

524 INTERNET ACCEPTABLE USE AND SAFETY

I. PURPOSE

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

II. GENERAL STATEMENT OF POLICY

In making decisions regarding student and employee access to the school district computer system and the Internet, including electronic communications, the school district considers its own stated educational mission, goals, and objectives. Electronic information research skills are now fundamental to preparation of citizens and future employees. Access to the school district computer system and to the Internet enables students and employees to explore thousands of libraries, databases, bulletin boards, and other resources while exchanging messages with people around the world. The school district expects that faculty will blend thoughtful use of the school district computer system and the Internet throughout the curriculum and will provide guidance and instruction to students in their use. All users are to use the school district's computer system for school-district-related business or educational purposes exclusively.

III. DEFINITION OF TERMS

School district computer system - The District's computer system is composed of all district purchased and operated hardware, software and services including all of the networking and computer hardware, operating system software, application software, and stored data. Stored data includes, but is not limited to, electronic mail, local databases, externally accessed databases (such the District's website), optical media, clip art, digital images, digitized information, communications technologies, and new technologies as they become available. The District reserves the right to monitor all technology resource activity.

Employees - An Employee is an individual approved and contracted to perform the duties of a full-time or part-time position within the District.

Faculty - Faculty are employees of the District who have earned and maintained a valid Teaching License for the State of Minnesota and are assigned to a teaching position within the District.

Internet - The Internet is a global system of interconnected computer networks that use the standardized Internet Protocol Suite (TCP/IP) consisting of millions of private and public, academic, business, and government networks of local to global scope that are linked by copper wires, fiber-optic cables, wireless connections, and other technologies. The Internet carries a vast array of information resources and services, most notably the inter-linked hypertext documents of the World Wide Web (WWW), and the infrastructure to support electronic mail (email) as well as other communication services via text, images, audio, voice and video.

IV. LIMITED EDUCATIONAL PURPOSE

The school district is providing students and employees with access to the school district's computer system, which includes Internet access. The purpose of the system is more specific than providing students and employees with general access to the Internet. The school district system has a limited educational purpose, which includes use of the system for classroom activities, educational research and professional or career development activities. Users are expected to use Internet access through the district system to further educational and personal goals consistent with the mission of the school district and school policies. Uses which might be acceptable on a user's private personal account on another system may not be acceptable on this limited-purpose network.

V. APPLICATION OF POLICY

The policy will apply to all users of the school districts computer systems, including, but not limited to students, employees, administrators, volunteers, parents, part-time employees, and Board members. The policy applies regardless of how, where, or when the school district's system is accessed.

VI. USE OF SYSTEM

A. The use of the school district system and access to use of the Internet is a privilege, not a right. Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of the school district system or the Internet may result in one or more of the following consequences: suspension or cancellation of use or access privileges; payments for damages and repairs; discipline under other appropriate school district policies, including suspension, expulsion, exclusion or termination of employment; or civil or criminal liability under other applicable laws.

B. Users may only access the school district's computer system through school district supplied software and in a manner specified by the school district's information officers. Default setting on school district supplied software may be altered.

C. Users may only access the school district's computer system with school district supplied passwords and user names. Passwords will be held as confidential by users.

D. Users may not install software on the school district's computers without the prior permission the Technology Department.

E. Users shall not transfer confidential school district files outside the school district network without assuring confidentiality of said information.

F. Each user is responsible for the security of the school district's computer systems. Users must prevent access to the school district's system by those who are not authorized to use the system.

1. E-mail and other communication are vulnerable to interception;
2. confidential communication is prohibited;
3. user will be held responsible for all confidential communications and scope of distribution.

G. Users will observe proper etiquette in their communications. All communications bear the school district's address and should reflect upon the school district.

H. The proper use of the school district's computer system is the responsibility of the individual user.

I. The school district reserves the right to limit or deny access to certain users and to certain types of information.

VII. UNACCEPTABLE USES

A. The following uses of the school district system and Internet resources or accounts are considered unacceptable:

1. Users will not use the school district system to access, view, upload, download, store, print, post, receive, transmit or distribute:

a. pornographic, obscene or sexually explicit material or other visual depictions that are harmful to minors.

b. obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language.

c. materials that use language or images that are inappropriate in the educational setting or disruptive to the educational process.

d. information or materials that could cause damage or danger of disruption to the educational process.

e. materials that use language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination. All school district policies against harassment will be applied with full force to misconduct using the school's computer systems.

f. No district employees or students shall use school district technology resources to promote or solicit support for any personal platform or religious affiliation.

g. Any materials that are not relevant to school and/or a school assignment.

2. Users will not use the school district system to knowingly or recklessly post, transmit or distribute false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.

3. Users will not use the school district system to engage in any illegal act or violate any local, state or federal statute or law.

4. Users will not use the school district system to vandalize, damage or disable the property of another person or organization, will not make deliberate attempts to degrade or disrupt equipment, software or system performance by spreading computer viruses or by any other means, will not tamper with, modify or change the school district system software, hardware or wiring or take any action to violate the school district's security system, and will not use the school district system in such a way as to disrupt the use of the system by other users.

5. Users will not use the school district system to gain unauthorized access to information resources or to access another person's materials, information or files without the implied or direct permission of that person.

6. Users will not use the school district system to post private information about another person, personal contact information about themselves or other persons, or other personally identifiable information, including, but not limited to, addresses, telephone numbers, school addresses, work addresses, identification numbers, account numbers, access codes or passwords, labeled photographs or other information that would make the individual's identify easily traceable, and will not repost a message that was sent to the user privately without permission of the person who sent the message.

a. This paragraph does not prohibit the posting of employee contact information on school district webpages or communications between employees and other individuals when such communications are made for education-related purposes (i.e., communications with parents or other staff members related to students).

b. Employees creating or posting school-related webpages may include personal contact information about themselves on a webpage. However, employees may not post personal contact information or other personally identifiable information about students unless:

(1) such information is classified by the school district as directory information, and verification is made that the school district has not received notice from a parent/guardian or eligible student that such information is not to be designated as directory information in accordance with Policy 515; or

(2) such information is not classified by the school district as directory information but written consent for release of the information to be posted has been obtained from a parent/guardian or eligible student in accordance with Policy 515.

In addition, prior to posting any personal contact or personally identifiable information on a school-related webpage, employees shall obtain written approval of the content of the postings from the building administrator.

c. These prohibitions specifically prohibit a user from utilizing the school district system to post personal information about themselves or any other individual on social networks, including, but not limited to, social networks such as "Facebook," "Twitter," or any non-school provided social network resource."

7. Users must keep all account information and passwords on file with the designated school district official. Users will not attempt to gain unauthorized access to the school district system or any other system through the school district system, attempt to log in through another person's account, or use computer accounts, access codes or network identification other than those assigned to the user. Messages and records on the school district system may not be encrypted without the permission of appropriate school authorities.

8. Users will not use the school district system to violate copyright laws or usage licensing agreements, or otherwise to use another person's property without the person's prior approval or proper citation, including

the downloading or exchanging of pirated software or copying software to or from any school computer, and will not plagiarize works they find on the Internet.

9. Users will not use the school district system for conducting business, for unauthorized commercial purposes or for financial gain unrelated to the mission of the school district. Users will not use the school district system to offer or provide goods or services or for product advertisement. Users will not use the school district system for personal gain. All forms of gambling using the school district's computer systems are forbidden.

10. Users may not enter into contractual relations over the Internet or other computer networks without the express prior permission of the school district administration.

11. No person should knowingly circumvent any security features that have been put in place by the district.

12. Users will not use the school district system to engage in bullying or cyberbullying in violation of the school district's Bullying Prohibition Policy 514. This prohibition includes using any technology or other electronic communication off school premises to the extent that student learning or the school environment is substantially and materially disrupted.

B. The school district has a special interest in regulating off-campus speech that materially disrupts classwork or involves substantial disorder or invasion of the rights of others. A student or employee engaging in any of the foregoing unacceptable uses of the Internet when off school district premises and without the use of the school district system also may be in violation of this policy as well as other school district policies. Examples of such violations may include, but are not limited to, serious or severe bullying or harassment targeting particular individuals, threats aimed at teachers or other students, failure to follow rules concerning lessons, the writing of papers, the use of computers, or participation in other online school activities, and breaches of school security devices. In situations when the school district receives a report of usage that may be illegal in nature, originating from a non-school computer or resource, the school district shall investigate such reports to the best of its ability. Students or employees may be subject to disciplinary action for such conduct including, but not limited to, suspension or cancellation of the use or access to the school district computer system and the Internet and discipline under other appropriate school district policies, including suspension, expulsion, exclusion, or termination of employment.

C. If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the inadvertent access to an appropriate school district official. In the case of a school district employee, the immediate disclosure shall be to the employee's immediate supervisor and/or the building administrator. This disclosure may serve as a defense against an allegation that the user has intentionally violated this policy. In certain rare instances, a user also may access otherwise unacceptable materials if necessary to complete an assignment and if done with the prior approval of and with appropriate guidance from the appropriate teacher or, in the case of a school district employee, the building administrator.

VIII. FILTER

In regard to filtering Internet access, the school district is responsible to:

A. With respect to any of its computers with Internet access, the School District will monitor the online activities of both minors and adults and employ technology protection measures during any use of such computers by minors

and adults. The technology protection measures utilized will block or filter Internet access to any visual depictions that are:

1. obscene;
2. child pornography; or
3. harmful to minors.

B. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or
2. depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

C. An administrator, supervisor or other person authorized by the Superintendent may disable the technology protection measure, during use by an adult, to enable access for bona fide research or other lawful purposes.

D. The school district will educate students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

IX. CONSISTENCY WITH OTHER SCHOOL POLICIES

Use of the school district computer system and use of the Internet shall be consistent with the school district policies and the mission of the school district.

X. LIMITED EXPECTATION OF PRIVACY

A. By authorizing use of the school district system, the school district does not relinquish control over materials on the system or contained in files on the system. Users should expect only limited privacy in the contents of personal files on the school district system.

B. Routine maintenance and monitoring of the school district system may lead to a discovery that a user has violated this policy, another school district policy, or the law.

C. An individual investigation or search will be conducted if school authorities have a reasonable suspicion that the search will uncover a violation of law or school district policy.

D. Parents have the right at any time to investigate or review the contents of their child's files and e-mail files. Parents have the right to request the termination of their child's individual account at any time.

E. School district employees should be aware that the school district retains the right at any time to investigate or review the contents of their files and e-mail files. In addition, school district employees should be aware that data and other materials in files maintained on the school district system may be subject to review, disclosure or discovery under Minnesota Statutes, Chapter 13 (the Minnesota Government Data Practices Act).

F. The school district will cooperate fully with local, state and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with school district policies conducted through the school district system.

XI. INTERNET USE AGREEMENT

A. The proper use of the Internet, and the educational value to be gained from proper Internet use, is the joint responsibility of students, parents and employees of the school district.

B. This policy requires the permission of and supervision by the school's designated professional staff before a student may use a school account or resource to access the Internet.

C. The Internet Use Agreement form for students must be read and signed by the user, the parent or guardian, and the supervising teacher. The form must then be filed at the school office. As supervising teachers change, the agreement signed by the new teacher shall be attached to the original agreement.

XII. LIMITATION ON SCHOOL DISTRICT LIABILITY

A. Use of the school district system is at the user's own risk.

B. The system is provided on an "as is, as available" basis.

C. The school district will not be responsible for any damage users may suffer, including, but not limited to, loss, damage or unavailability of data stored on school district diskettes, tapes, hard drives or servers, or for delays or changes in or interruptions of service or misdeliveries or nondeliveries of information or materials, regardless of the cause.

D. The school district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the school district system.

E. The school district will not be responsible for financial obligations arising through unauthorized use of the school district system or the Internet.

F. The school district disclaims all responsibility for any information obtained or released using the school district's computer systems.

G. The school district disclaims any liability for any financial obligations incurred over the district's system and any damage to personal property incurred while accessing or attempting to access the school district's computer system.

XIII. USER NOTIFICATION

A. All users shall be notified of the school district policies relating to Internet use.

B. This notification shall include the following:

1. Notification that Internet use is subject to compliance with school district policies.

2. Disclaimers limiting the school district's liability relative to:

- a. Information stored on school district diskettes, hard drives or servers.
- b. Information retrieved through school district computers, networks or online resources.
- c. Personal property used to access school district computers, networks or online resources.
- d. Unauthorized financial obligations resulting from use of school district resources/accounts to access the Internet.

3. A description of the privacy rights and limitations of school sponsored/managed Internet accounts.

4. Notification that, even though the school district may use technical means to limit student Internet access, these limits do not provide a foolproof means for enforcing the provisions of this acceptable use policy.

5. Notification that goods and services can be purchased over the Internet that could potentially result in unwanted financial obligations and that any financial obligation incurred by a student through the Internet is the sole responsibility of the student and/or the student's parents.

6. Notification that the collection, creation, reception, maintenance and dissemination of data via the Internet, including electronic communications, is governed by Policy 406, Public and Private Personnel Data, and Policy 515, Protection and Privacy of Pupil Records.

7. Notification that should the user violate the school district's acceptable use policy, the user's access privileges may be revoked, school disciplinary action may be taken and/or appropriate legal action may be taken.

8. Notification that all provisions of the acceptable use policy are subordinate to local, state and federal laws.

XIV. PARENTS' AND STUDENTS' COPYRIGHT WAIVER

If the school district wishes to publish students' works on the Internet, the parents and students should waive their copyrights and give the school district permission to reproduce, adapt, publish, and display such works on the Internet.

XV. PARENT RESPONSIBILITY; NOTIFICATION OF STUDENT INTERNET USE

A. Outside of school, parents bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephones, radio, movies and other possibly offensive media. Parents are responsible for monitoring their student's use of the school district system and of the Internet if the student is accessing the school district system from home or a remote location.

B. Parents will be notified that their students will be using school district resources/accounts to access the Internet and that the school district will provide parents the option to request alternative activities not requiring Internet access. This notification should include:

1. A copy of the user notification form provided to the student user.
2. A description of parent/guardian responsibilities.
3. A statement that the Internet Use Agreement must be signed by the user, the parent or guardian, and then returned to the respective Principal's Office prior to use by the student.
4. A statement that the school district's acceptable use policy is available for parental review.

XVI. IMPLEMENTATION; POLICY REVIEW

A. The school district administration may develop appropriate user notification forms, guidelines and procedures necessary to implement this policy for submission to the school board for approval. Upon approval by the school board, such guidelines, forms and procedures shall be an addendum to this policy.

B. The administration shall revise the user notifications, including student and parent notifications, if necessary, to reflect the adoption of these guidelines and procedures.

C. The school district's Internet policies and procedures are available for review by all parents, guardians, staff and members of the community.

D. Because of the rapid changes in the development of the Internet, the school board shall conduct an annual review of this policy.

Cross References:

Dover-Eyota Public Schools Policy 403 (Discipline, Suspension and Dismissal of School District Employees)
Dover-Eyota Public School Policy 406 (Public and Private Personnel Data)
Dover-Eyota Public Schools Policy 413 (Harassment and Violence)
Dover-Eyota Public Schools Policy 505 (Distribution of Nonschool-Sponsored Materials on School premises by Students and Employees)
Dover-Eyota Public Schools Policy 506 (Student Discipline)
Dover-Eyota Public Schools Policy 514 (Bullying Prohibition)
Dover-Eyota Public Schools Policy 515 (Protection and Privacy of Pupil Records)
Dover-Eyota Public Schools Policy 519 (Interviews of Students by Outside Agencies)
Dover-Eyota Public Schools Policy 521 (Student Disability Nondiscrimination)
Dover-Eyota Public Schools Policy 522 (Student Sex Nondiscrimination)
Dover-Eyota Public Schools Policy 603 (Curriculum Development)
Dover-Eyota Public Schools Policy 604 (Instructional Curriculum)
Dover-Eyota Public Schools Policy 606 (Textbooks and Instructional Material)
Dover-Eyota Public Schools Policy 804 (Bomb Threats)
Dover-Eyota Public Schools Policy 904 (Distribution of Materials on School District Property by Nonschool Persons)
Dover-Eyota Netbook Handbook