

STUDENT PERSONNEL

Series 500

Policy Title: INTERNET/TECHNOLOGY ACCEPTABLE USE POLICY

Code No. 524

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 technology, and the Internet, including electronic communications.

II. GENERAL STATEMENT OF POLICY:

In making decision 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.

III. 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 ore 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 or another system may not be acceptable on this limited purpose network.

IV. USE OF SYSTEM IS A PRIVILEGE:

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.

V. 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, review, upload, download, store, print, 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 education 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.
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 identity 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; 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.

In addition, prior to posting any personal contact or personally identifiable information to a school-related webpage, employees shall obtain a 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 a user or another individual on social networks, including, but not limited to, social networks such as "My Space" and "Facebook". The district technology committee must approve any exception for specific social network usage.

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 for product advertisement. Users will not use the school district system to purchase goods or services for personal use without authorization from the appropriate school district official.

B. A student or employee engaging in the foregoing unacceptable uses of the Internet when off school district premises also may be in violation of this policy as well as other school district policies. Examples of violations are, but are not limited to, situations where the school district system is compromised or if a school district employee or student is negatively impacted. If the school district receives a report of unacceptable use originating from a non-school computer or resource, the school district may 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.

VI. FILTER:

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

VII. CONSISTENCY WITH OTHER SCHOOL POLICIES:

Use of the School District computer system and use of the Internet shall be consistent with School District policies and the mission of the School District.

VIII. 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 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.

IX. 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 must be read and signed by the user and the parent or guardian. The form must then be filed at the school office.

x. LIMITATION ON SCHOOL DISTRICT LIABILITY:

Use of the School District system is at the user's own risk. The system is provided on an "as is, as available" basis. 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 of nondeliveries of information or materials, regardless of the cause. 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. The School District will not be responsible for financial obligations arising through unauthorized use of the school district system or the Internet.

XI. 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, network 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 or the student's parents.
6. Notification that should the user violate the School District's acceptable use policy, the student's access privileges may be revoked, school disciplinary action may be taken and/or appropriate legal action may be taken.

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

8. 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.

XII. 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 notification that the parents have the option to request alternative educational activities not requiring Internet access and the material to exercise this option.
4. A statement that the Internet Use Agreement must be signed by the user, and the parent or guardian, and be under staff supervision while using the Internet.
5. A statement that the School District’s acceptable use policy is available for parental review.

XIII. IMPLEMENTATION; POLICY REVIEW

A. The School District administration may develop appropriate guidelines and procedures necessary to implement this policy for submission to the School Board for approval. Upon approval by the School Board, such guidelines and procedures shall be an addendum to this policy.

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

C. The School District’s Internet/Technology 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.

Date of Adoption:
July 1, 1979

Revised:
March 8, 2001
April 15, 2004 / April 22, 2010
April 28, 2016

Authority for Policy:
Board of Education

STUDENT PERSONNEL

Series 500

Policy Title: PARENT PERMISSION LETTER

Code No. 524.1

LUVERNE PUBLIC SCHOOLS

DISTRICT #2184
LUVERNE, MINNESOTA

PARENT PERMISSION LETTER INTERNET, TECHNOLOGY & ELECTRONIC MAIL PERMISSION FORM

We are pleased to offer students of Luverne Public Schools access to the district computer networks for electronic mail and the Internet. To gain access to e-mail and the Internet, all students must obtain parental permission and must sign and return this form to the respective principals' office.

Access to e-mail and the Internet will enable students to explore thousands of libraries, databases, and bulletin boards while exchanging messages with Internet users throughout the world. Families should be warned that some materials accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people. While our intent is to make Internet access available to further educational goals and objectives, students may find ways to access other materials as well. We believe that the benefits to students from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. But ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the Luverne Public Schools support and respect each family's right to decide whether or not to apply for access.

District Internet and E-Mail Rules

Students are responsible for appropriate behavior on school computer networks just as they are in a classroom or a school hallway. Communications on the network are often public in nature. General school rules for behavior and communications apply.

The network is provided for students to conduct research and communicate with others. Access to network services is given to students who agree to act in a considerate and responsible manner. Parent permission is required. Access is a privilege – not a right. Access entails responsibility. Unethical and unacceptable behavior is just cause for taking disciplinary action, revoking information network access privileges, and/or initiating legal action for any activity through which an individual participates.

Individual users of the district computer networks are responsible for their behavior and communications over those networks. It is presumed that users will comply with district standards and will honor the agreements they have signed. Beyond the clarification of such standards, the district is not responsible for restricting, monitoring or controlling the communications of individuals utilizing the network.

Network storage areas may be treated like school lockers. Network administrators may review files and communications to maintain system integrity and insure that users are using the system responsibly. Users should not expect that files stored on district servers will always be private. Within reason, freedom of speech and access to information will be honored. During school, teachers of younger students will guide them toward appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio, and other potentially offensive media.

As outline in Board policy and procedures on student rights and responsibilities, copies of which are available in school offices, the following are not permitted:

1. Sending, receiving or displaying offensive messages or pictures;
2. Using obscene language;
3. Harassing, insulting or attacking others;
4. Damaging computers, computer systems or computer networks;
5. Violating copyright laws;
6. Using others' passwords;
7. Trespassing in other's folders, work or files;
8. Intentionally wasting limited resources;
9. Employing the network for commercial purposes;
10. Stealing data, equipment or intellectual property;
11. Invading the privacy of individuals;
12. Posting anonymous messages; and,
13. Violating any policy of the Luverne Public Schools.

Violations may result in a loss of access as well as other disciplinary or legal action.

DATE OF ADOPTION:

REVISED:

AUTHORITY FOR POLICY:

February 8, 1996

April 22, 2010
April 28, 2016

Board of Education

STUDENT PERSONNEL
Series 500

Policy Title: INTERNET/TECHNOLOGY USE AGREEMENT

Code No. 524.2

INTERNET/TECHNOLOGY USE AGREEMENT

STUDENT:

I have read and do understand the School District policies relating to acceptable use of technology and agree to abide by them. I further understand that any violation of the policies above is unethical and may constitute a violation of law. Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be taken.

User's Full Name (Please Print): _____ Grade: _____

User's Signature: _____ Date: _____

PARENT OR GUARDIAN:

As the parent or guardian of this student, I have read the School District policies relating to acceptable use of the Internet. I understand that this access is designed for educational purposes. The School District has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the School District to restrict access to all controversial materials and I will not hold the School District or its employees or agents responsible for materials acquired on the Internet. Further, I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give permission to issue an account for my child and certify the information contained on this form is correct.

Parent or Guardian's Name (Please Print): _____

Parent or Guardian's Signature: _____

Date: _____

DATE OF ADOPTION:

February 8, 1996

REVISED:

March 8, 2001
April 22, 2010
April 28, 2016

AUTHORITY FOR POLICY:

Board of Education