INDEPENDENT SCHOOL DISTRICT 196
Rosemount-Apple Valley-Eagan Public Schools
Educating our students to reach their full potential

Series Number **503.7AR** Adopted **March 1997** Revised **July 2013**

Title **Acceptable Use of Information Technology – Students**

1. **Permission to Use Networks** – District 196 offers students access to a variety of technology resources, including the Internet and email at approved grade levels. Before a student is permitted to access the Internet the student and his or her parent or guardian will be asked to complete and return Procedure 503.7.1P or 503.7.2P, Permission for Student Access and Use of the Internet.

2. **Network and Computer Use Guidelines**

   2.1 General Use Guidelines

   2.1.1 Use of the Internet, other computer networks and computer workstations is a privilege which may be revoked at any time for abusive conduct.

   2.1.2 Access to the Internet will be for specific educational purposes only, such as researching a specific topic for a classroom project. While on the Internet, students are expected to remain focused on the topic they are researching, and are expected to log off the system when the research is completed. Any information (including text, software, graphics and images) downloaded from the Internet should be classroom-related.

   2.1.3 In addition to the district's standard consequences for student misbehavior (refer to Administrative Regulation 503.3AR, Student Behavior Expectations and Consequences for Misbehavior), any network misuse or illegal activities will result in temporary or permanent cancellation of network privileges, contact with the student's parent or guardian and, if a violation of law has occurred, contact with law enforcement authorities. The following actions will not be permitted:

   2.1.3.1 Using abusive language, including hate mail, cyberbullying, harassment or discriminatory remarks;

   2.1.3.2 Participating in defamatory attacks on individuals or organizations;

   2.1.3.3 Sending fraudulent, intimidating or anonymous messages;

   2.1.3.4 Deliberately accessing inappropriate websites that contain objectionable, offensive or obscene material, including reviewing, downloading, storing or printing files or messages that are obscene, vulgar, sexually explicit or that use language that offends or tends to degrade others;

   2.1.3.5 Accessing social networking websites and chat rooms without permission or using such sites in a manner that is not authorized;

   2.1.3.6 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.);

   2.1.3.7 Deliberately or maliciously attempting to harm or destroy data of another user, school or district networks, or the Internet, including uploading or creating viruses;

   2.1.3.8 Using networks for any illegal activity, including violation of copyright, gambling or other laws;

2.1.3.9 Using networks for a commercial, political or profit-making enterprise, except as specifically approved by the superintendent or designee;

2.1.3.10 Gaining unauthorized access to resources or entities;

2.1.3.11 Using an account owned by another user, with or without their permission, or

2.1.3.12 Deliberately distributing any material in such a manner that might cause congestion of networks.

2.1.4 Students who come across any information that is obscene, vulgar, sexually explicit or offensive should immediately inform a teacher or other adult staff member. Students are responsible for not pursuing this type of information.

2.1.5 Students who feel they are victims of cyberbullying or who feel unsafe because of something they encountered online should immediately inform a teacher or other adult staff member.

2.1.6 District-owned networks, servers and end-user devices 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 district network and said devices, and to ensure 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 and other administrators. Students do not have an expectation of privacy with regard to district-owned networks, servers, computers and other devices.

2.1.7 Students who are permitted to bring their own electronic devices to school will comply with school-specific guidelines for the use of personal electronic devices in school.

2.2 Downloading Files from the Internet – There is always a risk that downloaded software may pose a threat to District 196 computer systems. If an authorized user locates a file that they need to acquire, they are expected to take the following precautions:

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

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

3. **Network, Internet and Email Etiquette** – All network, Internet and email users are expected to abide by school and district policies and rules, and the generally accepted rules of network etiquette. These include, but are not limited to, the following:

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

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

3.3 Seek guidance from school staff when personal contact information is solicited by websites.

Reference: - 47 U.S.C. § 254 (h), Children's Internet Protection Act
- Federal Bureau of Investigation Safe Surfing website https://sos.fbi.gov/