

Regulation IFBG-R(1): Acceptable Use

Status: ADOPTED

Original Adopted Date: 04/20/2023 | Last Reviewed Date: 04/20/2023

The Bibb County School District ("District") provides a full range of digital resources ranging from electronic devices to cloud-based solutions, for students and staff. Use of all digital resources shall support the vision, mission, and goals established by the District. This Regulation sets forth the District's expectations regarding acceptable use of digital resources to provide a safe and secure online environment for the District, staff, and students.

A. Definitions

1. **Blogs** are websites that contain the writer's or group of writers' own experiences, observations, opinions, etc., and often have images and links to other websites.
2. **Child pornography** means any visual depiction, including any live performance, photograph, film, video, picture, or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, as such term is defined in O.C.G.A. § 16-12-100, when:
 - a. The production of the visual depiction involves a minor engaging in sexually explicit conduct;
 - b. The visual depiction is of a minor engaging in sexually explicit conduct; or
 - c. The visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
3. The **Cloud** is a virtual location that is accessible through the Internet. Users are able to store and share media as well as use applications in the cloud. Microsoft 365 is an example of a cloud-based platform containing multiple applications.
4. **Cyberbullying** is bullying or harassment that happens online. It is the intentional and/or repeated harm to others using computers, mobile handheld devices, and/or other electronic devices to torment, threaten, harass, humiliate, or embarrass others.
5. **Deepfake** is highly realistic and often convincing manipulated media, such as videos or audio recordings, created using generative artificial intelligence (AI) techniques like deep learning.
6. **Digital Citizenship** is being an active member in a society full of technology, knowing what is considered appropriate technology use, and behaving responsibly with electronic resources.
7. **Electronic Vandalism** is any malicious attempt to harm or destroy the data of an individual or network.
8. **Generative Artificial Intelligence (Gen AI)** refers to networks of computer systems that are capable of generating original content, such as written or visual materials, with minimal human input. Examples of Gen AI content include text, images, music, and videos. Traditionally, Artificial Intelligence (AI) has consumed and analyzed data sets.
9. **Hacking** is any attempt to gain unauthorized access to a computer system(s), network, and/or its resources.
10. **Hallucination** is a generative AI creation/output that is incorrect or misleading.

11. **Harmful to minors** means that quality of description or representation, in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when:
 - a. Taken as a whole, it predominantly appeals to the prurient, shameful, or morbid interest of minors;
 - b. It is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors; and
 - c. Taken as a whole, it is lacking in serious literary, artistic, political, or scientific value for minors.
12. **Identifiable minor** means a person:
 - a. (i) Who was a minor at the time the visual depiction was created, adapted, or modified; or
(ii) Whose image as a minor was used in creating, adapting, or modifying the visual depiction; and
 - b. Who is recognizable as an actual person by such person's face, likeness, or other distinguishing physical characteristic or other recognizable physical feature.
13. **Illegal activities** include any action that violates federal, state, local law, or Bibb County Board of Education policy or regulation.
14. **Inappropriate material** means material that does not serve an instructional or educational purpose which includes, but is not limited to, material that:
 - a. Is profane, vulgar, lewd, obscene, offensive, indecent, sexually explicit, threatening, or harmful to minors and or includes child pornography;
 - b. Advocates illegal or dangerous acts;
 - c. Causes disruption to the District, its employees, or its students;
 - d. Advocates violence;
 - e. Contains knowingly false, recklessly false, or defamatory information; or
 - f. Contains media created using artificial intelligence (AI) tools to cause a false or negative impact and/or to impersonate others (e.g., name, image, or likeness) for negative intent.
15. The **Internet** is a global information system that is logically linked together by a globally unique address space based on the internet protocol or its subsequent extensions; that is able to support unencrypted communications using the transmission control protocol/internet protocol (TCP/IP) suite, its subsequent extensions, or other internet protocol compatible protocols; and that provides, uses, or makes accessible, either publicly or privately, high level services layered on such communications and related infrastructure.
16. The **Intranet** is a controlled internal network that serves as a conduit for employee communication, access to resources, and the exchange of information only within the District.
17. **Multi-factor authentication (MFA)** is a security measure that requires users to provide multiple forms of verification, beyond just a password, to access an account or application.
18. A **Network** consists of devices connected to communicate, access, retrieve, or share information.
19. **Obscene material** means material which meets the following requirements:
 - a. To the average person, applying contemporary community standards, taken as a whole, the material predominantly appeals or panders to prurient interest in nudity, sex, or excretion;

- b. The material, taken as a whole, lacks serious literary, artistic, political, or scientific value; and
 - c. The material depicts or describes in a patently offensive way sexual conduct as follows:
 - (i) Acts of sexual intercourse, heterosexual or homosexual, normal or perverted, actual or simulated;
 - (ii) Acts of masturbation;
 - (iii) Acts involving excretory functions or lewd exhibition of the genitals;
 - (iv) Acts of bestiality or the fondling of sex organs of animals; or
 - (v) Sexual acts of flagellation, torture, or other violence indicating a sadomasochistic sexual relationship.
20. **Podcasts** are audio/video files that can be streamed or downloaded and viewed and/or listened to using an electronic device.
21. **School equipment** means any computer or computer networking equipment, technology or technology related device or service, or communication system or service that is operated, owned, leased, and made available to students by a local board of education, local school system, or public school and that is used for transmitting, receiving, accessing, viewing, hearing, downloading, recording, or storing electronic communication.
22. **Social media/social networking** is participation in online communities for the sharing of interests and information. Social media platforms consist of various Internet services, including blogs, chat rooms, discussion boards, and the creation of personal profiles. Facebook, Instagram, X, and Snapchat, are all examples of social media platforms.
23. **Sexting** is the act of sending images or messages of a sexual nature using an electronic device.
24. **Technology Protection Measure** means a technology that inspects and analyzes unencrypted internet traffic for malware and that blocks or filters electronic access to obscene materials, child pornography, or material that is harmful to minors.
25. **Technology Resources** are local and networked resources provided by the District such as, but not limited to: computers, smartphones, portable handheld devices, electronic reference databases, Internet access, communication/assessment tools, audio and video equipment, distance learning, virtual field trips, and other educational or administrative programs. Most applications are accessible via the Internet in the cloud.
26. A **User** is anyone who is authorized to gain access to the District's technology resources and school equipment.
27. **Web Tools** are web applications (i.e., blogs, wikis, RSS feeds, and social networking websites) that facilitate participatory information sharing and collaboration on the Internet.
28. **Wikis** are websites that allow users to add, delete, or revise content using a web browser.

B. Technology Protection Measures

The District implements technology protection measures to block or filter, to the extent practicable, student and adult internet access to visual depictions that are defined by this Regulation and applicable law as obscene, pornographic, or harmful to minors, or include child pornography. Unauthorized disabling or circumventing any District internet filtering system is strictly forbidden. If a website that is needed for teaching and learning is filtered, an educator may request that it be unblocked via a service request to Technology Services. Once reviewed for resolution, the educator will be notified. Internet filtering may be minimized for bona fide research or other lawful purposes and only with the approval of Technology Services.

Technology protection measures shall comply with the standards and specifications established by the Georgia Department of Education.

C. User Responsibilities

Users have an obligation to be responsible participants while using the resources that are available on the Internet and Intranet, and must adhere to all federal, state, and local policies. Illegal activities of any kind are strictly forbidden. The responsibilities include, but are not limited to, the following:

1. **Educational/Administrative purposes.** Users will use all technology resources and school equipment for educational or administrative purposes only. Users shall not access inappropriate material on the Internet or use school equipment for personal, commercial, or financial gain (excludes personal professional learning used to enhance teaching and instructional methods).
2. **Appropriate Material.** No school equipment shall be used for accessing, sending, receiving, viewing, or downloading obscene material, child pornography, or material that is harmful to minors, as defined in this Regulation.
3. **Safety.** Publishing confidential student information without parental permission is prohibited. The student Code of Conduct rules for bullying are also applicable to cyberbullying, and violators are subject to the same disciplinary procedures. If a user encounters inappropriate or confidential information or messages he/she is required to notify a teacher, school administrator, or supervisor immediately.
4. **Privacy.** There should be no expectation of privacy when using District technologies or school equipment. The District reserves the right to record, monitor, review, and report all activities including emails or text messages. Unless protected by state or federal laws (such as medical records or student records under the Family Educational Rights and Privacy Act ("FERPA")), activities may be subject to an open records request pursuant to the Georgia Open Records Act. If deemed appropriate, information may be disclosed by the District to the courts, law enforcement, authorized representatives or parents of students, or other third parties without users' consent.
5. **Passwords.** User accounts are to be used only by the owner of the account. A user's password is to be protected and never shared. Passwords must be strong, kept confidential, and not shared with anyone else. A strong password is at least 10 characters in length with a mix of lower case (abc . . .) and upper case (ABC . . .) letters, symbols (#*@ . . .) and numerals (123 . . .). Multi-factor authentication (MFA) is required for all staff District user accounts. Accounts and passwords that are provided, opened, or maintained by users in the performance of their work or learning on school equipment are considered property of the District and must be disclosed upon request.
6. **Data Security.** Users are responsible for ensuring that sensitive information is used and stored securely. Users must ensure that all sensitive information is kept out of direct sight of others or left where it is easily accessible to others. No employee shall knowingly provide District e-mail addresses to outside parties whose intent is to communicate with District employees, students, or their families for non-District or non-school related purposes. Employees who are uncertain whether particular activities are acceptable should seek further guidance from their immediate supervisor.
7. **Data Breach/Security Concern.** Users are expected to access authorized websites and files only. Any suspected security breach must be reported immediately. Students should notify a teacher or administrator of any security concerns. Employees are required to notify their supervisor and contact Technology Services. Any user identified as a security risk may have their access to school equipment restricted.
8. **Electronic vandalism.** Users should not knowingly upload or create computer viruses, spyware, malware, or modify another person's files. Hacking, identity theft, falsifying documents, and releasing confidential information are strictly prohibited and will result in consequences referenced in the student Code of Conduct.
9. **Transmitting and receiving inappropriate materials.** Users should not knowingly transmit or receive

any materials in violation of federal, state, or local law. This prohibition includes, but is not limited to, improperly used copyrighted material; materials that is threatening, obscene, pornographic, or harmful to minors and/or constitutes child pornography; or material protected by patent.

10. **Copyright.** Copyright infringement is prohibited. Users are expected to follow copyright laws and fair use guidelines as specified by Board policy and federal laws. Users are prohibited from illegally downloading or illegally copying from any electronic resource such as music, software, videos, etc.
11. **Posting Student Work.** Educators may post student-produced work that does not show personally identifiable information ("PII") internally or externally. Posting of PII requires the consent of a parent/guardian or eligible student. All postings shall be endorsed by a teacher or administrator. Postings shall be monitored, maintained, and removed when no longer required. All work produced using school resources can be used by the District without the express permission from a student or their parent/guardian.
12. **Digital Citizenship.** Users should be aware of the benefits, opportunities, and risks of using online digital resources. Users are responsible for advocating and practicing safe and legal use of digital information and communication technologies.
13. **Proxies.** Users shall not use anonymous proxies or other techniques to circumvent content filtering. Circumventing technology protection measures is strictly prohibited and is a direct violation of Policy IFGB.

D. Technology Expectations for Students

All students are expected to review and abide by all technology rules and regulations stated in the student Code of Conduct, including the "Technology Do's and Don'ts".

Reminder: All students are expected to adhere to policy **JCDAF: Use of Electronic Devices by Students** which states students are not allowed to use any personal device during the instructional day. Staff are expected to enforce this policy.

See also **Regulation IFBG-R(2) - Responsible Use of Generative AI.**

E. Technology Expectations for Staff

All staff are expected to review and follow any technology-related policies, rules, and regulations set forth by the District. Staff should review the District's Employee Handbook annually. See also **Regulation IFBG-R(2) - Responsible Use of Generative AI.**

F. Digital Media Resources and Learning Management Systems (LMS)

The District provides digital media resources and blended learning opportunities through several different platforms for instructional use with students. When using such platforms, the following practices are recommended:

1. Have a clear statement of the purpose and clear outcomes for the use of the digital media.
2. Use District-vetted and approved digital resources and District provided LMS.
3. Students are to follow the District's student Code of Conduct for online participation.
4. Teachers are to monitor their class's content and report inappropriate postings or material.

G. Online Platforms

Staff use of online platforms(blogs, wikis, podcasts, etc.) for educational purposes are an extension of the classroom. Whether at home or in school, any speech that is considered inappropriate in the classroom is also inappropriate to use online.

H. Personal Responsibility

Users are personally responsible for the content they publish online. Online posts intended for an audience of students or parents must be consistent with and relevant to the curricular activities in the classroom and align with the District's values and professional/ethical standards.

Staff are responsible for monitoring all forms of direct electronic communications, including but not limited to, threaded discussions, chat rooms, email, and communications used for educational purposes that are posted online.

1. Students who use online resources and applications are expected to act safely by keeping personal information out of their posts.
2. Comments made on school-related platforms should follow this Regulation, the Employee Handbook for staff, and the student Code of Conduct (for students).
3. Content that fails to meet established educational objectives or that is in violation of any provision of this Regulation, the Employee Handbook, or student Code of Conduct will be removed.

All District employees who use personal technology and social media shall assume all risks associated with the use of personal technology and social media at school or school-sponsored activities, including responsibility for preventing students' viewing or use of inappropriate Internet materials through the District employee's personal technology or social media account. The District expressly disclaims any responsibility for imposing content filters, blocking lists, or monitoring of its employees' personal technology and social media.

I. School and Teacher Websites

The District continues to support school websites. These websites may include pages for or links to information about teachers. This information is intended to support families wishing to contact a teacher. Course content and other related curriculum materials should not be placed on a school or teacher web page. Instead, it is expected that teachers utilize district technology tools, such as our LMS, to provide student access to district-supported content.

J. Consequences

The use of District technology resources is a privilege, not a right. Inappropriate use may result in disciplinary action and/or restriction of that privilege. Use of District school equipment is contingent upon compliance with federal and state laws, District policies and regulations, the Code of Ethics for Educators (for certified employees), the Employee Handbook (for all staff), and the student Code of Conduct (for all students).

Students who intentionally violate Policy IFBG or Regulation IFBG-R(1), whether or not such student was, at the time of such violation, on school property, on a school bus or other school vehicle, at a school related function, or elsewhere, shall be disciplined as set forth in the student Code of Conduct and as otherwise provided by law.

District employees who intentionally violate Policy IFBG or Regulation IFBG-R(1), whether or not such District employee was, at the time of such violation, on school property, on a school bus or other school vehicle, at a school related function, or elsewhere, shall be disciplined as set forth in the Employee Handbook and/or Code of Ethics for Educators, and as otherwise provided by law.

Any person who is not a student or District employee who violates Policy IFBG or Regulation IFBG-R(1), whether or not such person was, at the time of such violation, on school property, on a school bus or other school vehicle, at a school related function, or elsewhere, may have their rights to access school equipment suspended or terminated, and depending on the circumstances may be subject to further consequences, including but not limited to referral to law enforcement.

K. Complaint Procedures

Any person who believes a student has violated Policy IFBG or Regulation IFBG-R(1) may report the violation to the student's school administrator. The school administrator will then determine whether a violation occurred and what consequence, if any, is appropriate, as outlined in Section J, above. The school administrator will provide a written response to the complainant within ten (10) school days from receipt of the complaint.

Any person who believes a District employee has violated Policy IFBG or Regulation IFBG-R(1) may report the violation to the Assistant Superintendent of Human Resources. The Assistant Superintendent of Human Resources or designee

will then determine whether a violation occurred and what consequence, if any, is appropriate, as outlined in Section J, above. The Assistant Superintendent of Human Resources or designee will provide a written response to the complainant within ten (10) school days from receipt of the complaint.

Any person who believes someone other than a student or District employee has violated Policy IFBG or Regulation IFBG-R(1) may report the violation to the Director of Technology Operations. The Director of Technology Operations or designee will then will then determine whether a violation occurred and what consequence, if any, is appropriate, as outlined in Section J, above. The Director of Technology Operations or designee will provide a written response to the complaint within ten (10) school days from receipt of the complaint.

L. Expedited Review - Denial of Access

If a District employee believes that the application of Policy IFBG or Regulation IFBG-R(1) is denying the employee access to material that does not fall within the prohibitions of Policy IFBG or Regulation IFBG-R(1), the District employee may submit a ticket through the IT Helpdesk for review and resolution by Technology Services within one to three business days.

If a student believes that the application of Policy IFBG or Regulation IFBG-R(1) is denying the student access to material that does not fall within the prohibitions of Policy IFBG or Regulation IFBG-R(1), the student should report the request for access to the student's teacher. The student's teacher should then submit a ticket through the IT Helpdesk for review and resolution by Technology Services within one to three business days.

M. Disclaimer

The District makes no warranties of any kind, whether expressed or implied, for the school equipment provided. The District will not be responsible for any damage suffered including, but not limited to, loss of data resulting from delays, service interruption, and/or exposure to offensive or threatening material. Use of any information obtained via the Network, Internet, or Intranet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of any information obtained through its services, Network, Internet, or Intranet.

Nothing in this policy shall be construed to permit any access to materials that can be harmful to minors or that violate any local, state, or federal laws.

Individuals with questions, concerns, or complaints regarding the contents or requirements of this Regulation should contact Technology Services.
