



North Branch Area Schools

Acceptable Use Policy in addition to Board Policy #7540.03

Technology Acceptable Use Policy

North Branch Area Schools encourages and strongly promotes the use of electronic information technologies in educational endeavors. The District provides access to information resources available in a variety of electronic formats, and for the development of information management skills. Students must conduct themselves in a responsible, efficient, ethical, and legal manner. Unauthorized or inappropriate use, including any violation of these guidelines, may result in cancellation of the privilege, disciplinary action consistent with the Student Handbook and Board Policy.

The District's technologies are District property and are intended for use for educational purposes. The District retains the right to access and review all electronic and voice mail communications, computer files, databases and any other electronic transmissions contained in or accessed by District technologies. Student users have no reasonable expectation that any information contained on any District technologies is confidential or private. The District's system is not a public forum and access to the technology is a privilege and not a right.

The District makes Chromebook protection available to families to cover accidental damage and theft of student Chromebooks. The District does not provide protection for other devices, nor is responsible for the loss of data. All District technologies are provided on an *"as is, as available"* basis.

District Definitions:

- Equipment includes, but is not limited to, computers, printers, scanners, networks, video and audio recorders, cameras, photocopiers, phones and other related electronic resources.
- Software includes, but is not limited to, computer software, print and non-print resources.
- Networks include, but are not limited to, all voice and data systems.
- Users include anyone who is accessing or using District equipment, software, and/or networks.

District Responsibility

Students who are currently enrolled in the District may be granted access to North Branch Area Schools' network upon agreement to the terms stated in this policy.

North Branch Area Schools is responsible for the management of the hardware and software that the District uses to allow access to technologies for educational purposes.

The District will designate a system administrator who will manage the system and make the final determination as to what is inappropriate use based on the student Technology Acceptable Use Policy. The system administrator may close an account at any time for infractions or temporarily remove a user account on the network to prevent further unauthorized activity.

The system administrator has the right to view, modify or remove a user's email account. This access shall be used to preserve network integrity or to prevent prohibited activity. The system administrator may review digital history created by students. The system administrator may determine and uncover inappropriate usage while on the network and may also inform other faculty members and the student user in question.

The North Branch Area Schools will implement filtering software intended to block minor's access to materials that are obscene, child pornography, harmful to minors, or that the District determines to be inappropriate for minors. However, the District does not guarantee that school officials will control user's access to such materials, or that users will not have access to such materials while using the District's information technologies. The filtering software operates both within the District and at remote locations.

The District does not take responsibility for resources located or actions taken by the users that do not support the purposes of North Branch Area Schools.

It shall be the responsibility of all members of the District staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act.

What is Google Workspace for Education?

North Branch Area Schools provides staff and students with a Google Workspace for Education account. Google Workspace is a web based suite of programs provided by Google for schools to use. Google Workspace includes such tools as Google Drive, Google Calendar, and Gmail.

All of the Google Workspace services can be accessed from anywhere you have an internet connection (school, home, mobile phone, etc.) This reduces and replaces the need for flash drives and/or external data drives. Since Google Workspace is all online, it is the same everywhere you use it. Google Workspace allows you to easily share documents and files with teachers and other students, so you can turn in assignments electronically and collaborate on projects with classmates.

If you'd like to know more information about the security of data in Google Workspace for Education, please visit <http://www.google.com/edu/trust>.

NBAS Student Google Workspace for Education Account

North Branch Area Schools student accounts are created using the students first initial, last name, and the last two digits of the student graduation year. This is the same as their network username. Passwords will be created and can be reset.

Student Users are Responsible for:

- Coming to school with Chromebook charged - applicable to 5th - 12th grade students
- Using information technologies in the school only for facilitating learning, appropriate personal growth and enhancing educational information exchange consistent with the purposes of the school
- Attending appropriate training sessions in the use and care of hardware, software and networks
- Seeking instruction for the use of any available technology with which they are not familiar
- Adhering to the rules established for the use of hardware, software, labs and networks in the school or through remote access outside of the school
- Immediately reporting any inappropriate content encountered on the network to their supervising teacher or building principal
- Maintaining the privacy of passwords and are prohibited from publishing or discussing passwords. Network accounts are to be used only by the authorized owner of the account for the authorized purpose
- Students may use e-mail, chat, instant messaging, and other forms of two-way electronic communications only for educational purposes and only under the direct supervision of an adult
- Having all electronic media scanned for virus, damage or other contamination which might endanger the integrity of District hardware, software or networks before they are used in District systems
- Material received, created or distributed using technologies
- Maintaining the integrity of the electronic messaging system (voice, e-mail, etc.), deleting files or messages if they have exceeded their established limit, reporting any violations of privacy and making only those contacts which foster learning and enhance educational information exchange. If a user remains in non-compliance, the System Administrator may delete files and messages, freeze the account, and/or close the account.
- Awareness of and adhering to copyright laws and guidelines and trademark laws and applicable licensing agreements in the use of information technologies and in the transmission or copying of text or files, on the Internet or from other resources. Users must also comply with all other applicable laws, both state and federal, with respect to their use of the District's information technologies
- Using caution (*Buyer Beware*) when considering the purchase of goods or services over the Internet. North Branch Area Schools is not liable for any financial obligations made or any personal information provided while using District technologies.
- Financial restitution for unauthorized costs incurred or damages or repair necessitated by inappropriate use or access
- Any damages to or incurred on, their personal equipment. Users accessing North Branch Area Schools' technologies on *personal* equipment must get prior permission from the Director of Technology and do so *at their own risk*.
- Abiding by the rules set forth in this policy, general District rules, and additional rules as may be established by the District. Board of Education policies, staff manuals, departmental procedures, and student handbooks may include such rules.

Student Users are prohibited from:

- Using the technology for a "for-profit" business, for product advertisement or political lobbying
- The malicious use of technology to disrupt the use of technology by others, to harass or discriminate against others and to infiltrate unauthorized computer systems
- Using District technologies to draft, send, or receive inappropriate communications and material including but not limited to, items which are pornographic, obscene, profane, vulgar, harassing, threatening, defamatory, or otherwise prohibited by law
- Participating in hate mail, harassment, discriminatory remarks and other antisocial behaviors on the network
- Vandalizing District or any other information technologies (the District's or any others) Vandalism is defined as any

attempt to harm, destroy, or disrupt or hack the operation of the District's information technologies. Vandalism includes, but is not limited to, the creation or intentional receipt or transmission of computer viruses

- Students may not use the Internet to engage in "hacking" or other unlawful activities.
 1. Students shall not use the Network/Internet to transmit material that is threatening, obscene, disruptive, or sexually explicit or that can be construed as harassment or disparagement of others based upon their race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs. Sending, sharing, viewing, or possessing pictures, text messages, e-mails, or other materials of a sexual nature (i.e. sexting) in electronic or any other form, including the contents of a wireless communication device or other electronic equipment is grounds for discipline. Such actions will be reported to local law enforcement and child services as required by law.
 2. Use of the Network/Internet to engage in cyberbullying is prohibited. "Cyberbullying" is defined as the use of information and communication technologies (such as e-mail, cell phone & text messages, instant messaging (IM), defamatory personal websites and/or blogs, and defamatory online personal polling websites); to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm others." [Bill Belsey (<http://www.cyberbullying.ca>)]

Consequences of Inappropriate Behavior

Access to technology is a privilege and not a right. Any user who does not comply with the Technology Acceptable Use Policy will lose network privileges. Repeated or severe infractions of the policy may result in permanent termination of privileges. Users violating any of the rights and responsibilities may face additional disciplinary action deemed appropriate in keeping with the disciplinary policies and guidelines of the School Handbook and Board Policy.

Challenges

Challenges regarding District technologies policies shall be made in writing following the Board adopted appeal process, and shall state the reasons for the challenge.