



Bellflower Unified School District

Network, Digital Resources, and Internet Acceptable Use Agreement

General

Internet, network access, district-provided devices, software, online accounts, and e-mail, which are provided by Bellflower Unified School District, are intended for educational use, instruction, research, and the facilitation of communication, collaboration, and other educational-related purposes. This includes access to and use of approved Artificial Intelligence (AI) tools, social media platforms for educational purposes, and other emerging technologies. Users are expected to uphold courteous, professional, ethical, and respectful standards while using these District-provided tools and resources. All use of District technology resources must comply with this agreement, the Bellflower USD Bring Your Own Device (BYOD) Policy, Board Policy, and applicable laws.

Prohibited Uses of the Network, Digital Resources, Internet, and Email

Users may not engage in any of the activities listed below as prohibited. If users are unsure whether a specific behavior/usage is permitted, they should contact their teacher or site principal before engaging in the activity.

Prohibited Uses

- Transmission or accessing of any material in violation of any federal or state law.
- Distribution of information which violates or infringes upon the rights of any other person.
- Transmission or accessing Information that is defamatory, inappropriate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, discriminatory (based on any protected characteristic), harassing, bullying, cyberbullying, or illegal.

- Advertisements, solicitations, commercial ventures, or political lobbying not previously approved by District administration.
- Transmission of or accessing information which encourages the use of controlled substances or the use of the system for the purpose of inciting crime or violence.
- Material which violates intellectual property law, including unauthorized sharing of music, video, software, or any other material under copyright. This includes plagiarism, such as submitting work generated by any AI tool as one's own without proper attribution or permission, and the unauthorized use or reproduction of content generated by AI tools where the user does not have the rights to do so.
- Damaging computer/network equipment, devices, files, data, or the Internet system in any way (including knowingly or negligently spreading computer viruses, vandalizing data, unauthorized alteration of District hardware or software configurations, or engaging in conduct that could interfere with or disrupt the District's educational or business environment). Students using personal devices on the District network must ensure their devices maintain up-to-date antivirus and malware protection.
- Gaining or attempting to gain unauthorized access to the District's Internet and Network systems, other users' accounts or files, or any third-party systems through any means (ex. Phishing, hacking, malicious tampering, sharing or disclosing passwords to anyone other than their own parents/guardians, etc.). Users are responsible for the security of their passwords and accounts.
- Attempting to gain access to material that is blocked or filtered by the District. Any attempt to bypass the District's network filters is prohibited.
- Using District technology resources, including District WiFi bandwidth with personal devices, for non-educational personal use that is excessive or interferes with educational activities.
- Using District-provided accounts (e.g., email, learning platforms) for any personal or non-district related activities, including personal social media.
- Creating, accessing, or transmitting an identifiable visual depiction of oneself or another student under the age of 18 (child pornography).
- Misrepresenting one's identity or assuming the identity of another person (false impersonation), including sending anonymous emails or creating fake profiles for malicious purposes.
- Cheating or academic dishonesty, including using technology or AI tools to complete assignments or tests in a manner not authorized by the teacher.
- Using "non-supervised AI platforms" without explicit teacher permission and guidance.
- Recording the voice or image of another without their consent, or in any way that

disrupts the educational environment or invades privacy.

The District reserves the right to take immediate action if any of the following instances occur:

- Student activity/behavior on the network or with District digital resources creates a security and/or safety issue for staff, students, the network, or internet resources.
- Student use of District resources in ways that the District determines to be lacking in legitimate, approved uses or is deemed inappropriate.

Filtering and Monitoring

While it is impossible to control all content on the Internet, the District has in place a network filter. In compliance with the Children's Internet Protection Act (CIPA), the District blocks or filters content on the District's network/internet that is deemed inappropriate for minors, lacking educational or work-related content, or poses a threat to the network. Users shall not use any website, application, or any other methods to bypass the filtering of the network or perform any other unlawful activities. The District monitors the use of its network and digital resources to ensure compliance with this agreement and applicable laws. Users should have no expectation of privacy in their use of District technology resources, including email, internet access, and files stored on District systems, except as provided by law. Personal devices used on the school network are subject to search by school administrators if suspected of a violation of school/district policy.

Data Handling

In accordance with the Children's Online Privacy Protection Act (COPPA), the district is committed to protecting the privacy and safety of student data when using educational websites, apps, and online services. Each year, the district will request permission that allows the district to act as the parent's agent in providing consent for the collection and use of student information within the school context.

This approach is permitted under the FTC's COPPA Rule when student information is used exclusively for educational purposes and not for commercial or other unrelated uses. By accepting this agreement, you, as a parent or legal guardian, acknowledge and consent to the district acting as your agent under COPPA for the purpose of providing consent on your behalf for the collection and use of your child's personal information by educational websites, applications, and online services used within the

school setting.

By granting this permission, parents authorize the school to manage access to educational websites and applications on behalf of their child, ensuring that all data collected is used solely to support learning, instruction, and academic progress. The district maintains control over the use of student data and requires that all approved providers adhere to strict limitations on data use. The district thoroughly reviews all online resources to ensure they meet strict data privacy and security standards. Any personal information collected through these services will be used only in ways consistent with educational goals and will not be shared for marketing, advertising, or any other non-educational commercial purpose.

Student Internet and Digital Safety

Student Responsibilities

- Students will not send abusive messages to anyone, transmit material to anyone that is threatening, obscene, disruptive, sexually explicit, protected by trade secret, or that could be interpreted as harassment or disparagement of others based on their race/ethnicity, national origin, gender, sexual orientation, age, disability, religion, or political beliefs. This includes any form of cyberbullying or harassment.
- Students should not reveal personal information (home address, phone number, full birthdate, passwords, or other sensitive data) about themselves or other persons on publicly viewable social networking sites, in chat rooms, in emails, or other direct electronic communications, or any other forum over the Internet, unless specifically authorized and guided by a teacher for an educational purpose.
- Students should not display photographs or videos of themselves or the images of others without appropriate consent and for educational purposes as directed by school staff. Recording others without consent is prohibited.
- Students should not meet in person anyone they have met only on the Internet without parental/guardian knowledge and approval, and ideally, in a safe, public place with adult supervision if such a meeting is deemed necessary by parents/guardians.
- Students must promptly disclose to their teacher or other school employee any message, image, video, or other activity they receive or observe that is inappropriate, makes them feel uncomfortable, or they believe violates this agreement.

- Students should not allow any devices (District-provided or personal devices used for school purposes) to save their passwords, and should log out of accounts when finished using a shared or public device.
- Students will respect copyrights, including proper citation of sources and adherence to fair use guidelines. This includes acknowledging the use of permitted AI tools in generating content as per teacher/district guidelines to avoid plagiarism.
- Students will not use the District network or digital resources in any way that will disrupt the use of the network by others.
- Students will use approved AI tools responsibly and ethically, for learning and research as permitted by their teachers. They will not use AI to cheat, plagiarize, engage in false impersonation, or misrepresent their own work. They will be mindful of the potential biases and inaccuracies in AI-generated content and will critically evaluate such information.
- Students using social media for approved educational purposes (e.g., class groups, school clubs) will maintain a respectful and appropriate tone, adhering to all other provisions of this AUP. Accessing personal social media using District networks or accounts is subject to the prohibitions on personal use outlined in this agreement and the BYOD policy.
- Students are responsible for taking precautions to protect their personal data and the data of others when using technology.
- Students participating in the BYOD program (grades 6-12) must adhere to the Bellflower USD BYOD Policy, including using devices with teacher approval for educational purposes and ensuring their device is charged before arriving at school.

Parent Responsibilities

- Parents are primarily responsible for transmitting their particular set of family values to their children.
- Parents will discuss with their children what material is and is not acceptable for their children to access and create through District and personal technology, including social media and AI tools.
- Parents are exclusively responsible for monitoring their children's use of the Internet and all digital resources, including District software platforms and personal devices, when accessed from home or a non-school location.
- Parents will report to their child's teacher or other school employee any message or other activity their child makes them aware of which is inappropriate or concerning while using the Internet or other digital resources for school purposes.

- Parents are encouraged to discuss online safety, digital citizenship, the responsible use of AI, concerns about plagiarism and false impersonation, and the contents of this AUP and the BYOD Policy with their children regularly.
- Parents understand that while students in grades 6-12 may bring personal devices to school under the BYOD policy, the District is not responsible for lost, loaned, damaged, or stolen personal devices.

Violations of The Acceptable Use Agreement and BYOD Policy

The District reserves the right to terminate or restrict any user's access to the District's network, digital resources, and Internet systems.

If a student violates this agreement or the BYOD Policy, appropriate disciplinary action will be taken consistent with the violation, California Education Code, Board Policy, the student handbook, and local law enforcement codes. Devices used for unlawful purposes or in violation of policy may be confiscated. If a student's access is revoked, the student may not be penalized academically. The District will ensure that the student continues to have a meaningful opportunity to participate in all educational programs provided. Consequences may include, but are not limited to, loss of access privileges, disciplinary action as outlined in the student code of conduct, confiscation of devices, restitution for damages, and referral to law enforcement if applicable.

Limitation of Liability

Bellflower Unified School District makes no warranties of any kind, whether expressed or implied, for the service it is providing. Bellflower Unified School District is not responsible for any claims, losses, damages, costs, or other obligations arising from use of the network or accounts. This includes, but is not limited to, the loss of data or revenue resulting from delays, non-deliveries, misdeliveries, or service interruptions caused by the District's own negligence or a user's errors and/or omissions. Use of the internet, network, or any District digital resource (including District WiFi with personal devices) is at the user's own risk. The District is not responsible for personal devices if they are lost, loaned, damaged, or stolen. The District is not responsible for any unauthorized charges or fees, including data charges to personal accounts that might be incurred during approved school-related use with personal devices, resulting from access to the Internet or online services. The District is not responsible for the accuracy or quality of information obtained through or stored on the system.

