Coe-Brown Student Acceptable Use Policy

Coe-Brown Northwood Academy recognizes that access to technology in school gives students and teachers 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 access to technologies for student and staff use. This Acceptable Use Policy outlines the guidelines and behaviors that students are expected to follow when using school technologies or when using personally-owned devices on the school campus.

- Technology and the network are 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).
- Students are expected to follow the same rules for good behavior and respectful conduct online as offline.
- Misuse of school resources can result in disciplinary action.
- We make a reasonable effort to ensure students' safety and security online, but will not be held accountable for any harm or damages that result from misuse of school technologies.

Users of the network or other technologies are expected to alert any member of administration or faculty immediately of any concern for safety or security.

Technologies Covered

Coe-Brown Northwood Academy may provide internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email and more.

As new technologies emerge, Coe-Brown Northwood Academy will attempt to provide access to them. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed.

Edline

All parents and students are issued an Edline account. You are encouraged to use your Edline login to check grades, conduct, and attendance information. Keep your login and password private; use by anyone other than you creates a security risk for both your own files and the network. If you forget your password or cannot get into your network account, seek assistance from the main office.

Usage Policies

All technologies provided by Coe-Brown Northwood Academy are intended for educational purposes at all times. All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, appropriate, careful and kind; don't try to get around technological protection measures; use good common sense; and ask if you do not know.

Network Access

Coe-Brown Northwood Academy provides its students with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with CIPA regulations and school policies. Web browsing may be monitored and web activity records may be retained indefinitely.

Internet access to visual depictions that are obscene, violent, pornographic or are of a harmful nature to minors are filtered or blocked. Students shall not intentionally access or attempt to access these sites.

Users are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the web. If a site is blocked and a user believes it shouldn't be, the user should follow protocol to alert an IT staff member or submit the site for review.

Always log out of the network so that your files, password, and network access are protected from abuse by others.

Students are ultimately responsible for backing up their data. File syncing and server space on CBNA servers is provided as a convenience only. CBNA is not responsible for any data loss.

Email

Coe-Brown Northwood Academy will provide students with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies.

If students are provided with email accounts, they should be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as allowed by the school 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 2.0 / Collaborative Content

Recognizing that collaboration is essential to education, Coe-Brown Northwood Academy may provide students 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.

School-Issued Netbooks and other devices

Coe-Brown Northwood Academy will provide students with netbook computers. Netbooks are expected to be used in accordance with the policies set forth in this document. Students should use common sense when using and caring for their netbooks. Provided cases should be used for netbook transfer and storage.

Students are responsible to bring a fully charged netbook to school each day. A limited number of replacement recharged batteries will be available in the library. Students should not bring battery chargers to school. Students will need to pay a $3.00 fee for a replacement battery on each occurrence.

Students must not attempt to fix or repair their computer. Students must contact the Technology Director.

The Coe-Brown Northwood Academy is not responsible for supporting home network and internet connectivity.

A loaner netbook will be provided to the student in the case of warranty repairs or accidental damage at the discretion of the Technology Director. A loaner will not be provided if the netbook was damaged by abuse, neglect or malicious intent. A loaner will not be provided if the student fails to bring the netbook to school. Students are responsible for all work issued even when they do not have a netbook. Failure to return a loaner on the specified due date will result in disciplinary action from the library staff.

Parents/guardians will assume any financial responsibility for damages not covered by warranty. Repairs to a student issued netbook made necessary by inappropriate handling or treatment will be billed to the student based upon the severity of the situation. Repair costs start at $50.00 and will range up to the full replacement cost of the unit as determined by the Technology Director.

Students must have their netbooks with them, locked in their school lockers, or in a designated area. Netbooks must not be left unattended. Faculty will pick up and deliver unattended netbooks to the main office.

Netbook Theft or Loss

In the case of a lost or stolen laptop the following procedures must be followed:

• The lost netbook must immediately be reported to the Technology Director and the School's Resource Officer.

• If the netbook is not immediately found and is believed to be lost or stolen, a police report must be filed by the parent or guardian.

• Only after a complete police report has been received will the student be allowed a loaner netbook. The determination of whether the student will be allowed to take the loaner off school grounds will be decided on a case-by-case basis.

• A replacement netbook will be provided only after the missing laptop has been determined to be a total loss.

Mobile Devices Policy

Coe-Brown Northwood Academy may provide users with mobile computers or other devices to promote learning both inside and outside of the classroom. Users should 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 should report any loss, damage, or malfunction to Technology Director immediately. Users may be financially responsible for any damage resulting from negligence or misuse.

Use of school-issued mobile devices, including use of the school network, may be monitored.

Personally-Owned Devices

Students may use personally-owned devices (including laptops, tablets, smartphones, and cell phones) if approved by the teacher, unless such use interferes with the delivery of instruction by a teacher or staff or creates a disturbance in the educational environment. Any misuse of personally-owned devices may result in confiscation and disciplinary action. Therefore, proper netiquette and adherence to the acceptable use policy should always be used. In some cases, a separate network may be provided for personally-owned devices.

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 IT. 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 programs over the school network or onto school resources without express permission from Technology Director. You may be able to download images or videos. For the security of our network, download such files only from reputable sites, and only for educational purposes.

Netiquette

- Users should always use the Internet, network resources, and online sites in a courteous and respectful manner.
- Users should also recognize that among the valuable content online is unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the internet.
- Users should also remember not to post anything online they wouldn't want 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.
- Students shall not deliberately use the computer to annoy or harass others with language, images, innuendoes, or threats. The user shall not deliberately access or create any obscene or objectionable information, language, or images. These violations will be handled in accordance with the CBNA Bullying /Harassment policy as well as computer use policies.

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

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 are at school; parent if you are using a device at home) immediately.

- 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 someone they meet online in real life without parental permission.

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.

Examples of Acceptable Use
I will:

- Use school technologies for school-related activities and research.
- 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 other staff member if I see threatening/bullying, inappropriate, or harmful content (images, messages, posts) online.
- Use school technologies at appropriate times, in approved places, for educational pursuits only.
- Cite sources when using online sites and resources for research; ensure there is no copyright infringement.
- Comply with all license agreements.
- 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 to myself or others.
- Search inappropriate images or content.
- Engage in cyberbullying, harassment, or disrespectful conduct toward others–staff or students.
- Try to find ways to circumvent the school's safety measures and filtering tools.
- Use school technologies to send spam or chain mail.
- Plagiarize content I find online.
- Post personally-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, accounts, 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.