STAFF TECHNOLOGY USE POLICY

I. PURPOSE

The purpose of this policy is to set forth policies and guidelines for access to the school district computer system and acceptable use of the Internet.

II. GENERAL STATEMENT OF POLICY

The New Prague School District provides technology resources to its students and staff for educational and administrative purposes. The goal in providing these resources is to promote educational excellence in the New Prague Schools by facilitating collaboration, innovation, and communication with the support and supervision of parents, teachers and support staff. The use of these technology resources is a privilege, not a right.

With access to computers and people all over the world comes the potential availability of material that may not be considered to be of educational value in the context of the school setting. The New Prague School District firmly believes that the value of information, interaction, and research capabilities available outweighs the possibility that users may obtain material that is not consistent with the educational goals of the district.

Proper behavior, as it relates to the use of technology, is no different than proper behavior in all other aspects of New Prague School's activities. All users are expected to use the technology equipment and technology networks in a responsible, ethical and polite manner. This document is intended to clarify those expectations as they apply to computer and network usage and is consistent with district policy.

III. EMPLOYEE USE GUIDELINES

The Internet, an international network of networks, allows people to access networks and computers, including local, national and international resources such as libraries, government agencies, universities, K-12 schools, social media, software, technical information, news and weather. Other technologies such as voicemail, copy machines and fax modems allow enhanced communication opportunities.

A. The Internet, district computer networks, computer workstations and voicemail network, copy and fax machines must be used responsibly, ethically and legally. Failure to adhere to district policies, regulations and guidelines for the use of computers, networks and the Internet will result in a revocation of access privileges or more.

B. The District recognizes that student groups or members of the public may create social media representing students or groups within the District. When employees, including coaches/advisors, choose to join or engage with these social networking groups, they do so as an employee of the District. Employees have responsibility for maintaining appropriate employee-student relationships at all times and have responsibility for addressing inappropriate behavior or activity on these networks. This includes acting to protect the safety of minors online.

C. The following actions will not be permitted:

1. Using abusive language, including hate mail, harassment or discriminatory remarks;

2. Deliberately accessing inappropriate websites that contain obscene material, including reviewing, downloading, storing or printing files or messages that are obscene, vulgar or sexually explicit, or that use language that degrades others;

3. Copying or using anything as public without the permission of the author. (All communications and information accessible through the Internet or other computer networks should be assumed to be private property.)

4. Maliciously attempting to harm or destroy data of another user, school or district networks, or the Internet, including uploading or creating viruses;

5. Using networks or technology equipment for any illegal activity, including violation of copyright or other laws;

6. Employees shall not use obscene, profane or vulgar language on any social media network or engage in communications or conduct that is harassing, threatening, bullying, libelous, or defamatory or that discusses or encourages any illegal activity or the inappropriate use of alcohol, use of illegal drugs, sexual behavior, sexual harassment, or bullying.

7. Using networks for a commercial, political or profit-making enterprise, which may include fund raising for which no personal gain is involved; except as specifically agreed to with the district,

8. Using or accessing a file or an account owned by another user without their permission, or

9. Deliberately distributing or downloading any material in such a manner that causes congestion of networks.

C. Downloading software to District machines, which includes; software from home, shareware, freeware and purchased software is not acceptable and will not be supported by District Technology staff. All software needs to be approved through proper channels.

D. Downloading Files from the Internet – There is always a risk that downloaded software may pose a threat to District #721 computer systems. If an authorized user locates a file that they have a need to acquire, they are required to take the following precautions:

1. Make sure the file is within the guidelines of district policies and regulations on acceptable use of technology and

2. Apply available approved virus scanning software on the file before the file is opened or launched.

IV. EMPLOYEE SUPERVISION OF STUDENT NETWORK USE

District 721 employees are responsible for supervising student use on the Internet.

A. When students use the Internet independently for school work, it is the teacher's responsibility to make sure the students comply with guidelines on acceptable use of the Internet.

V. NETWORK, E-MAIL AND VOICEMAIL ETIQUETTE

A. All network, e-mail and voicemail users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

1. Be polite. Refrain from any abusive language. (District policies on harassment and discrimination also apply to electronic communications.)

2. Use appropriate language. Swearing, vulgarities and other similar use of language is not acceptable.

3. Do not send messages of a personal nature to groups of people, Schools and /or the entire district (such as to sell a personal possession, look for a roommate, express personal opinions, conduct a personal survey, etc.)

4. Do not use e-mail, district computer or voicemail networks for commercial, profit-making, personal gain, political or political campaign purposes.

5. Do not send fraudulent, intimidating or anonymous messages.

6. Do not participate in defamatory or other unprofessional attacks on individuals or organizations.

B. Security

1. Electronic mail (e-mail), voicemail and telecommunications are not to be used to share confidential information about students or other employees.

2. The networks and voicemail systems are a shared resource, which are the property of the District and as such, may be subject to district-authorized search to ensure the integrity of the networks and compliance with policies and laws. If there is reason to believe that there has been misuse of district resources, user accounts may be accessed by network administrators.

3. Anything posted on an employee's Web site or Web log or other Internet content for which the employee is responsible will be subject to all District policies, rules, regulations, and guidelines. The District is free to view and monitor an employee's Web site or Web log at any time without consent or previous approval. Where applicable, employees may be asked to disclose to the District the existence of and to provide the District with access to an employee's Web site or Web log or other personal social media network as part of an employment selection, promotion, or disciplinary process.

VI. PERSONAL USE

School computers, networks, Internet access, copy and fax machines are provided to support the educational mission of the school. They are to be used primarily for school-related purposes. Incidental personal use of school computer must not interfere with the employee's job performance, must not violate any of the rules contained in this policy or the Student Acceptable

Use Policy, and must not damage the school's hardware, software or computer communications systems.

VII. SAFEGUARDING ACCOUNTS AND PASSWORDS

Employees are responsible for safeguarding their own passwords. Each employee will be held responsible for the consequences of intentional or negligent disclosure of this information.

VIII. REPRESENTING PERSONAL VIEWS AS THOSE OF THE SCHOOL DISTRICT

Any e-mail sent from a school computer is likely to contain a return address identifying the school district. Thus, sending an e-mail from the school is analogous to an employee using school letterhead. Employees should be careful not to have their own statements mistakenly attributed to the district.

Adopted: 08/27/01
Revised: 08/11/08; 12/10/15
Reviewed: 05/24/10; 05/22/17