



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

Parent(s)/guardian(s) must electronically sign the Authorization for Network Access and Technology User Agreement for each enrolled student before the student is granted access to District networks, accounts, and devices. Please read this document carefully before agreeing.

This document does not attempt to state all required or prohibited behavior by users; examples are provided. **Failure to follow these terms may result in loss or restriction of privileges, disciplinary action, financial responsibility where permitted by law and District policy, and/or appropriate legal action.** By electronically signing, the student and parent/guardian acknowledge that they have read the terms and conditions carefully and understand their significance.

Terms and Conditions

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

Privileges - Use of the District's network and technology is a privilege, not a right, and inappropriate use may result in restrictions of those privileges. District administration will determine whether a violation has occurred and may deny, restrict, suspend, or revoke access consistent with District policy and applicable law.

Unacceptable Use - The user is responsible for their actions and activities involving District technology resources. Examples of unacceptable use include:

- Using District technology resources for illegal activity, including violating copyright, license agreements, or other contracts, or transmitting material in violation of State or Federal law;
- Downloading or installing unauthorized software, applications, browser extensions, or files;
- Hacking or gaining unauthorized access to files, resources, accounts, or systems, or using proxies, virtual private networks (VPNs), or other methods to bypass District security, filtering, or access controls;
- Invading the privacy of others, including the unauthorized disclosure, distribution, or use of personal or confidential information, photographs, video, or audio;
- Using another user's account or password, or sharing account credentials with another person;
- Using technology to bully, threaten, harass, or discriminate against others;
- Posting or distributing material authored or created by another person without permission when permission is required;
- Posting malicious anonymous messages;
- Accessing, submitting, posting, publishing, or displaying material that is defamatory, abusive, obscene, sexually explicit and unrelated to an approved educational purpose, threatening, bullying, discriminatory, harassing, fraudulent, otherwise unlawful, or materially disruptive to the educational environment;
- Using the network while access privileges are suspended or revoked;
- Using electronic media in a manner that materially disrupts the educational process or interferes with the rights of others;
- Intentionally disrupting or interfering with the District network, servers, devices, or other technology;
- Sending mass communications to multiple users without prior authorization from the appropriate teacher or District administrator;
- Misrepresenting one's identity in electronic communications;
- Taking or posting photographs, video, or audio without authorization when authorization is required by law or District policy;

- Plagiarizing or using another person's work without permission or proper attribution. Users must respect intellectual property rights and comply with copyright and licensing requirements, including citation where appropriate.

Reliability - Users are responsible for backing up their own data. The District makes no guarantee, expressed or implied, for the network service it provides. To the extent permitted by law, the District is not responsible for loss of data, service interruptions, or damages resulting from the use or unavailability of District technology resources.

Responsibility for Loss or Damage - Users may be held responsible, to the extent permitted by law and District policy, for losses or damages resulting from intentional misuse of District technology resources.

Security - Network and information security are of the highest priority. If a security problem or suspected compromise is identified, users must promptly notify appropriate District personnel and must not demonstrate, exploit, or share the problem with other users. Users must keep account, password, and authentication information confidential. Attempts to log on as another user may result in privilege restrictions and disciplinary action.

Vandalism - Vandalism is any malicious attempt to harm or destroy a District technology resource, the data of another user, the Internet, the intranet, or another network. Vandalism may result in cancellation of privileges, appropriate disciplinary action, and financial responsibility for damages to the extent permitted by law and District policy. This includes, but is not limited to, uploading or creating malicious code, including computer viruses.

Internet Safety - The District uses filtering technology on District Internet access that is designed to block visual depictions that are obscene, constitute child pornography, or are harmful to minors, as required by the Children's Internet Protection Act (CIPA). Students should not attempt to bypass protections in place.

Digital Citizenship - Students are expected to comply with digital citizenship requirements. District digital citizenship instruction includes cyberbullying awareness and response, reporting concerns, and online security and safety.

Student Data Privacy - The District complies with FERPA, COPPA, CIPA, and other applicable requirements. Student data collected through District services and devices is handled in accordance with applicable law, District policy, and approved agreements. Only approved educational tools may be used, and personal or confidential data may not be entered into unapproved third-party platforms.

Educational Software - The District uses a review process that considers educational value and data privacy and approves tools that meet District requirements. Software is provided for educational purposes and is subject to applicable privacy protections. The District provides students with accounts for online learning platforms, including Google Workspace for Education core products and additional services. Students may use District-approved artificial intelligence (AI) tools only when authorized by a teacher or District staff member for an educational purpose. Misuse, including cheating, impersonation, or sharing personal or confidential information, is prohibited.

Use of Electronic Communications - The District's communication systems, software, hardware, and data files are owned and controlled by the District and are provided as educational tools. The District uses filtering and security tools for electronic communications. These tools cannot block all spam or inappropriate messages, and legitimate messages from external accounts may sometimes be blocked or delayed.

- The District may access, monitor, preserve, or disclose District-system records when reasonably necessary for system administration, safety, security, investigation, or legal compliance, consistent with applicable law and District policy. Except for authorized District access, accounts may be accessed only by the assigned user;

- Users must not reply to, click links in, or open attachments from suspicious or unexpected messages. Suspicious messages should be reported to a teacher, administrator, or District technology staff member;
- Downloading or opening a file attached to an electronic message is prohibited unless the user reasonably verifies the sender, authenticity, and nature of the file;
- Messages relating to, or in support of, illegal activities may be reported to the appropriate authorities;
- Users must never reply to or share communications requesting a password, authentication code, or other sensitive information;
- Use of the District's communication systems constitutes consent to these regulations.

Authorization and Electronic Signatures

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.

Parent/Guardian Acknowledgment and Authorization

I have read this Authorization for Network Access and Technology User Agreement and discussed its terms with my child. By signing, I authorize the District to create and manage accounts for my child for District-approved educational software and services, including, but not limited to, Google, PowerSchool, Heartland, Follett, NWEA, and DESE testing programs. I understand that access is designed for educational purposes and that the District uses reasonable filtering and safety measures designed to limit access to inappropriate material; however, no filtering system can restrict access to all inappropriate material. When my child uses a District-issued device outside a school setting, I will provide reasonable supervision and reinforce this agreement. I request that my child be allowed access to the District's network and technology resources.