NORTHBRIDGE PUBLIC SCHOOLS EMPOWERED USE POLICY

January 2023

I. Introduction

The Northbridge Public Schools offer network access to its students, staff, and others such as citizens, volunteers, and elected officials ("the Users"). As digital technologies emerge it is essential that all users of the Northbridge Public Schools Computer Networks ("The Networks") have an understanding of the available technology and its appropriate use. The intent of this policy is to establish a set of guidelines that all users of any private (NPS) or public (Cell Carrier) networks while in the district will understand and practice while accessing them.

II. Purpose

This policy outlines the ideal characteristics of users in a digital world through the norms of appropriate, responsible behavior with regard to technology use called *Digital Citizenship*. There are three guiding principles within the framework of digital citizenship:

- **Safe** - Protecting others and yourself from danger, risk, or injury.
- **Savvy** - Maturing into educated digital citizens by developing wisdom, practical knowledge, and the understanding to make good judgments.
- **Social** - Respecting yourself as a digital citizen through creating cooperative and interdependent relationships and understanding of others (Ribble).

When accessing any private (NPS) or public (Cell Carrier) networks, users must take full responsibility for their own actions. While the network's possibilities are tremendous, it also has potential for abuse. The Northbridge Public Schools shall not be liable for the actions of anyone accessing those networks. Users assume full responsibility for any costs, liabilities, or damages arising from the way the user chooses to access those networks. Use of those networks constitutes their agreement to abide by this policy as set forth below, or as modified in the future.

NORTHBRIDGE PUBLIC SCHOOLS EMPOWERED USE POLICY

January 2023

III. The Nine Elements of Digital Citizenship

Within the framework of the 3 guiding principles of Safe, Savvy, and Social, the specific nine elements guide all technology use by users of any private (NPS) or public (Cell Carrier) networks while in the district. Integrated within the curriculum throughout all grade levels, students will learn and develop skills in each of these elements.

Element 1 - Digital Access

Many students and families are fortunate to have near constant access to technology. The district, as a result of infrastructure development and technology purchases, is fortunate to have a substantial amount of technology available to staff and students throughout the school day. However, there remains a digital divide to technology access due to a variety of factors (socio-economic status, disabilities, etc.) Students and staff will make use of digital technology when and where appropriate and take necessary steps to ensure that regardless of technology availability, all students and families will have access to curriculum and information, whether online or offline.

Examples of Inappropriate Digital Access	Examples of Appropriate Digital Access
Schools ignore or overlook the digital needs of disenfranchised groups (e.g., not viewed as important	District administrators work toward providing technology opportunities for all students within their schools
Teachers fail to accommodate students who do not have access to technology	Technology leaders provide technology to students for use in school and out, such as a one-to-one laptop program ((Ribble 51)

NORTHBRIDGE PUBLIC SCHOOLS EMPOWERED USE POLICY

January 2023

Element 2 - Digital Commerce

With near ubiquitous access to technology, students are regularly exposed to the commercial nature of apps and the internet. At an early age, children encounter online games that offer upgrades or special powers as well as videos and ads for products that are easily purchased online. In coordination with families, students will be aware of the financial and security implications of making online purchases in addition to the possibility of identity theft and credit issues.

Examples of Inappropriate Digital Commerce	Examples of Appropriate Digital Commerce
Students purchase goods online without knowing how to protect their identity (leaving them open to identity theft).	Students become informed consumers so they can safely purchase items online.
Students fail to realize that poor online purchasing practices lead to poor credit ratings.	Students spend the time to research what they want to purchase, then take the time to identify safe, secure, and reputable sites with the best prices. (Ribble 55)

Element 3 - Digital Communication

“Cell phones, social networking, and texting have changed the way people communicate. These forms of communication have created a new social structure governing how, when, and with whom people interact”. (Ribble 58) With the ease of digital communication, students will understand positive best practices in appropriate email use, texting issues, cell phone etiquette, and choosing technology communication models.

Examples of Inappropriate Digital Communication	Examples of Appropriate Digital Communication
Students text or use social media during class time.	Students do not use digital communication devices at any point during school hours and teachers only do so when on their break.
Students use text messaging to cheat on tests.	Teachers use blogs and other communication sites to inform parents of classroom activities. (Ribble 61)
Sharing of graphically inappropriate pictures with others.	Students use school-appropriate images to enhance presentations, reports, and other assignments.
Using anonymous or other social media sites to bully or berate others.	Students uplift each other with positive conversations online and in person.

Element 4 - Digital Literacy

Students of the 21st Century are often referred to as “digital natives”. Having been born into a society where technology is virtually everywhere, it is easy to make this assumption. However, just because a student has had access to technology their whole lives, does not mean they know how to use it effectively. Learning the digital basics (web browsing, searching the web, email, office tools), evaluating online resources (discerning the accuracy and trustworthiness of content on websites), and exploring and developing online learning modes (Ribble 65) are all essential components of developing digital literacy.

Examples of Inappropriate Digital Literacy	Examples of Appropriate Digital Access
Students choose alternative educational opportunities because their school or district does not offer online classes or a distance education program.	Students take online courses (or mixed delivery--part face-to-face, part online) that are designed to keep them interested in the material.
Teachers do not provide resources and materials that students can get from digital sources (e.g., blogs, websites, podcasts).	Teachers use digital technologies in new and innovative ways, such as creating content for the web that can be accessed by students away from the classroom. (Ribble 65)

Element 5 - Digital Etiquette

With the ubiquitous access to technology, all users of technology are looked to as role models of appropriate use. If students see others using technology in one way (positive or negative), they will engage in that same behavior. Students will use technology in ways that have a positive effect on others, when it is contextually appropriate, and maintain respect for others.

Examples of Inappropriate Digital Etiquette	Examples of Appropriate Digital Etiquette
Students use cell phones to text in situations where they should be listening/focusing on others.	Students work with their teachers to understand what information can be shared from their devices, and when it is appropriate to do so.
Students communicate on a social networking site without knowing the	When communicating with a messaging app, users learn the rules of the group

rules (who can see posts or personal information) or responsibilities (letting others know when threats or negative comments have been made about them).	before becoming involved in the conversation. (Ribble 70)

Element 6 - Digital Law

On the internet, copyrighted, inappropriate, and sometimes illegal material and information can be found. It is essential that all users understand the legal implications of accessing file-sharing websites, using pirated software, hacking or bypassing systems and networks, and assuming or stealing someone's identity.

Examples of Illegal Technology Use	Examples of Legal Technology Use
Students using copyrighted material such as photographs, artwork, music or movies without permission.	Students understand what can be downloaded without charge and what is considered copyrighted material and should be paid for. They are aware of free alternatives such as Creative Commons licensed work.
Students scripting (using computer code), using VPNs, extensions, or other means to bypass firewalls or other network protection.	Students understand that the restrictions put in place by the school district and their parents are for their safety.
Students sharing inappropriate material with others.	Students inform an adult when they learn of someone sharing graphically inappropriate material. (Ribble 75)

NORTHBRIDGE PUBLIC SCHOOLS EMPOWERED USE POLICY

January 2023

Element 7 - Digital Rights and Responsibilities

All users need to understand the difference between what they are capable of doing with access to available networks and what should be done for the overall good of the group of teachers and learners. Following accepted norms, using online material ethically (including citing sources and asking for permission), and identifying cyberbullies, threats, and other inappropriate behavior are expectations of all users.

Examples of Inappropriate Digital Rights and Responsibilities	Examples of Appropriate Digital Access
Users use material from the internet without properly citing the source.	Users cite websites or other digital media sources when using information for class projects or presenting material.
Users violate their school's Empowered Use Policy because they view it as unfair.	Users are informed of their rights when using digital technologies, while also being aware of their responsibilities. (Ribble 79)

Element 8 - Digital Health and Wellness

In addition to social and emotional well-being regarding technology use, all users should be aware of how they can be physically affected by technology. This includes using proper ergonomics and avoiding repetitive motion injuries as well as developing addictive behaviors towards the internet and video games.

Examples of Inappropriate Digital Health and Wellness	Examples of Appropriate Digital Health and Wellness

Administrators and teachers ignore the possible harmful physical effects of technology on students.	Technology leaders learn how to promote health and wellness with technology.
Teachers do not model proper ergonomics when using technology.	Teachers model digital safety in their classrooms and expect their students to do the same. (Ribble 85)

Element 9 - Digital Security

Protecting digital equipment (including desktop computers, tablets, chromebooks, personal devices, etc.) is a personal responsibility that has implications for all users on the networks. The importance of creating and maintaining secure passwords, updating software to prevent viral threats, and understanding how to identify potential hacking, phishing, and spoofing threats are essential for all users. In addition to being educated about these, it is important to protect technology through use of spyware/adware blockers, data backup, understanding the role of the firewall, and using effective passwords and passcodes.

Examples of Inappropriate Digital Security	Examples of Appropriate Digital Security
District fails to maintain current software updates or patches that protect their computers from viruses and exploitation. Users fail to report notifications of possible virus detection or updates.	Users take the time to make sure their virus protection and firewalls are properly updated and configured to protect personal information.
Users fail to protect their identity when using email, social networking, or text	Teachers and parents talk to students about the dangers of providing

messaging.	information to anyone over the internet.
Students use weak or non-existent passwords. (Check yours here: https://howsecureismypassword.net)	All devices are secured with some kind of lock, passcode, combination, or fingerprint or facial recognition sensor. (Ribble 89)

IV. Responsibilities of the District

The primary purpose of the ("the Network") is to support the educational objectives of the Northbridge Public Schools and Northbridge's educational community in general. The use of any private (NPS) or public (Cell Carrier) networks while in the district provides opportunities for research, curriculum support, and career development. The network is not a public forum (although its contents may be disclosed as a public record), and the Northbridge Public School system reserves the right to place reasonable limits on materials posted or accessed through these networks. The Northbridge Public School System will take reasonable precautions to filter out inappropriate materials; however, it is impossible to monitor all content.

This policy seeks to educate staff about online content monitoring and to ensure student personal information is not disclosed; as required under the Children's Internet Protection Act (Federal Communications Commission) and the Family Educational Rights and Privacy Act (US Department of Education). Staff are expected to monitor student internet use in such a manner to prevent access by minors to inappropriate content on the internet, including attempts to access inappropriate materials and circumvent system security; and provide instruction to students on interacting with other individuals on social networking websites and in chat rooms, and responses to cyberbullying.

NORTHBRIDGE PUBLIC SCHOOLS EMPOWERED USE POLICY

January 2023

V. Network Usage Guidelines

Use of any public or private networks while in the district must be consistent with its purpose as stated in Section IV. This policy outlines acceptable use of those networks. However, it does not attempt to articulate all required or proscribed behaviors by users of the network. Users are expected to conform to the purpose, spirit, and examples set forth in this policy, as well as the standards of Digital Citizenship set forth by this document as well as the International Society for Technology Education (ISTE), and the Massachusetts Digital Literacy and Computer Science Standards, and to abide by the standards and rules of acceptable use (Appendix A).

Privacy

Users should not have an expectation of privacy or confidentiality in the content of electronic communications or other computer files sent or received and/or stored on any private or public network while in the district. Users should be aware that the data they create, receive, or send on the private network is the property of the Northbridge Public School system, and that the data may be recovered and reviewed, even after it has been deleted. The Northbridge Public School system captures and archives all Email, including attachments, sent and received through the district's mail servers and also reserves the right to monitor use of the private network and to examine all data stored on district servers or other systems maintained by third parties under contract with the district.

Any Emails or other communication or data may be a public record and thus possibly subject to public disclosure. All communications, including text and images, regardless of content or purpose, are public, not private and may be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. Network administrators or their designees may review communications to maintain integrity system-wide and to ensure users are accessing the system in a responsible manner. All

private network activities are logged. These logs may be disclosed to law enforcement or other third parties.

Violations

The district reserves the right to deny, revoke or suspend, without prior notification, specific user privileges and/or to take other disciplinary action, up to and including suspension or dismissal, for violation of this policy. The system will advise appropriate law enforcement agencies of illegal activities conducted through the private network. The Northbridge Public School system also will cooperate fully with local, state, and/or federal officials in any investigation related to any illegal activities conducted through the network. Any known breach of this policy should be immediately reported to the Director of Technology.

Departure

Upon departure of the district, users will no longer have access to the Northbridge Public Schools private network nor communication (Email) platform. User accounts are suspended and archived as a matter of public record. Access to former accounts or material contained in accounts is prohibited without written consent of the Superintendent of Schools.

Acceptance

All users of the networks should acknowledge the understanding of and compliance with this policy on an annual basis.

NORTHBRIDGE PUBLIC SCHOOLS EMPOWERED USE POLICY

January 2023

Appendix A - Network Usage Guidelines

This list of guidelines is intended to serve as an outline of the general parameters and expectations of any private (NPS) or public (Cell Carrier) networks while in the district. It is not intended to be an exhaustive list of all potential infractions and situations.

1. It is the policy of Northbridge Public Schools to maintain a school environment free of harassment based on race, color, religion, national origin, age, gender, gender identity, sexual orientation, disability, or any other characteristic protected by law. Users shall observe this policy in the use of the network and employ digital etiquette by using appropriate, non-abusive language, refrain from making defamatory remarks or slurs of any kind, bullying, and from the use of obscene or profane language.
2. Network IDs and passwords are provided for each user's personal use only. Passwords should be secured and not shared with anyone. Users must not use another person's password. If you suspect that someone has discovered your password, please communicate with a technology department staff member or a building administrator to have it changed immediately.
3. Any use for, or in support of, illegal purposes or activities is prohibited. This includes, but is not limited to, gaining unauthorized access to other systems, arranging for the sale or purchase of drugs or alcohol, information about dangerous materials or devices such as weapons, threatening others, transferring obscene material, or attempting to do any of the above.
4. Any use for commercial purposes is prohibited. Users may not create web pages to advertise or sell products or services and may not offer, provide, or purchase products or services through the network.
5. Any use for fundraising for any non-school sponsored purpose, whether for charity or otherwise, is prohibited.
6. Any use for political purposes is prohibited except for using the networks to communicate with elected officials. (For example, lobbying for a political

cause using these networks would be inappropriate while inviting a political figure to class as a guest speaker would be appropriate.)

7. Downloading, using, or copying software in violation of a license agreement or copyright, or otherwise infringing on intellectual property rights is prohibited.
8. Users should assume that most materials available on the Internet are protected by copyright. Unauthorized use of copyrighted materials is prohibited. Additionally, any material obtained from the Internet and included in one's own work must be properly cited regardless of copyright status.
9. Users shall not access, upload, download, transmit, or distribute material that is pornographic, obscene, sexually explicit, threatening, discriminatory, intimidating, abusive, harassing, or would otherwise be deemed offensive by a reasonable person.
10. Users shall neither download nor install any commercial software, shareware or freeware onto network drives or disks without prior permission of the Director of Technology. Appropriate educational apps and browser extensions and add-ons may be downloaded to your iPad or Chromebook without prior permission.
11. Staff must obtain the permission of their supervisor or supervisor's designee prior to creating, publishing, or using any district web pages, social media pages or any other digital content which is school-related, or which could be reasonably understood to be school-related. This includes any content which identifies the school or affiliated club, team, or organization by name in the account name or which uses the school's name or image. When creating accounts, staff must use an official Northbridge Schools Email address and confirm the proper use of privacy settings with the approving supervisor or supervisor's designee. No social media account covered by this policy shall permit comments by the public unless otherwise approved by a supervisor or supervisor's designee.

12. Staff may be required to provide their supervisor or supervisor's designee with the username and password to district social media accounts, if such accounts are authorized. However, staff may not provide the username and password to district accounts to any unauthorized individual, including students and volunteers.
13. Any student-related content, including pictures, is subject to the same restrictions governing the Web Page Protocol and a parent's decision to opt their student out of certain publications. Each school office maintains a list of students whose parents have opted-out of publication. It is the staff member's responsibility to check that list before posting such information.
14. Social media accounts should be used exclusively for district and classroom-related work and communication, with prior authorization from building or district administration, and should be set up with an nps.org email account. Staff members may not use district accounts for personal use.
15. Staff shall not access social media networking sites on school-owned devices unless such access is for an educational activity which has been pre-approved by a supervisor or supervisor's designee. This prohibition extends to using chat rooms, message boards, messaging in social media applications, and includes posting on social networking sites.
16. Users shall be aware of their use of social media; as others may conduct their own search of you. Such searches may result in discovery of personal postings and/or your comments made about work, fellow staff/users, and/or students. Given such possible searches and your status as a school district employee, staff are held to a higher standard of conduct that reflects on your reputation and/or that of the school district. Staff shall refrain from "friending" or creating other electronic relationships with students.
17. Staff shall refrain from sharing personally-identifiable information such as home addresses and telephone numbers.

18. Staff shall not connect any device not owned and managed by the school district to the network, apart from use of public wi-fi network, unless prior authorization is given by building or district administration.
19. Users shall not access, receive, upload, download, transmit, or distribute information promoting the use of dangerous instruments such as bombs or other explosive devices, firearms, or other weaponry.
20. Users must not attempt to gain unauthorized access to any file servers or data in the Northbridge Public Schools system, outside file servers or data, or go beyond the user's authorized access. This includes logging in through another person's account and/or accessing another person's files. Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users.
21. Not all material accessible through the Internet is of educational value. Users are expected to refrain from seeking, accessing, uploading, downloading, transmitting, or distributing material that is not relevant to their work. Users are to access the district network only for purposes related to the schools and the performance of their jobs. Incidental personal use of school information technology is permitted as long as such use is not excessive, wasteful, and/or otherwise does not interfere with the employee's job duties and performance and is in accordance with the policies set forth in this policy. Incidental personal use is defined as use by an individual employee for occasional personal communications. Personal means of communication should not be used to conduct district-related business.
22. Use appropriate judgment and caution in communications concerning students and ensure that personally identifiable information remains confidential. In order to limit the possibility of the disclosure of student records, student information shall be stored only on systems and devices approved by the district. Student information should not be stored in an unsecured manner such as CDs, DVDs, USB drives, other portable media, or on personal devices. Teachers shall take reasonable steps to ensure privacy

and security of student information. Examples include locking their computer when they leave their classroom, ensuring that private student information is not visible when sharing their screen via video conferencing or classroom projector, and selecting a secure password.

Appendix B - Bibliography

Federal Communications Commission. “Children's Internet Protection Act (CIPA).” *Children's Internet Protection Act (CIPA)*, Federal Communications Commission, 2011, https://www.fcc.gov/consumers/guides/childrens-internet-protection-act. Accessed 22 March 2021.

Massachusetts Department of Elementary and Secondary Education. “2016 Digital Literacy and Computer Science Framework.” *2016 Digital Literacy and Computer Science Framework*, 2016, https://www.doe.mass.edu/frameworks/dlcs.docx. Accessed 22 March 2021.

Ribble, Mike. *Digital Citizenship in Schools: Nine Elements All Students Should Know*. International Society for Technology in Education, 2015.

Ribble, Mike. “Nine Elements.” *Nine Themes of Digital Citizenship*, https://www.digitalcitizenship.net/nine-elements.html. Accessed 17 March 2021.

US Department of Education. “Family Educational Rights and Privacy Act (FERPA).” *Family Educational Rights and Privacy Act (FERPA)*, 2020,

https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html. Accessed 22 March 2021.