding District Asset Tag (4-digit number), a Charger, and a bookbag..					

Note: At the end of the school year, or If a family leaves the District, but does not return the Chromebook and its charger, they will be charged for the full replacement costs, and standard rules for the restriction of records and transcripts would apply.

Bogalusa City Schools - Device Usage Policy Agreement - Signature Required

Student Name _____

Grade _____

School _____

STUDENT MUST READ AND SIGN BELOW:

I have read, understand and agree to abide by the terms of the **Device Usage Policy**. I agree it is ultimately my responsibility to make good choices when I use the Chromebook. Should I commit any violation or in any way misuse or abuse my Chromebook, I understand the extra protection afforded under the terms of the Device Usage Policy may be revoked and disciplinary action may be taken against me.

Student Signature

Date

Parent or Guardian Device Usage Policy Agreement

(to be read and signed by parents or guardians)

As the parent or legal guardian of this student, I have read, understand and agree that my child shall comply with the terms of the Device Usage Policy. **In the case of a lost, stolen, or damaged Chromebook, I accept responsibility for the replacement cost as outlined in the Device Usage Policy.**

PAYMENT SECTION:

Once a determination of damage has been assessed, the school will issue an invoice. **Checks should be made to Bogalusa City Schools and submitted to your school's office.**

I have read and understand the rules and the financial responsibilities of the Bogalusa City Schools' Device Usage Policy for Chromebooks. I agree to all terms and conditions of the program and voluntarily enroll my student for the current school year.

Parent/Guardian Name *(Please print clearly)*

Parent/Guardian Signature

Date

Please return this completed form to your child's school office.