

Brownsburg Community School Corporation

Acceptable Use Policy

2018 - 2019

INTRODUCTION

The Brownsburg Community School Corporation (BCSC) 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. We are committed to helping students develop 21st century technology and communication skills. To that end, we provide the privilege of access to technologies for student and staff use.

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:

- A. The BCSC network is intended for educational purposes only, and is not a public access service or public forum.
- B. All activity over the network or using District technologies may be monitored and retained.
- C. 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).
- D. Students and staff are expected to follow the same rules for good behavior and respectful conduct online as offline.
- E. Misuse of school resources can result in disciplinary action.
- F. BCSC makes a reasonable effort to ensure students' and staff safety and security online, but will not be held accountable for any harm or damages that result from use of school technologies.
- G. Users of the District network or other technologies are expected to alert IT staff immediately of any concerns for safety or security.

TECHNOLOGIES COVERED

BCSC may provide the privilege of Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more. This Acceptable Use Policy applies to both school-owned technology equipment utilizing the BCSC network, the BCSC 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 BCSC network, the BCSC Internet connection, and/or private networks/Internet connections while on school property. As new technologies emerge, BCSC may 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 technologies provided by the District are intended for education purposes. 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.

WEB ACCESS

BCSC 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. All users must utilize the BCSC internet for web browsing while on campus. Personal mobile hotspots and 'tethering' are not permitted while users are on campus. 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 BCSC Technology Service Ticket Help Desk.

WEB PAGES

The District authorizes the creation of websites by third parties, staff, and students for the purpose of educating, informing, and communicating. Student websites are subject to the requirements of Policy 5722 – Student Publications and Productions. Websites created by students must be prepared under the supervision of a staff person. Any hosted site or service which requires a student login or other credentials must meet FERPA guidelines. If you are unsure whether a site is FERPA-compliant, please submit a Helpdesk ticket. All websites created under this policy are subject to Policy 8330 – Student Records, copyright laws, and other Board policies. Under no circumstances is a website to be created for commercial purposes, political lobbying or personal financial gain of a student or staff person. Staff members shall not require students to connect to the staff person's non-BCSC webpages to complete the work of any class.

EMAIL

BCSC 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. School-sponsored clubs and organizations are required to utilize a BCSC email account. If users are provided with email accounts, the account(s) should be used with care. Users should not send personal information; 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 staff member. 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 2.0/COLLABORATIVE CONTENT

Recognizing the benefits collaboration brings to education, BCSC 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.

MOBILE DEVICES POLICY

BCSC may provide users with mobile computers or other devices to promote learning outside of the classroom. A BCSC or grant-funded mobile device's primary function is for classroom and educational purposes. Users shall abide by the same acceptable use policies when using school devices off the school network as on the school network. Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users shall immediately report any loss, damage, or malfunction to IT 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.

PERSONALLY-OWNED DEVICES POLICY

Students should keep personally-owned devices (including laptops, tablets, smart phones, and cell phones) turned off and put away during school hours - unless in the event of an emergency or as specifically instructed and permitted by a teacher or staff. Personally-owned staff or student mobile devices, including printers, wireless access points, storage devices, physical or virtual servers, and similar equipment, shall not be connected to the school network without express permission from IT staff. In some cases, a separate network may be provided for personally-owned devices. Please remember, this Acceptable Use Policy applies to privately-owned devices accessing the BCSC network, the BCSC Internet connection, and private networks/Internet connections while on school property.

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 the BCSC Technology Department. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

Users may not post or share their username/password information. Copyrighted materials from software or content publishers shall not be posted on webpages without express written consent from the publisher.

The use of personal USB drives is strongly discouraged for staff and is not permitted for students. Users should instead utilize BCSC-provided network storage and OneDrive account.

Students may not use a computer that has been designated as a staff PC without extremely close supervision. Use should be restricted to class presentations. All users are expected to lock their PC's when not in use. Never attempt to use a PC which has been logged in under another user's account.

All files with personal student information shall be stored on local BCSC storage (G Drive, S Drive) and NOT in any cloud or portable storage devices, such as OneDrive, DropBox, Google Drive, etc.

DOWNLOADS

Users should not download or attempt to download or run .exe 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 or 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, 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 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 an adult (teacher or staff if you're at school; parent if you're using the device at home) immediately.

CYBERBULLYING

Cyberbullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking 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, cyberbullying can be a crime. Remember that your activities are monitored and retained.

SOCIAL MEDIA POLICY

The District has a separate Social Media Policy that applies to all staff, and may have implications for students. By signing the Acceptable Use Policy users are acknowledging they have been made aware of the Social Media Policy and agree to abide with the requirements of the Social Media Policy. Violations of the Social Media Policy are in effect violations of the Acceptable Use Policy.

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 if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher or staff member if I see threatening, inappropriate, or harmful contact (images, messages, posts, etc.) 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.

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

EXAMPLES OF UNACCEPTABLE USE

I will not:

- Use school technologies in a way that could be personally or physically harmful.
- Attempt to find inappropriate images or content; intent to seek inappropriate images or content is a violation of this Acceptable Use Policy.
- Create a personal mobile “hot-spot” or utilize a “proxy site” for the purpose of circumventing network safety measures and filtering tools.
- Create, distribute, or deploy multi-user servers or gaming software on or within the BCSC network.
- Engage in cyberbullying, harassment, or disrespectful conduct toward others.
- 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.
- Use school technologies to send spam or chain mail.
- Plagiarize content I find online.
- Post or otherwise disclose personal-identifying information about myself or others.
- Agree to meet someone I meet online in real life.
- Use language online that would be unacceptable in the classroom.
- Use school technologies for illegal activities or to pursue information on such activities.
- Attempt to hack or access sites, servers, or content that isn’t intended for my use.

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

LIMITATION OF LIABILITY

BCSC will not be responsible for damage or harm to persons, files, data, or hardware.

While BCSC employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

BCSC will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

VIOLATIONS OF THIS ACCEPTABLE USE POLICY

Violations of this policy may have disciplinary repercussions, including:

- A. Suspension of network, technology, or computer privileges;
- B. Notification to parents;
- C. Detention or suspension from school and school-related activities;
- D. Employment disciplinary action, up to and including termination of employment;
- E. Legal action and/or prosecution.

This AUP may be periodically revised and updated. As alterations are made, all users will be required to acknowledge and accept the new AUP prior to being permitted access to the BCSC network.

Student and Parent agreement to AUP is part of the Brownsburg Community Corporation Parent Signature Page.

For BCSC Staff only:

I have read and understand this Acceptable Use Policy and agree to abide by it:

(Staff Signature) (Date)

(Staff Printed Name)

P.L. 106-554 (2000), Children's Internet Protection Act
47 U.S.C. 254(h), (1), Communications Act of 1934, as amended (2003)
18 U.S.C. 1460
18 U.S.C. 2246
18 U.S.C. 2256
20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965,
as amended (2003)
20 U.S.C. 6777, 9134 (2003)
76 F.R. 56295, 56303
15 U.S.C. 6501 et seq., Children's Online Privacy Protection Act
34 C.F.R. Part 99, Family Educational Rights and Privacy Act
47 C.F. 54.520, Children's Internet Protection Act