ACCEPTABLE USE POLICY STAFF

TERMS AND CONDITIONS FOR USE OF TECHNOLOGY AT BAINVILLE PUBLIC SCHOOLS
2020-2021 School Year

THIS IS A LEGALLY BINDING DOCUMENT. PLEASE READ THE FOLLOWING BEFORE SIGNING THIS DOCUMENT.

Introduction

Access to BPS's network is a privilege, not a right. The use of technology whether owned by BPS or devices supplied by the Users entails personal responsibility. It is expected that Users will comply with BPS rules, act in a responsible manner, and will honor the terms and conditions set by BPS.

This Acceptable Use Policy outlines the guidelines and behaviors that all users are expected to follow when using school technologies or when using personally-owned devices on the school campus, including:

- The BPS network is intended for educational purposes.
- All activity over the network or using district technologies may be monitored and retained.
- Access to online content via the network may be restricted in accordance with our policies and federal regulations, such as the Children's Internet Protection Act (CIPA).
- Misuse of school resources can result in disciplinary action up to and including termination of employment.
- BPS makes a reasonable effort to ensure safety and security online, but will not be held accountable for any harm or damages that result from use of school technologies. Every User must take responsibility for his or her use of technology and make every effort to avoid inappropriate types of content.
- Users of the district network or other technologies are expected to alert BPS immediately of any concerns for safety and/or security.

Technologies Covered

BPS may provide the privilege of Internet access, desktop computers, mobile computers or devices, video conferencing capabilities, online collaboration capabilities, message boards, email, and more.

This Acceptable Use Policy applies to both school-owned technology equipment utilizing the BPS network, the BPS Internet connection, and/or private networks/Internet connections accessed from school-owned devices at any time. This Acceptable Use Policy also applies to privately-owned devices accessing the BPS network, the BPS Internet connection, and/or private networks/Internet connections while on school campus, busses, or events. As new technologies emerge, BPS will seek to provide access to them. The policies outlined in this document cover *all* available technologies now and into the future, not just those specifically listed or currently available.

Usage Policies

All users are expected to use good judgment and to follow the specifics as well as the spirit of this document: be safe, appropriate, careful and kind; don't try to get around technological protection measures; use good common sense; and ask if you don't know. A User is defined as anyone, including employees, students, and guests attending school or any school-related activity or are on a school bus.

Web Access

BPS provides its users the privilege of access to the Internet, including web sites, resources, content, and online tools. Access to the Internet will be restricted as required to comply with CIPA regulations and school policies. Web browsing may be monitored and web activity records may be retained indefinitely.

Users are expected to respect the web filter as a safety precaution, and shall not attempt to circumvent the web filter when browsing the Internet. The determination of whether material is appropriate or inappropriate is based solely on the content of the material and the intended use of the material, not on whether a website has been blocked or not. If a user believes a site is unnecessarily blocked, the user should submit a request for website review through a report to administration.

Email

BPS may provide users with the privilege of email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies. If users are provided with email accounts, the account(s) should be used with care. Users should not attempt to open files or follow links from unknown or untrusted origins; should use appropriate language; and should only communicate with other people as allowed by the district policy or the teacher. Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

Social / Web/ Collaborative Content

Recognizing the benefits collaboration brings to education, BPS may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users. Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally identifying information online.

Security

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. If you believe a computer or mobile device you are using might be infected with a virus, please alert BPS administration. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

Downloads

Users should not download or attempt to download or run *.exe* programs (executable/or installable programs) over the school network or onto school resources without express

permission from IT staff. You may be able to download other file types, such as images of videos. For the security of our network, download such files only from reputable sites, and only for education purposes.

Netiquette

Users should always use the Internet, network resources, and online sites in a courteous and respectful manner. Users should recognize that among the valuable content online there is also unverified, incorrect, or inappropriate content. Users should only use trusted sources when conducting research via the Internet.

Users should remember not to post anything online that they wouldn't want students, parents, teachers, or future colleges or employers to see. Once something is online, it's out there—and can sometimes be shared and spread in ways you never intended.

Plagiarism

Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Personal Safety

Users should never share personal information, including phone number, address, social security number, birthday, or financial information of yourself or others, over the Internet without permission. Users should recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others. Users should never agree to meet in real life someone they meet online without parental permission. If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of administration for reference to technology staff.

Cyber Bullying

Cyber bullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyber stalking are all examples of cyberbullying. Don't be mean. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else. Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyber bullying can be a crime. Remember that your activities are monitored and retained.

Cyber bullying includes inappropriate communication. Inappropriate communication includes, but is not limited to, the following: obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language or images typed, posted, or spoken by students; information that could cause damage to an individual or the school community or create the danger of disruption of the academic environment; personal attacks, including prejudicial or discriminatory attacks; harassment (persistently acting in a manner that distresses or annoys

another person) or stalking of others; knowingly or recklessly posting false or defamatory information about a person or organization; and communication that promotes the destruction of property, including the acquisition or creation of weapons or other destructive devices. If a student is told to stop sending communications, that student must cease the activity immediately.

Vandalism

Vandalism will result in a cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy hardware or data of another user, Internet, or network. This includes, but is not limited to, the uploading or creation of computer viruses.

Examples of Acceptable Use

I will:

● Use school technologies for school-related activities.
● Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
● Treat school resources carefully, and alert staff/administration if there is any problem with their operation.
● Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
● Alert a teacher or other staff member/administration if I see threatening, inappropriate, or harmful content (images, messages, and posts) online.
● Use school technologies at appropriate times, in approved places, for educational pursuits.
● Cite sources when using online sites and resources for research.
● Recognize that use of school technologies is a privilege and treat it as such.
● Be cautious to protect the safety of myself and others.
● Help to protect the security of school resources.
● Help to protect the security of school resources.

Examples of Unacceptable Use

I will **not** :

Vandalize computers, software or devices (Major Offense)
● Use school technologies in a way that could be personally or physically harmful. (Major offense)
● Attempt to find inappropriate images or content; intent to seek inappropriate images or content is a violation of this Acceptable Use Policy. (Major Offense)
● Create a personal mobile “hot-spot” or utilize a “proxy site” for the purpose of circumventing network safety measures and filtering tools. (Major Offense)
● Use school technologies for illegal activities or to pursue information on such activities. (Major Offense)
● Attempt to hack or access sites, servers, or content that isn’t intended for my use. (Major Offense)
● Engage in cyber bullying, harassment, or disrespectful conduct toward others. (Depending on degree, Major or Minor Offense)
● Try to find ways to circumvent the school’s safety measures and filtering tools; intent to

circumvent safety measures and filtering tools is a violation of this Acceptable Use Policy. (Minor or Major Offense depending on severity)
● Agree to meet someone I meet online in real life. (chatting Minor Offense, meeting Major Offense)
● Create, distribute or deploy multi-user servers or gaming software on or within the JCISD network. (Minor Offense)
● Use computer for shopping for nonacademic items Minor Offense
● Use school technologies to send spam or chain mail. (Minor Offense)
● Plagiarize content I find online, including downloads, or printing. (Minor Offense)
● Post or otherwise disclose personally-identifying information, about myself or others. (Minor Offense)
● Use language online that would be unacceptable in the classroom. (Minor Offense)
● Violate rules of net etiquette and common sense (Minor Offense)
● Log onto another user's account without permission (Minor Offense)
● Alter computer files, desktops or other setting without permission (Minor Offense)
● Download and or install software from internet or home without permission (Minor Offense)
● Access any email program other than school approved without express permission. (Minor Offense)

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Limitation of Liability
● BPS will not be responsible for damage or harm to persons, files, data, or hardware.
● While BPS employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.
● BPS will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.
● BPS will not be responsible, financially or otherwise, for lost, stolen, or damaged devices.

Violations of this Acceptable Use Policy
Violations of this policy may have disciplinary repercussions, including but not limited to:
• Suspension of network, technology, or computer privileges;
• Notification to parents;
• Detention or suspension from school and school-related activities;
• Employment disciplinary action up to and including termination.
• Legal action and/or prosecution.

School Assigned Equipment:
BPS owns any assigned electronic equipment, including Chromebooks, and may access that equipment, search it, or remove it at any time

EXCEPTION OF TERMS AND CONDITIONS - These terms and conditions reflect the agreement of the parties and supersedes all prior oral and written agreements and understandings of the parties. These terms and conditions shall be governed and interpreted in accordance with the laws of the State of Montana and the United States of America.

All acceptable use policy violations are subject to disciplinary procedures up to and including termination.

[For additional information, see policy 3612 and 5450]