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

Series Number **407.7AR** Adopted **March 1997** Revised **February 2019**

Title **Acceptable Use of Information Technology - Employees**

1. **Employee Use Guidelines**

   1.1 The Internet, district computer networks, computing devices and the voicemail network must be used responsibly, ethically and legally.

      1.1.1 Failure to adhere to district policies, regulations and guidelines for the use of computers, networks and the Internet may result in a revocation of access privileges.

      1.1.2 Misuse or illegal activities may also result in disciplinary action, up to and including termination of employment.

   1.2 The following actions will not be permitted:

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

      1.2.2 Participating in defamatory or other unprofessional attacks on individuals or organizations;

      1.2.3 Sending fraudulent, intimidating or anonymous messages;

      1.2.4 Sending 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.);

      1.2.5 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 visual depictions that are obscene or child pornography, or that use language that degrades others;

      1.2.6 Violating copyright laws 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);

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

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

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

      1.2.10 Gaining unauthorized access to resources or entities or accessing private or confidential data without authority and a professional need to access the data;

      1.2.11 Unauthorized use or access of a file or an account assigned to another user without their permission;

1.2.12 Deliberately distributing or downloading any material in such a manner that causes congestion of networks, and

1.2.13 Excessive personal use of district technology including misuse of social media per Administrative Regulation 407.8AR, Employee Use of Online Social Media.

1.3 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 have a need to acquire, they are required to take the following precautions:

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

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

2. **Employee Supervision of Student Network Use** – District 196 employees are responsible for supervising student use of the Internet.

2.1 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, Permission for Student Access and Use of the Internet.

2.2 When students use the Internet independently for school work under the supervision of a teacher, it is the teacher's responsibility to make sure the students comply with the guidelines in Administrative Regulation 503.7AR, Acceptable Use of Information Technology – Students.

2.3 Employees shall be aware of and shall help address the components of the Internet Safety Policy, as required in the federal Children's Internet Protection Act (CIPA), including the following issues:

2.3.1 Access by minors to inappropriate material on the Internet and World Wide Web;

2.3.2 The safety and security of minors when using email, chat rooms and other forms of direct electronic communications;

2.3.3 Unauthorized access, including so-called "hacking" and other unlawful activities by minors online;

2.3.4 Unauthorized disclosure, use and dissemination of personal information regarding minors, and

2.3.5 Measures designed to restrict minors' access to materials harmful to minors.

2.4 Employees shall comply with any terms of use requirements of applications.

3. **Network, Internet, Email and Voicemail Etiquette** – All network, Internet, email and voicemail users are expected to abide by 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 also apply to electronic communications.)

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

4. **Security**

4.1 Email, voicemail and other electronic transmissions are not to be used to share confidential information about students or other employees, except as permitted by state and federal data privacy laws. When private or confidential information is shared via email, voicemail or other electronic transmission methods, steps must be taken to protect the privacy of the subject of the information or to preserve information privacy.

4.2 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. User accounts may be accessed by network administrators, supervisors and other administrators. Employees do not have an expectation of privacy with regard to district-owned networks, servers, computers and other devices.

4.3 When accessing information on students through information technology, employees may only access information on those students for whom the employee has legitimate educational interest as a result of the employee's direct professional responsibilities. It is a data privacy violation for an employee to access information on a student for whom the employee does not have direct professional responsibilities or to access information on a student that goes beyond the employee's direct professional responsibilities or for purposes unrelated to those responsibilities.

4.4 Reasonable precautions must be taken to safeguard the privacy and security of student information or other private or confidential information stored on mobile electronic devices, whether district owned or employee owned. Such devices should not be used to store or communicate private data unless security features, such as encryption or password protection, are utilized. All private or confidential information stored on an employee's personal electronic devices must be removed upon separation of employment.

4.5 An employee who becomes aware of a breach of the security of private or confidential data must report the breach to a supervisor immediately. Supervisors will determine, in consultation with appropriate district administrators, what measures should be taken to address the security breach. For purposes of this paragraph, a breach of the security of data may include the loss or theft of a device containing private of confidential data or the unauthorized acquisition of data by a person.

Reference:
- 47 U.S.C. § 254 (h), Children's Internet Protection Act
- District 196 Administrative Regulation 407.8AR, Employee Use of Online Social Media
- Minnesota Statute 13.055, Disclosure of Breach in Security; Notification and Investigation Report Required