



Belton School District #124 Authorization for Network Access & Technology User Agreement

Each student and his or her parent(s)/guardian(s) must electronically sign the Authorization for Network Access & Technology User Agreement before being granted access to the District network & devices. Please read this document carefully before signing.

This document does not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. **The failure of any user to follow these terms will result in the loss of privileges, disciplinary action, and/or appropriate legal action.** The acceptance of this document is legally binding and indicates the parties who signed have read the terms and conditions carefully and understand their significance.

Terms and Conditions

Acceptable Use - Access to the District's network must be: (a) for the purpose of education or research, and be consistent with the District's educational objectives, or (b) for a legitimate school activity.

Privileges - The use of the District's network and technology is a privilege, not a right, and inappropriate use will result in restrictions of those privileges. District administration will make all decisions regarding whether or not a user has violated the terms of access privileges and may deny, revoke, or suspend access at any time.

Unacceptable Use - The user is responsible for his/ her actions and activities involving the network. Some examples of **unacceptable uses are:**

- Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any State or Federal law;
- Downloading unauthorized software;
- Hacking or gaining unauthorized access to files, resources or entities, as well as using non-district proxies;
- Invading the privacy of individuals: this includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature, including a photograph or video;
- Using another user's account or password;
- Using technology in any way to bully others;

- Posting material authored or created by another without his/her consent;
- Posting malicious anonymous messages;
- Accessing, submitting, posting, publishing, engaging, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, bullying, racially offensive, harassing, commercial in nature, political, religious, or illegal material. J. Using the network while access privileges are suspended or revoked.
- Using electronic media that disrupts the educational process or interferes with the rights of others at any time;
- Intentionally disrupting or interfering with the District network, servers or other technology;
- Sending mass communications to multiple users without prior authorization by the appropriate teacher or district administrator;
- Misrepresenting one's identity in electronic communications..
- Taking unapproved videos/photos of people and events at school, and/or the posting of such on any website is strictly forbidden.
- Plagiarize or use of others' work without written permission. Users will respect intellectual property of other users & information providers and obey copyright guidelines, providing proper citation.

Reliability - All users are responsible for backing up their own data. The District makes no guarantee of any kind, whether expressed or implied, for the network service it is providing. The District will not be responsible for any damages the user suffers.

Indemnification -The user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any violation of this *Authorization*.

Security - Network security is of the highest priority. If a security problem is identified on the network or Internet, users must notify appropriate District personnel. Users are not to demonstrate the problem to other users. Users are to keep account and password information confidential. Attempts to log on to the network and/or Internet as another user could result in privilege restrictions.

Vandalism -Vandalism is defined as any malicious attempt to harm or destroy any district technology tool, data of another user, the Internet, the Intranet, or any other network. Vandalism will result in cancellation of privileges as well as appropriate disciplinary action and financial responsibility for damages incurred. This includes, but is not limited to, the uploading or creation of computer viruses.

Internet Safety - Each District device with Internet access will be filtered that attempts to block most depictions which are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act (CIPA), and as determined by the Superintendent or designee. Staff members shall supervise student use of District Internet access to ensure compliance.

Digital Citizenship - Students are expected to comply with digital citizenship requirements. The District has developed digital citizenship programs, which include cyberbullying and what actions to take if they are bullied or are a witness to it, as well as online security and safety.

Student Data Privacy – The District complies with FERPA, COPPA, and CIPA. All student data collected through district services and devices is protected. Only approved educational tools may be used, and personal data may not be entered into unapproved third-party platforms.

Educational Software - The District employs a thorough vetting process that examines educational value as well as data privacy, and only approves use of tools that meet those high standards. Software is provided solely for educational purposes and is subject to privacy protections under FERPA and COPPA. The District provides students with accounts for online learning platforms including Google Workspace for Education core products and additional services. Students may only use district-approved artificial intelligence (AI) tools under direct supervision for educational purposes. Misuse (e.g., for cheating or personal data sharing) is strictly prohibited.

Use of Electronic Communications - The District's communication systems, its constituent software, hardware, and data files, are owned and controlled by the District and are provided as educational tools. Even though CIPA does not require the District to filter emails, the Belton School District has a filtering system in place. However, it does not assure all spam will be caught, nor does it assure all personal emails from outside district accounts will be delivered.

- The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. All electronic communications accounts shall be accessed only by the assigned user.
- Any message received from an unknown sender via the Internet should be immediately deleted. If the message is deemed to be of an inappropriate nature, the user needs to notify a school administrator or teacher.
- Downloading any file attached to an Internet-based message is prohibited unless the user is certain of the message's authenticity and the nature of the file transmitted.
- Messages relating to, or in support of, illegal activities will be reported to the authorities.
- Users are never to reply to or share any communication containing any password or sensitive information.
- Use of the School District's communication systems constitutes consent to these regulations.

Authorization Signature

I have read this *Authorization for Network Access & Technology User Agreement*. By signing this agreement, the parent/guardian gives permission for the school district to act on their behalf to create and manage accounts for any approved software including, but not limited to, Google, PowerSchool, Heartland, Follett, NWEA and DESE testing programs. I understand access is designed for educational purposes and the District has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the District to restrict access to all controversial and inappropriate materials. I will hold harmless the District, its employees, representatives, or Board members, for any harm caused by materials or software obtained via the network. I accept full responsibility for supervision, if and when my child is not in a school setting and on a district-issued device. I have discussed the terms of this *Authorization* with my child, and hereby request that my child be allowed access to the District's network resources.

By entering your name below it will be considered your electronic signature for this form.