

RESPONSIBLE USE OF TECHNOLOGY AND INTERNET AGREEMENT

The Bluffton-Harrison Metropolitan School District (“BHMSD” or “Corporation”) considers technology integral to our learning environment and believes that it will only continue to grow in importance. In this age, students denied access to modern technology resources would be as unable to function in the learning environment as students denied books or pencils.

Therefore, given that a wide variety of digital electronic devices and internet-based technologies are utilized at all grade levels across the curriculum in support of teaching, learning, and assessing traditional and technology standards, given that many traditional resources are now available online only, and given our requirement and obligation as a school district to teach technology standards and digital citizenship, the use of modern educational resources such as computers and the internet is an acknowledged condition of enrollment.

Introduction

BHMSD recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. The Corporation is committed to helping students develop progressive technology and communication skills. To that end, the Corporation provides the privilege of access to technologies for student and staff use.

BHMSD is committed to providing educational opportunities for all students, and it maintains compliance with the state and federal nondiscrimination laws in its provision of technology.

This Responsible Use of Technology and Internet Agreement (“Agreement”) outlines the guidelines and behaviors that all Corporation students and employees (collectively “Users”) are expected to follow when using school technologies or when using personally owned devices on BHMSD property, including:

- Corporation network is intended for educational purposes.
- All activity over the network or using Corporation technologies may be monitored, documented 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).
- Students are expected to follow the same rules for good behavior and respectful conduct online as offline.
- Misuse of Corporation resources can result in disciplinary action.
- Corporation makes a reasonable effort to ensure students’ safety and security online by using an internet filter and other technologies, however, it will not be held accountable for any harm or damages that result from the use of Corporation technologies.
- Users of the district network or other technologies are expected to alert technology staff immediately of any concerns for safety or security.

Technologies Covered

BHMSD may provide the privilege of internet access, desktop computers, mobile computers or

devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more.

This Agreement applies to any Corporation-owned technology equipment including school-owned devices utilizing the Corporation network or internet connection and school-owned devices utilizing private networks/internet connections. This Agreement also applies to privately owned devices accessing the Corporation network, the Corporation internet connection, and/or private networks/internet connections while on BHMSD property. As relevant new technologies emerge, Corporation will seek to provide access to them. The policies outlined in this Agreement cover all technologies provided by the Corporation or used on Corporation property or network, not just those specifically listed or currently available.

Usage Policies

All technologies provided by BHMSD are intended for educational purposes. All users are expected to use good judgment by following this Agreement, the Student Code of Conduct and social media policy, and all other Corporation policies. The use of technology is a privilege, not a right. Use of technology may be prohibited during certain times or activities. Users should be safe, appropriate, careful and kind; not try to circumvent technological protection measures; use good common sense; and ask if unsure.

Pursuant to Federal law, students shall receive education about the following:

- Safety and security while using email, chat rooms, social media, and other forms of direct electronic communications.
- Dangers inherent with the online disclosure of personally identifiable information.
- Unauthorized disclosure, use, and dissemination of personal information.

Staff shall provide instruction for students regarding the appropriate use of technology and online safety and security as specified above. Furthermore, staff shall monitor the online activities of students while in school. Monitoring may include, but is not necessarily limited to, visual observations of online activities during class sessions or use of specific monitoring tools to review browser history and network, server, and computer logs.

Web Access

BHMSD 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 Corporation 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 the Technology Department.

Email

BHMSD may provide users with the privilege of email accounts for the purpose of school-related communication. Availability and use may be restricted based on Corporation policies.

If users are provided with email accounts, the accounts should be used with care. Users should not send personal information and should not attempt to open files or follow links from unknown or untrusted origins. Users should use appropriate language and should only communicate with other people as allowed by Corporation policies or staff.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

Mobile Devices Policy

BHMSD may provide users with mobile computers or other devices owned by Corporation to promote learning outside of the classroom or efficient performance of job functions. Users should abide by the same Agreement and policies when using Corporation devices off the Corporation network as on the Corporation network.

Users are expected to treat Corporation devices with extreme care and caution. Users should immediately report any loss, damage, or malfunction to technology staff. Users may be financially accountable for any damage resulting from negligence or misuse. Use of school-issued mobile devices off the school network may be monitored in appropriate situations. Users should have no expectation of privacy in Corporation-owned devices.

Personally Owned Devices

BHMSD offers a filtered public Wi-Fi on all Corporation property. Students in grades K-12 may bring a personal device to school and use it for educational purposes. Students are expected to connect to the non-public Wi-Fi using their login credentials. In addition, students should be aware of the following guidelines:

- Students are solely responsible for personal devices they bring to school.
- Corporation assumes no responsibility for personal devices if they are lost, loaned, damaged, or stolen, and only limited time or resources will be spent trying to locate stolen or lost items.
- Personal devices may be subject to investigation in accordance with Corporation policy.
- Students must keep personal devices secure at all times and not loan personal devices to others.
- Students must keep devices on silent or vibrate mode.
- Users of the Corporation's public Wi-Fi network have filtered internet access just as they would on district-owned devices. Only guests are to access the Corporation's public Wi-Fi network.
- Subject to school and teacher discretion, students may bring personal devices (laptop, netbook, cell phone, tablet, smart watches or other wearable devices, etc.) to school.

- By connecting to the Corporation's public Wi-Fi, users accept the terms of this Agreement and the school's agreement located on the school's website. Only guests are to access the Corporation's public Wi-Fi network.

Security

Users are expected to take reasonable safeguards against the transmission of security threats over the Corporation network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. This also includes using a passcode or password on all devices and not sharing that password with anyone. Users should never share personal information. Users should immediately report any suspicious information or activity to a teacher or an appropriate administrator.

A user shall never use another user's password or account, even with the permission from the user. Any need to have access to another user's account should be addressed with IT or their designee.

If users believe a computer or mobile device they are using might be infected with a virus, they should alert IT. Users should not attempt to remove the virus themselves or download any programs to help remove the virus.

Search of Technology or Devices

By entering into this Agreement, the user agrees that any device subject to the Agreement, including school-owned devices used anywhere and personally owned devices used on the Corporation network or on Corporation property, is subject to search by an appropriate school staff member. See Board Policy A300. Users shall have no expectation of privacy in the use of Corporation-owned technology subject to this Agreement.

If a user creates a password or code to restrict access to email, files, a device or other technology subject to this Agreement, the user will provide access to that information when requested to do so only by the user's supervisor, teacher, or the Technology Department. Students shall not be required to divulge personal information for access to a non-District managed technology.

An appropriately trained staff member may examine a device and search its contents if the administrator has reasonable suspicion to believe that the device contains evidence of unlawful conduct or conduct that is in violation of school rules. The search, however, will be limited in scope based upon the limitations of the Fourth Amendment and any other applicable legal restrictions. School staff members may also use software or other techniques to search for the location of a device subject to this policy if the device is reported missing or stolen.

Responsible Use

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 use only known or trusted sources when conducting research via the internet.

Users should not post anything online that they wouldn't want students, parents, teachers, or future colleges or employers to see. Once something is online, it cannot be completely retracted and can sometimes be shared and spread in ways the user never intended.

Plagiarism and Copyright

Users are not to 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. Information obtained via the internet should be appropriately cited, giving credit to the original author.

Users will respect the rights of copyright owners, including in their use of materials found on, disseminated through, or posted to the internet. Copyright infringement occurs when a work that is protected by a copyright is reproduced without explicit permission from the copyright holder or outside the limitations of copyright law.

Personal Safety

Users should never share personal information, including phone number, address, social security number, birthday, or financial information over the internet without adult 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 person someone they meet online without parental permission.

If users see a message, comment, image, or anything else online that makes them concerned for their personal safety, they should immediately bring it to the attention of an adult or supervisor. All students and those staff members who work directly with students shall receive annual training on social media safety, cyberbullying, and appropriate responses.

Cyberbullying

Cyberbullying, including but not limited to harassing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking, will not be tolerated. Users should not be mean or send emails or post comments with the intent to harass, ridicule, humiliate, intimidate, or harm the targeted person and create for the targeted person an objectively hostile school or work environment.

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, cyberbullying can be a crime. Users should remember that online activities may be monitored and retained.

All students will be educated about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response. School uses an anonymous reporting tool for students to report bullying to appropriate staff members.

Email, Social Media, Collaborative Content

Recognizing the benefits collaboration brings to education, BHMSD 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.

Please refer to the Social Media Policy for additional information on social communication.

Social Media Policy

Websites and other social media provide the corporation with unique and ever-changing ways which provide information to the community. Websites allow for current and complete information to be provided to its community at large. Websites for purposes of this policy include all forms of social media used by the school corporation to communicate to the community, parents, and students.

The Corporation website provides a resource for obtaining information about the Corporation and for informing patrons about School Board activities and serves as a vehicle for communication to parents and patrons.

Electronic media includes all forms of social media, such as text messaging, instant messaging, electronic mail (e-mail), blogs, electronic forums (chat rooms), video-sharing websites, group messaging applications, editorial comment posted on the Internet, social network sites, and all forms of telecommunication, such as landlines, cell phones, and web-based applications. Electronic mail or a district approved communication platform is the recommended electronic media between any BHMSD employee and student.

Use with Students

A certified employee may use electronic media to communicate with currently enrolled students about matters within the scope of the employee's professional responsibilities. All other employees are limited to using the following to communicate directly with students who are currently enrolled in the school corporation within the scope of the employee's professional responsibilities:

- Electronic mail (e-mail)
- Video-sharing websites (using district owned equipment)
- Landlines (using district owned equipment)
- Group messaging applications (approved by administration)

Exception for family and social relationships;

1. The circumstances under which employees may use text messaging to communicate with students; and
2. Other matters deemed appropriate by the Superintendent or designee.

Personal Use

Employees shall be held to the same professional standards in their public use of electronic media as they are for any other public conduct. If an employee's use of electronic media violates state or federal law or corporation policy or interferes with the employee's ability to effectively perform his or her job duties, the employee is subject to disciplinary action, up to and including termination of employment.

Relationships with Students

Employees shall not form romantic or other inappropriate social relationships with students. Any sexual relationship between a student and a school employee is always prohibited even if it is consensual.

School Board Members

A school board member has the right to have their own personal social media as a private citizen. If a school board member wishes to have a personal social media page, the board member is responsible for the content on the page and links on the page. The school board member is responsible for maintaining the privacy settings appropriate to the content and posting a disclaimer that the content of the posts by the board member are the personal opinions of the board member and are not representative of the school board.

In addition, users should ...

- Be aware of what they post online. Social media venues, including wikis, blogs, photo and video sharing sites, are very public. Users should not post anything they wouldn't want friends, enemies, parents, teachers, colleges or a future employer to see.
- Follow the school's Code of Conduct when writing online. It is acceptable to disagree with someone else's opinions; however, it should be done in a respectful way. Criticism should be constructive and not hurtful. What is inappropriate in the classroom is inappropriate online.
- Practice online safety. Never give out personal information, including, but not limited to, last names, phone numbers, addresses, birth dates, and pictures. Do not share passwords with anyone besides teachers and parents.
- Link to other websites to support thoughts and ideas when possible. However, users should be sure to read the entire article prior to linking to ensure that all information is appropriate for a school setting.
- Do their own work and not use other people's intellectual property without their permission. It is a violation of copyright law to copy and paste others' thoughts without

giving credit. When paraphrasing another's idea(s), students should be sure to cite your source with the URL. It is good practice to hyperlink to sources.

- Be aware that pictures may be protected under copyright laws. Users must verify they have permission to use the image or that it is under Creative Commons attribution.
- Remember that how you represent yourself online is an extension of yourself. Do not misrepresent yourself by using someone else's identity.
- Make sure that blog and wiki posts are well written. Writers should follow writing conventions including proper grammar, capitalization, and punctuation. Edits of someone else's work should be done in the spirit of improving the writing.
- Notify a teacher or other school staff right away if you run across inappropriate material that makes you feel uncomfortable or is not respectful.
- Remember that students who do not abide by these terms and conditions may lose their opportunity to take part in schoolwork and/or access to future use of online tools.
- Not access social media for personal use from the Corporation network.
- Remember that access social media is permitted for educational use only in accordance with a teacher's approved plan for such use.

Limitation of Liability

BHMSD will not be responsible for damage or harm to personal files, data, or hardware.

Although the Corporation employs filtering and other safety and security mechanisms and attempts to ensure their proper function, it makes no guarantees as to their effectiveness. The Corporation will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Violations of this policy may have disciplinary consequences, including:

- Installation of a restricted iPad profile, or removal of apps;
- Suspension of network, technology, or computer privileges;
- Notification of parents;
- Detention or suspension from school and school-related activities;
- Legal action and/or prosecution.

Confidential Information Communicated or Stored on School Technology

Users of Corporation technology are expected to protect the integrity of data, comply with data-privacy regulations, and protect the personal privacy of other people when using Corporation technology. Users should not access confidential information in the presence of others who do not have authorization to have access to the information and should not leave confidential information visible when a user is away from a screen.

Student/Parent Technology Agreement 2024-2025

Student:

Address:

Parent/Guardian Last Name *

Parent/Guardian First Name *

Parent/Guardian Email Address *

The Bluffton-Harrison Metropolitan School District's Responsible Use Agreement allows students to use technology inside and/or outside of the classroom. School may provide Internet access, desktop computers, mobile devices, video conferencing capabilities, online collaboration capabilities, message boards, email, and more.

I have reviewed and understand the rules and guidelines for the following:

1. District Technology Goals
2. Responsible Use Agreement

Terms of Agreement

The student is responsible at all times for the care and appropriate use of technology. I understand if my child violates the guidelines agreed to, his/her privilege to use technology may be restricted or removed and he/she may be subject to disciplinary action.

I understand that I may be held responsible for reimbursement for loss, theft, damage, or repair of my child's mobile device, which may have occurred at school or at home, or while the mobile device was being transported.

The mobile device remains the property of School. At the end of the school year or upon transfer from the district, parents and students agree to return the mobile device to the school in the same condition it was issued to the students less reasonable wear. Failure to return the mobile device constitutes theft of School's property.

Parent or Guardian Signature *