

JEFFERSON COUNTY BOARD OF EDUCATION TECHNOLOGY ACCEPTABLE USE AGREEMENT

The Jefferson County Board of Education (the "Board") is pleased to provide network and Internet access to students. In exchange, student cooperation in exercising and promoting responsible use of this access is required.

The Technology Acceptable Use Agreement (AUA) applies to all technology resources owned, leased, operated, or maintained by the Board, regardless of the physical location of the resource or the user. It also applies to student use of all personally owned devices and technology resources (regardless of ownership) brought onto school grounds or to school activities during school hours or at school functions. Violations of the AUA and/or Board policy may result in suspension or termination of network or computer privileges, disciplinary action, and/or appropriate legal action. Each student and his or her parent or guardian will be solely responsible for unauthorized use of the Board's technology resources, and will bear any cost resulting from or associated with such unauthorized use or misuse including, but not limited to, any and all damages, restitution, liabilities and costs of defense incurred by the Board.

In exchange for access to and use of the Jefferson County Board of Education technology resources, I agree to abide by the Technology Acceptable Use Agreement and all Board policies, rules, and regulations regarding the use of technology. My signature on the Notice of Receipt page in the Code of Student Conduct indicates that I have received, understand and agree to all of the following terms, conditions and requirements:

Access

The Jefferson County Board of Education's technology resources are made available to students for bona fide educational and school-related purposes. All technology resources are the property of the Jefferson County Board of Education, and any use is by permission only.

- A. The use of all Board technology resources is a privilege, not a right, and inappropriate use will result in cancellation of those privileges. The district Technology Director and/or school administrators will determine when inappropriate use has occurred and may deny, revoke or suspend specific user privileges and accounts accordingly.
- B. Each student may use only accounts, files, software, and technology resources that are assigned to him/her and may not attempt to log in to the network as another person or use a computer that is logged on as another person.
- C. Students must not reduce the efficiency of use for others or attempt to modify or hack technology resources, utilities, and configurations, change the restrictions associated with his/her accounts, or attempt to breach any technology resource security system, either with or without malicious intent.
- D. A user may not copy software, programs, source code, data or any other computer resource for unauthorized or unlicensed use. A user may not modify or delete computer data or information of another student, faculty or the school.

- E. Students are not permitted to connect or install any computer hardware, components, or software, which is not school system property, without prior approval from the district technology department.
- F. All passwords are required to be kept private and may not be posted online.

Internet

- A. All school rules and guidelines for appropriate technology usage shall apply to Internet usage.
- B. No student may access, view, download, or attempt to access, view or download profane, lewd, obscene, pornographic, abusive, objectionable, illegal, or otherwise prohibited content on the Board's computer system or through any of its other technology resources or on personally owned devices.
- C. Student access to the Internet will be restricted in compliance with Children's Internet Protection Act (CIPA) regulations and Board policies. The Board has implemented filtering software and other security measures designed to block and prohibit access to inappropriate materials based on CIPA guidelines.
- D. The Board may also utilize monitoring software to control and monitor access to its system and the internet and to further the safety and security of its students. Any attempt to disable, modify or circumvent this software or other limiting device is strictly prohibited.

Privacy and Personal Safety

- A. There is no right or expectation of privacy in any Board technology resource, and the Board will monitor internet use, network use, electronic mail, or any other use of its technology resources without limitation. All computers, devices or other components of the Board's system may be inspected by the Board or its designees at any time.
- B. The Board cannot guarantee the privacy, security, or confidentiality of any information sent or received via the Internet.
- C. Student data will only be collected with district approved data collection resources to protect minors from unauthorized disclosure, use, and dissemination of personal data in compliance with FERPA (Family Educational Rights and Privacy Act).
- D. Students shall not reveal or post any personal or contact information about themselves or other people on websites and/or social media sites while utilizing the Board's technology resources. Personal information includes, but is not limited to, names, addresses, telephone numbers, photos or likenesses, video, ages, dates of birth, grade levels, social security numbers, or any other information by which a person might be identified.
- E. Any online message, comment, image, or anything else that causes a student to be concerned for his/her personal safety, should be brought to the attention of an adult. Students should immediately bring any threatening or unwelcome communications to the attention of school personnel.

Copyright and Plagiarism

- A. All users are expected to abide by copyright laws and to follow the Fair Use Guidelines for Educational Multimedia. If you don't know if your use of online material is legal or ethical, ask your teacher or administrator for guidance.
- B. Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Cyberbullying

- A. Cyberbullying will not be tolerated. Engaging in these behaviors will result in disciplinary actions and loss of privileges.
- B. Examples of cyberbullying include but are not limited to harassment, intimidation, threats, impersonation, insults, displaying offensive pictures, or lewd behavior.

Education of Students

- A. The Board provides ongoing education to all students concerning appropriate online behavior, including appropriate interaction with individuals on social networking websites and in chat rooms and cyberbullying awareness and response.
- B. Students are expected to adhere to specific classroom guidance and directives, as well as to the letter and spirit of this AUA and other Board policies. Use good judgment, and ask if you don't know.

Online Collaborative Systems

The Board provides valuable online learning resources to employees and students. These resources promote collaboration and provide a controlled environment for course content. Examples of online collaborative systems used by the Board include, but are not limited to, Google Apps for Education, Microsoft 365, Moodle, and Edmodo.

- A. Accounts for these services are provided to all students through a controlled environment that is for Board use only.
 - a. Email and other collaborative accounts are provided to students for educational purposes only.
 - b. Employees and students will collaborate in these environments on documents, presentations, quizzes, classroom assignments, and more.
- B. All school rules and guidelines for appropriate technology usage shall apply to online collaborative system.

Bring Your Own Device - BYOD

- A. Student devices must only access the Internet via the JefCoEd Public wireless network. **3G, 4G, or LTE access will not be allowed while on school property.**

- B. Permission for personal devices to be brought to school will be at the discretion of and as authorized by the local school administration.
- C. Personal devices are only to be used for educational purposes as directed by the teacher and/or school administration.
- D. Personal devices may not be used to record, transmit or post photographs, images, or video of a person or persons on campus during school activities and/or during school hours unless assigned or authorized by the teacher or school administrator.
- E. The school district may collect and examine any personal device at any time for the purpose of enforcing the terms of this agreement, investigating student discipline issues, or for any other school-related purpose. Personal devices are subject to immediate inspection when there is a reasonable suspicion that the contents or recent utilization of the device is in violation of any of the Board's policies, rules or regulations.
- F. The school or district assumes no responsibility for personal devices.
- G. Students are not allowed to loan, trade, or sell devices on district property, including school buses.

Violations of Acceptable Use Agreement

Violations of this agreement or other Board directives regarding use of technology may have disciplinary repercussions, including, but not limited to, the following:

- Suspension or termination of network, technology, or computer privileges
- Loss of privilege of bringing personally-owned technology devices to school
- Notification of and/or conference with parents
- Disciplinary actions as authorized by the Code of Student Conduct
- Financial accountability for damage or loss
- Legal action and/or prosecution

Limitation of Liability / Disclaimers

The Board makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the Board's technology resources will be error-free or without defect.

Although the Board employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

The Board will not be responsible, financially or otherwise, for unauthorized transactions conducted or financial obligations incurred on the system network.

The Board will not be responsible for damage or harm to persons, files, data, or hardware, or for any damages or losses incurred, including but not limited to: loss of data resulting from delays or interruption of service; loss of data stored on system resources; damage to personal property used to access system resources; the accuracy, nature, or quality of information stored on system resources; or unauthorized financial obligations incurred through system provided access.

CELL PHONE POSSESSION AND USE

The Jefferson County Board permits students to bring cell phones to school. Cell phone, (includes wearable technology used for phone purposes), use is permitted with permission for educational use (see BYOD page 34). However, cell phones brought to school must be stored appropriately, either in the student's backpack, locker, personal vehicle, and/or a designated place assigned by the administrator.

Cell phone use is prohibited during the school day (which is usually the time students arrive at school until dismissal) and anytime students are being transported on a school bus unless specific permission is given by a certificated school board employee.

Should a cell phone be either seen or heard, the phone will be taken from the student, and placed in an appropriate location until the parent reclaims it. A parent may reclaim any cell phone so taken during the hours specified by the school administrator. The school system, which includes the school, administrator, teacher or staff member, shall not assume responsibility for theft, loss, or damage to any personal/wireless communication device, even for cell phones that are taken. If the phone is suspected to contain illegal or inappropriate material, the administrator has the right to inspect the contents of the phone. Any illegal or inappropriate material found on the phone may lead to further disciplinary action. Violation of the rules regarding cell phone possession will be considered a Class I infraction (possession during the school day), Class II infraction (use during the school day or on a school bus), or Class III infraction (where context or manner of the use falls properly in the Class III infraction category), depending on the nature of the rule violated.

Cell phone use is prohibited during the school day unless used for educational purposes with the support of the local administration

Alabama State Department of Education Policy Use of Digital Device during the Administration of a Secure Test

Student Policy

The possession of digital devices (including, but not limited to, cell phones, MP3 players, cameras, or other telecommunication devices capable of capturing or relaying information) is strictly prohibited during the administration of a secure test. If a student is observed in possession of a digital device during the administration of a secure test, then the device will be confiscated.

If a student is observed using a digital device during the administration of a secure test, testing for the student will cease, the device will be confiscated and is subject to search, the student will be dismissed from testing, and the student's test will be invalidated.

Additional disciplinary action may be taken by the LEA.