

ELECTRONIC COMMUNICATION SYSTEM POLICY

A. PURPOSE

1. Colby School district is providing employees and students with access to the district's electronic communication system, which includes Internet access. This policy pertains to all users of District technology.
2. The district's technology has an educational purpose. The purpose of the technology is to assist in preparing students for success in life and work in the 21st century by providing them with electronic access to a wide range of information and the ability to communicate with people from throughout the world. Additionally, the technology will be used to increase district intracommunication, enhance productivity, and assist district employees in upgrading their skills through greater exchange of information with their peers. The district technology will also assist the district in sharing information with the local community, including parents, social service agencies, government agencies, and businesses.
3. Users may not use the district technology for commercial purposes, defined as offering or providing goods or services or purchasing goods or services for personal use.
4. Users may not use the network for political lobbying. District employees and students may use the technology to communicate with their elected representatives and to express their opinion on political issues.
5. The term "educational purpose" includes use of the system for classroom activities, professional or career development.

B. TECHNICAL SERVICES PROVIDED THROUGH THE ELECTRONIC COMMUNICATION SYSTEM

1. **E-mail.** E-mail will allow employees and students to communicate with people from throughout the world. Users will also be able to subscribe to mail lists to engage in group discussions related to educational subjects.
2. **World Wide Web.** The Web provides access to a wide range of information in the form of text, graphics, photographs, video, and sound, from throughout the world. The Web is a valuable research tool for students and employees.
3. **Groups.** The district will provide access to selected groups that relate to subjects that are appropriate for educational purposes.
4. **Instant Messenger(IM).** IM provides the capability of engaging in "real-time" discussions. The district will provide access to IM only for specifically defined educational activities.

C. ACCESS TO THE SYSTEM

1. The district's Acceptable Use Policy, set forth in **Section K of this policy**, will govern all use of the district technology. Student use of technology will also be governed by the appropriate disciplinary code. Employee use will also be governed by district policy and handbook.
2. **World Wide Web.** All district employees and students will have access to the Web through the district's networked computers. Parents may specifically request that their child(ren) not be provided such access by notifying the building principal in writing.
3. **Individual E-mail Accounts for Students.** Secondary students are provided with individual e-mail accounts starting in 3rd grade. An agreement will be required for an individual e-mail account.

4. **Individual E-mail Accounts for district Employees.** All district employees will be provided with an individual account.
5. **Guest Accounts.** Guests may receive an individual account with the approval of a district administrator if there is a specific, district-related purpose requiring such access.

D. PARENTAL NOTIFICATION AND RESPONSIBILITY

1. The district will notify the parents about the district network and the policies governing its use. Parents must sign an agreement to allow their student to have an individual access.
2. The district Acceptable Use Policy contains restrictions on accessing inappropriate material. There is a wide range of material available on the Internet, some of which may not be fitting with the particular values of the families of the students. It is not practically possible for the district to monitor and enforce a wide range of social values in student use of the Internet. Further, the district recognizes that parents bear primary responsibility for transmitting their particular set of family values to their children. The district will encourage parents to specify to their child(ren) what material is and is not acceptable for their child(ren) to access through the district system.
3. The district will provide guidelines for student safety while using the Internet.

E. DISTRICT LIMITATION OF LIABILITY

The district makes no warranties of any kind, either express or implied, that the functions or the services provided by or through the district system will be error-free or without defect. The district will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. The district is not responsible for the accuracy or quality of the information obtained through or stored on the system. The district will not be responsible for financial obligations arising through the unauthorized use of the system.

F. DUE PROCESS

1. The district will cooperate fully with local, state, or federal officials in any investigation concerning to or relating to any illegal activities conducted through the district system.
2. Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network. If the alleged violation also involves a violation of other provisions of the building disciplinary code, the violation will be handled in accordance with the applicable provision of the building disciplinary code.
3. Employee violations of the district Acceptable Use Policy will be handled in accordance with district policy and handbook.
4. The building principal may terminate the account privileges of a guest user. Guest accounts not active for more than 30 days may be removed, along with the user's files without notice to the user.

G. SEARCH AND SEIZURE

1. System users have no privacy expectation in the contents of their personal files on the district system.
2. Routine maintenance and monitoring of the system may lead to discovery that the user has or is violating the district Acceptable Use Policy, the disciplinary code, or the law.
3. An individual search will be conducted if there is reasonable suspicion that a user has violated the law or the disciplinary code. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation.
4. District employees should be aware that their personal files are discoverable and may be considered public record.

H. COPYRIGHT AND PLAGIARISM

1. District policies on copyright will govern the use of material accessed through the district system. Because the extent of copyright protection of certain works found on the Internet is unclear, employees will make a standard practice of requesting permission from the holder of the work if their use of the material has the potential of being considered an infringement. Teachers will instruct students to respect copyright and to request permission when appropriate.
2. District policies on plagiarism will govern use of material accessed through the district system. Teachers will instruct students in appropriate research and citation practices.

I. ACADEMIC FREEDOM, SELECTION OF MATERIAL, STUDENT RIGHTS TO FREE SPEECH

When using the Internet for class activities, teachers will select material that is appropriate in light of the age of the students and that is relevant to the course objectives. Teachers will preview the materials and sites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the site. Teachers will provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers will assist their students in developing the skills to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.

J. DISTRICT WEB SITE

1. **District Web Site.** The district web site and web pages present information about the district. The Technology Coordinator, or his/her appointee will be designated the Webmaster, responsible for maintaining the district Web site.
2. **Extracurricular Organization Web Pages.** With the approval of the building principal, extracurricular organizations may establish Web pages. The principal will establish a process and criteria for the establishment and posting of material, including pointers to other sites, on these pages. Material presented on the organization Web page must relate specifically to organization activities and will include only student-produced material.

K. DISTRICT ACCEPTABLE USE POLICY

THE FOLLOWING USES OF THE DISTRICT SYSTEM ARE CONSIDERED UNACCEPTABLE:

1. Personal Safety (Restrictions are for students only)
 - a. Users will not post personal contact information about themselves or other people. Personal contact information includes address, telephone, school address, work address, or any other personal information.
 - b. Users will not agree to meet with someone they have met online without their parent's approval and participation.
 - c. Users will promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.
2. Illegal Activities
 - a. Users will not attempt to gain unauthorized access to the district system or to any other computer system through the district System, or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing".

- b. Users will not make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means. These actions are illegal.
 - c. Users will not use the district system to engage in any illegal act.
3. System Security
- a. Users are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a user provide their password to another person.
 - b. Users will immediately notify the system administrator if they have identified a possible security problem. Users will not go looking for security problems, because this may be construed as an illegal attempt to gain access.
4. Inappropriate Language
- a. Restrictions against Inappropriate Language apply to public messages, private messages, and material posted on Web pages.
 - b. Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
 - c. Users will not post information that, if acted upon, could cause damage or a danger of disruption.
 - d. Users will not engage in personal attacks, including prejudicial or discriminatory attacks.
 - e. Users will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending them messages, they must stop.
 - f. Users will not knowingly or recklessly post false or defamatory information about a person or organization.
5. Inappropriate Access to Material
- a. Users will not use the district system to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature).
 - b. If a user inadvertently accesses such information, they should immediately disclose the inadvertent access in a manner specified by their school. This will protect users against an allegation that they have intentionally violated the Acceptable Use Policy.
6. Respecting Resource Limits
- a. Users will use the system only for educational and professional or career development activities.
 - b. Users will not install files without permission from the system administrator.
 - c. Employees are allowed no more than 5 GB of network storage, unless specifically approved by administration.
 - d. Students are allowed no more than 1 GB of network storage, unless specifically approved by an administrator.