JEFCOED ACCEPTABLE USE AGREEMENT

The 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. The AUA applies to all technology resources for remote learner use or virtual school use. 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 custodian 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, students agree to abide by the Acceptable Use Agreement and all Board policies, rules, and regulations regarding the use of technology. Signature(s) on the Notice of Receipt page for school registration indicates receipt, understanding and agreement to all of the following terms, conditions and requirements:

Access

The Jefferson County Board of Education's technology resources are made available to users 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 may result in cancellation of those privileges. Suspected inappropriate use may result in cancellation of privileges, pending investigation. The district Technology Director and/or school system administrators will determine when inappropriate use has occurred and may deny, revoke, or suspend specific user privileges and accounts accordingly.
B. Individuals may only use accounts, files, software, and technology resources that are assigned to, provided, or approved for him/her. Individuals may not attempt to log in to the network as another person or use a computer that is logged on as another person.
C. Individuals may not reduce the efficiency of use for others or attempt to modify 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. Individuals identified as a real or suspected security risk may be denied access.
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 user or the school.
E. Modification or alteration of the Board's resources without authorization of the technology director is strictly prohibited. Users may not modify system settings or install software without specific authorization from the technology director.
F. Users are not permitted to connect or install any computer hardware, components, or software, without prior approval from the district technology director.

Internet

A. All school rules and guidelines for appropriate technology usage shall apply to Internet usage.
B. Users may not access, capture/record, view, download, transmit or attempt to access, capture/record, view download, or transmit 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 users. Any attempt to disable, modify or circumvent this software or other limiting device is strictly prohibited.
E. Successful or unsuccessful attempts to bypass Internet or network filters by using proxies or other resources are a violation of this agreement.
F. Faculty and staff should screen all Internet resources before distributing them for use for instructional purposes.

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 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.
C. The Board cannot guarantee the privacy, security, or confidentiality of any information sent or received via the Internet.
D. 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).
E. 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.
F. 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.
G. All passwords are required to be kept private.

Care of Devices

A. The device is the property of Jefferson County Schools and all users should follow the procedures outlined in the JEFCOED Acceptable Use Agreement.
B. Students are responsible for the care of the device(s) assigned to them.
C. Adding stickers, markings, or other cosmetic alterations is prohibited.
D. Identifying information on the device added by the school or manufacturer may not be removed.
E. Students should only use the device(s) assigned to them.
F. Damaged or malfunctioning devices must be turned in to the school for evaluation and/or repair as soon as the damage or malfunction is discovered.
G. Cords and cables should be inserted carefully into the device to prevent damage.
H. Devices should not be left unattended, in an unlocked locker, or in a vehicle.
I. Students should protect the device from extreme heat or cold, food or liquids, small children, and pets.
J. In case of theft, the school must be notified immediately so a police report can be filed.
K. Deliberate damage to a device and/or device accessories, including but not limited to, cases, cords, and headphones, as determined by the school administrator or Director of Technology may result in disciplinary action in accordance with the Student & Parent Handbook and restitution may be required.

Copyright and Plagiarism

A. All users are expected to abide by copyright laws and to follow the *Fair Use Guidelines for Educational Multimedia*. If students do not know if use of online material is legal or ethical, ask teachers or administrators 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 may result in disciplinary actions and/or 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 Workspace for Education, Schoology (LMS), and single sign-on applications such as Clever and ClassLink.

A. Accounts for these services are provided to all users through a controlled environment that is for Board use only. A Google Workspace for Education unique account will be assigned to each student.

- Email and collaborative accounts are provided for educational purposes only.
- Students will create, save, and collaborate in these environments via email, documents, presentations, quizzes, classroom assignments, and more.

B. All school rules and guidelines for appropriate technology usage shall apply to online collaborative systems, including the Learning Management System (LMS).

Devices

A. Personally owned devices will not be allowed to access the Internet via the JEFCOED network. **Personal hotspot/wifi access is not allowed while on school property for personally-owned or district devices.**
B. Personally owned or district 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 school administration.
C. The school or district assumes no responsibility for personal devices.
D. Technical support will not be provided for personal devices.
E. Students are not allowed to loan, trade, or sell devices.

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 JEFCOED Student & Parent Handbook
- 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.