Northshore School District

ADMINISTRATIVE PROCEDURE

No. 2022 P

INSTRUCTION

A. PURPOSE

The purpose of the Northshore School District Responsible Use Procedure is to provide rules, guidelines, personal safety recommendations and the code of conduct for the use of technology, the district network and other connected networks including the Internet.

This Responsible Use Procedure (RUP) applies to staff, students and guests who utilize:

- District-owned technology on the NSD network, on non-school networks and offline
- Non-District technology, including privately owned technology that is connected to the NSD network or using non-district networks while on school property

B. DEFINITIONS

Technology

Technology shall be defined as any electronic device that can use a network connection, process information, display information or store information for long-term retrieval and the software and services that are used by these devices. This includes:

- All Internet services and shared network resources
- Desktop, mobile computers, tablets, phones and other handheld devices
- Videoconferencing, monitors, projection systems and telephones
- Online collaboration services, message boards, email and other messaging services
- Copiers, printers, peripheral equipment and external file storage devices
- Social media, web-based or Internet tools such as blogs, wikis, social networks, podcasts, or other Internet tools
- Additional technologies as developed

Network

The District network includes wired and wireless computers and peripheral equipment, files and storage, e-mail and Internet content (blogs, web sites, web mail, groups, wikis, etc.). The District reserves the right to prioritize the use of, and access to, the network. All use of the network must be consistent with efforts to enhance learning, support education and research consistent with the mission of the District and to provide support for district operations.

Responsible Use

Northshore provides access to technologies for all users (staff, students, and guests in some cases). Access to technology is a privilege, not a right, and as such, all users must seriously consider the responsibilities associated with the opportunity to use technology devoted to activities that support teaching and learning. The norms of behavior with regard to responsible use of technology are defined as Digital Citizenship. It is the responsibility of both NSD staff and parents to help prepare students to be members and citizens of a digital society.

A digital citizen is one who:

1. Understands human, cultural and societal issues related to technology and practices legal and ethical behavior.
2. Advocates and practices safe, legal and responsible use of information and technology.
3. Exhibits a positive attitude toward using technology that supports collaboration, learning and productivity.
4. Demonstrates personal responsibility for lifelong learning.
5. Exhibits leadership for digital citizenship.

It is assumed that parents grant their child the right to access the network and have a desire to have their child use the Internet as an educational resource. Parents who do not want their child(ren) to have access and use the Internet must sign and return the opt out form that is made available to families annually.

Annually, students will receive grade level appropriate instruction on digital citizenship and Internet safety educating them about appropriate online behavior, using personal portable devices at school, interacting with other individuals on social networking websites, cyber-bullying awareness and response, and other relevant topics.

Annually, all staff must sign a Responsible Use and Internet Safety Agreement or take an online Responsible Use and Internet Safety course prior to using the network.

COPPA and Internet Tools Terms and Conditions

The Children's Online Privacy Protection Act (COPPA) is a federal law, enacted in April 2000, related to the online collection of personal information from students under age 13. COPPA makes it clear to website owners what they must include in their privacy policy, when they must seek consent from parents for a child under 13 to use their services, and what the website owner's responsibilities are to protect the online privacy and safety of children. These rules apply regardless of whether the website is fee-based or not. COPPA does not preclude schools from acting as intermediaries between operators and parents in the notice and consent process, or from serving as the parent's agent in the process of collecting personal information online from students in the school context when parents have provided permission for student Internet use.

Northshore's use and sharing of student data is solely for education purposes. District staff must maintain the confidentiality of student data in accordance with the Family Educational Rights and Privacy Act (FERPA).

Northshore uses a variety of software systems in the classroom, including some that are hosted outside the District's facilities in "the Cloud." When used appropriately and thoughtfully, these tools can help create a rich, flexible and engaging learning environment for Northshore students. Additionally, an important part of students becoming good digital citizens is having opportunities to access materials in the Cloud and/or on the Internet in a responsible and effective manner.

Northshore supports COPPA and insists that websites the District uses adhere to this law. It is important that all Northshore staff members who work with children be aware of and follow COPPA and other state and federal regulations related to student Internet access and related data use. Staff using web-based tools shall be aware of the Terms of Use and Privacy Policies for those systems. Staff, who want to use "outside" resources with students, shall obtain approval prior to use from the Technology Department. Depending on the nature of the resources and how they will be used with students, it may be necessary to obtain approval from groups such as the Curriculum Materials Adoption Committee (CMAC).

C. GUIDELINES

Responsible use by students, staff and guests shall include the following:

1. Creation of files, digital projects, videos, web pages and podcasts using network resources shall be in support of educational activities;
2. When participating in blogs, wikis, bulletin boards, social networking sites and groups, and the creation of content for podcasts, e-mail and web pages that support educational research, users will create online names that are appropriate and use appropriate language/content in all online posts;
3. Student and Staff use of the network for incidental personal use shall be in accordance with all District policies and procedures. Such incidental work, while not prohibited, will not be provided any additional staffing resources to support or enable;
4. Connection of personal electronic devices (wired or wireless) including portable devices with network capabilities to the District network using NSD credentials. Students will only use personal electronic devices on the District's network at the discretion and approval of their teacher, school building staff and/or administration. Connection of any personal electronic device to the District network by any person is subject to all guidelines in this document;
5. Users will help maintain a safe computing environment by notifying appropriate campus or district officials of inappropriate behavior, vandalism, vulnerabilities, risks and breaches of NSD policy involving technology. If the user is uncertain whether an activity is permitted or appropriate, he/she will ask a teacher/administrator before engaging in that activity.

Network Security and Privacy

Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account for authorized district purposes. Students and staff are responsible for all activity on their account, must not share their account password, must not use the account of other users, and must exercise responsible password management.

Internet Safety

Personal Information and Inappropriate Content:

1. Students and staff should not reveal personal information, including a home address and phone number on websites, blogs, podcasts, videos, social networking sites, wikis, e-mail or as content on any other electronic medium;
2. Students and staff should not reveal personal information about another individual on any electronic medium without first obtaining permission;
3. No student pictures or names can be published on any public class, school or district website unless the appropriate permission has been obtained according to District policy; and
4. If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

Use of Social Media and Web-based Tools

Online communication is critical to students' learning 21st-century-skills. Social media, web-based or Internet tools such as blogs, wikis, social networks, podcasts, email or other Internet tools offer an authentic, real-world vehicle for student expression. Examples of social media include, but are not limited to Facebook, Twitter, YouTube, Google+, Instagram, LinkedIn and Flickr. The District's primary responsibility to students is their safety. The District holds staff and students, using these tools to the same responsible use, terms of agreement, standards and expectations and must follow all established Internet safety guidelines. When these tools are used by staff or students with District resources, while on district property or while acting as a representative of the District, the District reserves the right to monitor appropriate behavior and adherence to instructional guidelines. Anything deemed to be inappropriate will be subject to deletion. The District may also take other disciplinary actions as appropriate.

The District will provide all secondary students and many elementary grades with free email service for educational purposes only. These students will be offered email accounts managed by the District using an Internet-based service. These accounts are offered to students to provide consistent and reliable communication with their respective teachers and staff members. Use of these email accounts is subject to the same conditions and restrictions applicable to use of the District's network. Any references to email or electronic resources in this RUP shall incorporate Google Apps for Education email accounts.

The District maintains the right to withdraw account access should there be reason to believe that the account has been misused or that the individual has violated the District's policies or the responsible use guidelines. Violation of district policy or these guidelines by staff, students and/or guests may result in disciplinary action as well as revocation of network and computer access privileges.

Social Media for Personal Use by Staff

Communication with Students:

In order to maintain a professional and appropriate relationship with students, district employees should not communicate with individual students who are currently enrolled in district schools on personal social media sites. Additionally, district employees should not communicate with students via social media tools in a manner that is not readily visible and accessible to the students' parents/guardians and the employee's supervisor. This provision is subject to the following exceptions: (a) staff communication with their own family members and (b) if an emergency situation requires such communication, in which case the District employee should notify his/her supervisor of the contact as soon as possible.

Guidance Regarding Personal Social Media Sites

District employees should exercise caution and common sense when using personal social media sites:

1. Employees are prohibited from inappropriate online socializing with students or from engaging in any conduct on social networking Web sites that violates the law, district policies, or other generally recognized professional standards. Employees whose conduct violates this policy may face discipline or termination, consistent with the District's policies, responsible use agreement and collective bargaining agreements, as applicable;
2. District employees are encouraged to use appropriate privacy settings to control access to their personal social media sites although there are limitations to privacy settings. Private communication published on the Internet can easily become public; social media sites can change their current default privacy settings and other functions. As a result, employees have an individualized responsibility to understand the rules of the social media site being utilized;
3. District employees should not "tag" photos of other district employees, district volunteers, district contractors or district vendors without the prior permission of the individuals being tagged;
4. Personal social media use, including off-hours use, has the potential to result in disruption at school and/or the workplace, and can be in violation of district policies and federal and/or state law;
5. The posting or disclosure of personally identifiable student information or confidential information via personal social media sites, in violation of these guidelines is prohibited; and
6. District employees should not use the District's logo in any postings or post district material on any personal social media sites without the written permission of a district administrator.

Copyright and Ownership of Work
Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of materials for educational purposes are permitted when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately (School Board Policy 2025 and 2025P Copyright).

Work created by employees as part of their employment is considered property of the District under the terms of "work made for hire." The District owns any and all rights to such work including any and all derivative works, unless there is a written agreement to the contrary.

All work completed by students as part of the regular instructional program is owned by the student as soon as it is created, unless such work is created while the student is acting as an employee of the school system or unless such work has been paid for under a written agreement with the school system. If under such agreement with the District, the work will be considered the property of the District. Staff members shall obtain a student's permission prior to distributing his/her work to parties outside the school.

D. UNACCEPTABLE USE AND PREVENTATIVE MEASURES
The guidelines for responsible use are in place to protect users and systems from harm. Unacceptable use is prevented through the implementation of filtering and monitoring systems and training on topics such as digital citizenship and responsible use of technology. When these guidelines are not followed and unacceptable use occurs, the District shall impose disciplinary action.

Examples of unacceptable use:
1. Use for personal gain, commercial solicitation or compensation of any kind;
2. Actions that result in unapproved liability or cost incurred by the District;
3. Downloading, installing and use of games, audio files, video files or other applications for anything other than in the support of educational research;
4. Support or opposition for ballot measures, candidates and any other political activity;
5. Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software and monitoring tools or any other activities that would damage, hinder or alter the use of District technology without permission;
6. Unauthorized access to other district computers, networks and information systems or unauthorized use of district-managed accounts on other systems;
7. Cyber bullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;
8. Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
9. Accessing, uploading, downloading, storage and distribution of obscene, offensive, pornographic or sexually explicit material;

10. Connecting unauthorized devices to the District network. Any such device will be confiscated and additional disciplinary action may be taken;
11. Publishing personal details for any user; making available personal schedules available for public viewing;
12. Making audio or video recordings of any user without their prior permission; and
13. Posing as someone else when online.

Filtering and Monitoring

Filtering software is used to block and/or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Filtering software is not 100% effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a complete solution. Every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites.

The District will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is appropriate and effective training followed by deliberate and consistent monitoring of student access to district computers. Staff members who supervise students, control electronic equipment or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of the District. Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.

Any attempts to defeat or bypass the District's Internet filter or conceal Internet activity are prohibited. This includes proxies, https, special ports, modifications to district browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content. E-mail inconsistent with the educational mission of the District will be considered Spam and blocked from entering district e-mail boxes.

Expectation of Privacy

The District provides the network system, e-mail and Internet access as tools for education in support of the District's mission. The District reserves the right to monitor, inspect, copy, review and store, without prior notice, information about the content and usage of:

1. The network;
2. User files and disk space utilization;
3. User applications and bandwidth utilization;
4. User document files and folders;
5. E-mail and other electronic communications;
6. Internet access; and
7. Any and all information transmitted or received in connection with Network and email use.

Users of the District's network should not have any expectation of privacy when using the District's network. The District reserves the right to disclose any electronic messages to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of the State of Washington.

Disciplinary Action

Use of the computer network and Internet is a privilege, not a right. A user who violates this agreement shall, at a minimum, have his or her access to the network temporarily limited or terminated. The District may also take other disciplinary actions as appropriate.

All users of the District's electronic resources are required to comply with the District's policy and procedures (and agree to abide by the provisions set forth in the District's user agreement). Violation of any of the conditions of use explained in the District's online network user agreement training, Internet safety training, student handbook, Electronic Resources Policy and/or in this RUP would be cause for disciplinary action, including revocation of network and computer access privileges.

Issued: 1/22/96
Revised: 5/23/02, 5/5/06, 10/8/07, 9/15/14