Purpose

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

It is assumed that parents and guardians grant their student(s) the right to access digital resources and have a desire to use the internet as an educational tool. Parents and guardians 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.

Digital Citizenship

Northshore provides access to technologies for all users (staff, students, and guests in some cases). All users must seriously consider the responsibilities associated with the opportunity to use technology devoted to activities that support learning. The expectations for behavior with regard to the responsible use of technology are defined as Digital Citizenship. Northshore students are expected to recognize the rights, responsibilities, and opportunities of living, learning, and working in an interconnected digital world, and will act in ways that are safe, legal, and ethical. Students will:

- Cultivate and manage their digital identity and reputation while being aware of the permanence and repercussions of their actions in the digital world.
- Engage in positive, safe, legal, and ethical behavior when using technology, including social interactions online or when using networked devices.
- Demonstrate an understanding of and respect for the rights and obligations of using and sharing intellectual property.
- Manage their personal data to maintain digital privacy and security while being aware of data-collection technologies used to track their navigation online.

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

Responsible use by students shall include, but not be limited to, the following:

- Completion of assignments and creation of original materials using digital resources which are in support of educational activities;
- Communication with staff and educational content experts using district-provided accounts and services such as email, collaboration platforms, and learning management systems (LMS) such as Schoology or Seesaw;
- Use of district computing devices and network resources for educational purposes only;

- Protection of personal information and passwords, including keeping account information private;
- Notifying appropriate campus or district officials of inappropriate behavior, vandalism, vulnerabilities, risks, and breaches of NSD services. If the student is uncertain whether an activity is permitted or appropriate, they will ask a teacher or administrator before engaging in that activity, and;
- Care of district technologies and prompt reporting of any damage or technical issue with any computing device.

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. When utilizing generative AI tools to create or support the creation of texts or creative works, students are expected to adhere to these guidelines as well as additional guidance provided by their classroom teacher:

- Students should use AI tools and techniques in a responsible and ethical manner. This includes not using AI to cheat, plagiarize, or gain an unfair advantage. Generative AI tools should only be used for school-related creative work (e.g., to generate text or other creative works) when given approval or guidance from the classroom teacher.
- Students should understand the limitations of AI and recognize that it is not a substitute for critical thinking, creativity, and problem-solving skills.
- Students should be aware that AI tools and techniques may be biased and should take steps to mitigate bias when using AI.
- Students should not share any personally-identifiable information (PII) with AI technologies, including name, birth date, address, or other financial or confidential information. The use of AI should be done in a way that protects PII.
- Students should use information and media literacy skills to check sources and find independent facts to confirm AI-generated content. AI has been known to create inaccurate information, and can be used to create misinformation and disinformation.
- When using AI tools and techniques, students should provide proper attribution and credit to the source of the tool or technique.
- When unsure whether the use of AI is appropriate for a particular assignment or project, students should seek guidance from their teacher.

Student Data Privacy

Students in Northshore are provided with a district account, which provides access to a wide variety of services for learning. This includes, but is not limited to, access to a monitored email account, an account in a learning management system, an account in the student information system, and accounts in curriculum-based services to support learning outcomes. These services are reviewed and vetted by Technology staff and should only be used when approved for use. If a parent or guardian has questions about the use of services regarding student data privacy, they should first contact their teacher or school administrator.

Network Security and Safety

Passwords are the first level of security for a user's account. Students 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.

- Students should not reveal personal information, 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;
- Students should not share their passwords, nor write them down in a public place;
- Students should not reveal personal information about another person on any digital service; and
- If students encounter dangerous or inappropriate information or messages, they should notify their teacher or school administrator.

Care of Assigned Technology

Northshore students are expected to exercise good judgment in the care of any district-assigned technology. If a device is lost, damaged, or permanently defaced in some way, fines may be imposed. Fine information and procedures for paying fines can be found on the district website. Students will:

- Report damage and/or device malfunction to school staff in a timely manner;
- Protect the device from exposure to food and liquids, whether while storing, transporting, or using the device;
- Avoid storing materials within the closed device, such as papers, pens, or paperclips;
- Secure devices that are not in use;
- Maintain the device by leaving intact all district labels, rubber bumpers, keys, and buttons, and by not decorating the device with markings or stickers;
- Avoid leaving technology unattended or visible in a parked vehicle or other vulnerable location;
- Keep track of accessories such as the power cable and bag;
- Bring the device to school each day fully charged and ready for learning.

Filtering and Monitoring

Filtering software is used to block and/or filter access to web-based content that may be harmful or inappropriate. While filters make it more difficult for objectionable material to be received or accessed, filters don't catch everything that may be objectionable. Students are expected to take reasonable care to avoid inappropriate web content.

Staff have the ability and responsibility to monitor and adjust student access to web content. The District employs several services that allow staff to view student internet history and searches and to control the content a student views within the context of a learning experience. Any attempts by students to defeat or bypass the District's internet filter or conceal internet activity are prohibited and may result in disciplinary action and loss of access to devices and network resources.

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:

- Student files both local and in the cloud;
- Student web browsing history and search history, including blocked content;
- Email and other electronic communications;
- Digital interactions with other students and staff.

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.

Unacceptable Use

Students are expected to use technology and network resources with care and responsibility. Expectations for use of these resources are outlined above. 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 damage or breach of district services;
- Attempting to or completing the downloading, installing or use of games, audio files, video files or other applications for anything other than the support of approved educational research;
- Support or opposition for ballot measures, candidates and any other political activity;
- Attempting to or completing any hacking, cracking, or vandalizing District technology, devices, software, or systems;
- Attempting to or successfully introducing viruses, worms, Trojan horses, time bombs or other 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 to other district computers, networks, and information systems or unauthorized use of district-managed accounts on other systems;
- Attempting to circumvent any content filtering or management system;
- Cyberbullying, 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 or attempting to connect unauthorized devices to the District network. Any such device will be confiscated and additional disciplinary action will be taken;
- Publishing personal details for any student and/or making available personal information available for public viewing. Parents and guardians shall refrain from publishing pictures or information about other students without first seeking permission;
- Taking pictures of or making audio or video recordings of any user without their prior permission; and
- Posing as someone else when online.

Consequences for unacceptable use are outlined in the Student Rights and Responsibilities Handbook.

Issued: 5/21/2024