

## **Northshore School District**

# **ADMINISTRATIVE PROCEDURE**

**No. 2022P-2 (or 2022P-Staff)**

**Page 1 of 9**

### **INSTRUCTION**

#### **Responsible Use Procedure - Staff**

##### **Purpose**

The purpose of the Northshore School District Responsible Use Procedure is to provide rules, guidelines, personal safety recommendations and expectations for the use of technology and district network resources, including internet access.

##### **Digital Citizenship**

Northshore provides access to various technologies for all users (staff, students, and guests). All users must seriously consider the responsibilities associated with the opportunity to use technology devoted to activities that support teaching and learning and operational tasks that serve the district's mission. The rules and norms of behavior with regard to responsible use of technology are defined as Digital Citizenship. NSD staff are expected to practice and model for students the behaviors of a member of a global digital community.

Digital Citizenship requires that staff will inspire students to positively contribute to and responsibly participate in the digital world. Our staff will:

- Create experiences for learners to make positive, socially responsible contributions and exhibit empathetic behavior online that build relationships and community.
- Establish a learning culture that promotes curiosity and critical examination of online resources and fosters digital literacy and media fluency.
- Mentor students in safe, legal, and ethical practices with digital tools and the protection of intellectual rights and property.
- Model and promote management of personal data and digital identity and protect student data privacy.
- Take an active role in supporting students in their efforts to meet the tenets of Student 2022P.

To ensure that all staff have the skills and knowledge required to meet these expectations, annual training will be provided on elements of this procedure, including cybersecurity. Staff will be required to acknowledge the expectations set forth in this document by signing an agreement annually and participating in any prescribed training related to use of technology and network resources.

**Responsible use by staff and guests shall include, but not be limited to, the following:**

- Supporting and encouraging equitable and appropriate opportunities for students to use technology to support the strategic goals of the district;
- Creation of files, digital content, videos, and other materials using network resources which are in support of educational activities;
- Communication with students, staff, and families using only district-provided accounts and services such as email, collaboration platforms, and learning management systems;
- Use of the network for limited incidental personal use in accordance with all district policies and procedures. Such limited incidental work, while not prohibited, will not be provided any additional staffing resources to support or enable;
- Connection of personal devices to the district's public network. Connection of any personal device to the district network by any person is subject to all guidelines in this document, including web filtering;
- Maintaining a safe computing environment by notifying appropriate campus or district officials of inappropriate behavior, vandalism, vulnerabilities, or damage to district provided technology;
- Prompt reporting of any suspicious cyber activity, including, but not limited to, phishing, money or gift card scams, false tech support requests, and other email-driven illegal activities.

**Use of Artificial Intelligence**

Artificial Intelligence (AI) is defined as a set of technologies that simulate human intelligence processes by machines, especially computer systems. This includes, but is not limited to, machine learning, natural language processing, speech recognition, and image or video creation. AI's potential to enhance learning, personalize educational experiences, and streamline administrative tasks is considerable. A human-centered AI learning environment is one that prioritizes the needs, abilities, and experiences of students, educators, and administrators. Student and staff use of generative Artificial Intelligence technologies should be used to support and extend student learning and workplace productivity. Student and staff use of AI will be in accordance with the expectations outlined in Policy 2022, this document (2022P), and any published guidance for the use of AI in Northshore.

**Staff will abide by the following guidelines in their use of AI:**

- Decisions made with the assistance of AI should be subject to a human-centered approach, especially those affecting student assessments, placements, or significant outcomes.
- AI should be integrated into curriculum and teaching practices in a way that supports and enhances learning objectives, critical thinking, and digital literacy.
- AI shall supplement, not replace, interactions between students and educators in a way that enhances the learning experience for students.
- Staff and students should never input personal, sensitive, or confidential data, including any data related to student education records, into any AI system without first ensuring

that the system meets applicable district school board policies and procedures along with federal and state statutes, including FERPA, COPPA, SUPER, and CIPA. (see below)

- Staff must never use AI tools to create misleading or inappropriate content, take someone's likeness without permission, or harm another person or the community at large.

The district will provide guidance to reflect technological advancements, legal requirements, and educational best practices regarding AI consistent with the procedures outlined here.

## **Data Privacy**

The Children's Online Privacy Protection Act (COPPA) is a federal law, enacted in 1998, related to the online collection, use, and sharing of personal information from students under age 13. Similarly, Student User Privacy in Education Rights (SUPER) is a Washington State law, enacted in 2015, related to the collection, sharing, and use of personal information for all K-12 students in the State of Washington. Neither COPPA nor SUPER preclude schools from acting as intermediaries between operators and parents/guardians in the notice and consent process or from serving as the parent/guardian's agent in the process of collecting personal information online from students in the school context when parents/guardians have provided permission for student internet use. Northshore supports COPPA and SUPER and insists that the services the district uses adhere to these laws. It is important that all Northshore staff members who work with children or their data be aware of and follow COPPA, SUPER, and other relevant state and federal regulations as well as associated district school board policies and procedures related to student internet access and related data use.

Northshore's collection, use, and sharing of student data is solely for educational purposes. The Family Educational Rights and Privacy Act (FERPA) mandates that the district protect the confidentiality of a student's Education Record, as defined within the statute. FERPA also affords parents/guardians (or students in some cases) rights related to the review, release, and correction of these education records. As with COPPA and SUPER, FERPA does not prohibit schools from appropriately using these data, but it does establish parameters around that use. These parameters include occasions where a parent/guardian has exercised their rights to have even their student's directory information, as defined in School Board Policy 3250, withheld from any directory release. It is important that all staff with access to a student's data understand and adhere to FERPA.

Northshore uses a variety of software systems in the classroom, the majority of which are hosted outside the district's facilities. 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.

Staff using web-based tools shall be aware of the Terms of Use and Privacy Policies for those systems. Staff who want to use any web-based resources (whether paid or "free" versions) with students shall obtain approval prior to use from the Technology Department via the Digital Resource Review (DRR) process before using the resource in any manner or creating any

accounts for themselves or others. Staff should exclusively utilize district-provided accounts and logins for professional purposes, refraining from creating accounts with personal information or using personal funds to subscribe to services. Depending on the nature of the resources and how they will be used with students, it may be necessary to obtain approval from the Curriculum Materials Adoption Committee (CMAC).

### **Network Security and Safety**

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. 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.

#### Safeguarding User Accounts:

- Lock the screen or log off if leaving the computer;
- Change passwords according to district policy;
- Do not use or attempt to use another user's account;
- Do not insert passwords into email or other communications;
- Keep user account passwords in a safe location;
- Do not use the 'remember password' feature of internet browsers; instead, use a password manager;
- When using non-NSD networks, such as those provided by a business, recognize that web filtering and network protections are not the same as when on NSD's network. Report any unexpected technical issues promptly.

#### Personal Information and Inappropriate Content:

- Staff should not reveal personal information publicly, including a home address and phone number on websites, blogs, videos, social networking sites, wikis, learning management systems, or as content on any other electronic medium;
- Staff should not reveal personal information about another individual on any digital service without first obtaining permission;
- 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
- If staff encounter dangerous or inappropriate information or messages, they should notify the appropriate school administrator.

### **Use of Social Media and Communication Platforms**

In order to maintain a professional and appropriate relationship with students, district employees must 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 any digital services or 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 their supervisor of the contact as soon as possible.

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

- Employees are prohibited from inappropriate online socializing with students or from engaging in any conduct on social networking websites 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 and collective bargaining agreements, as applicable;
- District employees are encouraged to use appropriate privacy settings to control access to their personal social media profiles. Private communication published on the internet can easily become public; social media sites can change their privacy settings and other functions without prior notice to subscribers. As a result, employees have an individual responsibility to understand the rules of the social media site being utilized;
- 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;
- Personal social media use, including communication with parents/guardians or community members, 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;
- The posting or disclosure of personally identifiable student information or confidential information via personal social media sites is prohibited;
- 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; and
- District employees should not create social media accounts which represent the district, a school, class, club, sport, program, or activity without prior approval from Technology and Communications staff representatives.

**Care of Assigned Technology**

Northshore staff are expected to exercise good judgment in the care of any district-assigned technology. Such technologies may include, but not be limited to, computers, accessories, audio/video equipment, and printers. To be good stewards of the funds paid through levies by taxpayers, Staff will:

- Report damage and/or malfunction to Technology staff in a timely manner;
- Protect devices from physical damage such as liquid exposure, scratches, dents, port or housing damage, or dropping;
- Avoid storing materials within the closed device, such as papers, pens, or paperclips;
- Maintain the security of computing devices, digitally and physically, by locking the screen and leaving the device in a secure location when the device is not in use;
- Follow directives to run applicable software updates and security patches as prescribed by the Technology Department;
- When taking equipment off site, staff will not leave technology unattended or in plain sight in a vehicle or other vulnerable location;

- Take regular inventory of peripherals and devices stored in a classroom or shared learning space to avoid loss;
- Turn off, shut down, and responsibly store devices over breaks and summer.

Loss and/or damage of district property may result in a financial liability to the building or employee, depending on the situation.

### **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. While network filters are not in effect when connected to non-NSD networks, employees are expected to act with professionalism and caution in accessing internet resources.

Trained and diligent staff are expected to be the first line of defense in controlling access by minors to inappropriate material on the internet that isn't caught by the filter. Staff are provided access to monitoring tools to ensure that students are accessing only those sites which benefit learning. Staff members who supervise students, control electronic equipment or have occasion to observe student use of said equipment online, will monitor the student use to assure that student use conforms to the mission and goals of the district. Staff must become familiar with the district-provided services for monitoring and filtering to instruct and assist students effectively. Staff will monitor and manage students using district-provided tools (training provided and/or required).

Any attempts to defeat or bypass the district's internet filter or conceal internet activity are prohibited. Staff will only use a network override privilege to access educational material. Use of override is tracked. Staff will not use proxies, unauthorized VPNs, special ports, unauthorized applications, modifications to district browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content.

### **Expectation of Privacy**

The district provides the network system, email and online services 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:

- The network;
- User files both local and in the cloud;
- User applications and bandwidth utilization;
- Email and other electronic communications;
- Internet access and browsing history; and
- Any and all information transmitted or received in connection with the network and use of district services.

Email inconsistent with the educational mission of the district or that poses a cybersecurity threat will be considered spam and blocked from entering district email boxes.

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.

## **Copyright**

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 is permitted when such duplication and distribution falls within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

## **Ownership of Work**

All work completed by employees as part of their employment will be considered property of the district as "work made for hire." The district will own any and all rights to such work including any and all derivative works, unless there is a written agreement to the contrary. Staff may not sell or share such property without explicit written permission from the district.

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 district. If under an agreement with the district, the work will be considered the property of the district. Staff members must obtain a student's permission prior to distributing their work to parties outside the school.

## **Unacceptable Use**

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 responsible use of technology. When these guidelines are not followed and unacceptable use occurs, the district shall impose disciplinary action.

### Examples of unacceptable use:

- Use for personal gain, commercial solicitation or compensation of any kind;
- Actions that result in unapproved liability or cost incurred by the district, including the sharing of student data without approval;
- Attempting to or completing the downloading, installing or use of games, audio files, video files or other applications for anything other than in the support of educational activities;
- Support or opposition for ballot measures, candidates and any other political activity;

- Attempting to or completing any hacking, cracking, vandalizing of district technology, devices, software, or systems;
- Attempting to or successfully introducing viruses, worms, Trojan horses, time bombs or changes to hardware, software and monitoring tools or any other activities that would damage, hinder or alter the use of district technology, devices, software, or systems;
- Unauthorized access or attempt to access other district computers, networks and information systems or unauthorized use of district-managed accounts on other systems;
- Attempting to inappropriately circumvent and district-managed content filtering or management system;
- Cyber bullying, phishing, hate mail, defamation, harassment, or discriminatory jokes or remarks;
- Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
- Accessing, uploading, downloading, storage and distribution of obscene, offensive, pornographic or sexually explicit material;
- Connecting unauthorized devices to the district network. Any such device will be confiscated and additional disciplinary action may be taken;
- Publishing personal details for any user (staff or student); making available personal information available for public viewing;
- Sharing student data with any digital service that has not been approved by Technology through the Digital Resource Review (DRR) process;
- Making audio, photo, or video recordings of any user (staff or student) without their prior permission; and
- Posing as someone else when online.

Issued: 1/22/96

Revised: 5/23/02, 5/5/06, 10/8/07, 9/15/14, 5/21/24