



District employees under appropriate circumstances, may have the need to view electronic mail messages. It is also possible that others may view mail messages inadvertently, since there is no guarantee of privacy for an electronic mail message. If confidentiality is a priority, alternative methods of communication should be considered.

Guidelines for System Users

**System Users** (district employees, Board members, students, and other appropriate affiliates) are responsible for:

1. Understanding, agreeing to, and complying with all security policies governing district computer and network resources and with all federal, state and local laws applicable to the use of computer facilities, electronically encoded data and computer software.
2. District employees and Board members of the Bellefonte Area School District are advised to use only the official e-mail address as issued by the district when conducting district business.
3. Safeguarding passwords and/or other sensitive access control information related to their own accounts or network access. Such information must not be transmitted to, shared with, or divulged to others. Similarly, system users must recognize the sensitivity of all other passwords and computer or network access information in any form, and must not use, copy, transmit, share, or divulge such information. Any attempt to conduct such actions by a system user is a violation of this policy.
4. Taking reasonable precautions, including personal password maintenance and file protection measures, to prevent unauthorized use of their accounts, programs or data by others.
5. Ensuring accounts or computer and network access privileges are restricted to their own use only. System users must not share their accounts, nor grant accounts to others nor otherwise extend their own authorized computer and network access privileges to others.
6. Using accounts or network access only for the purposes for which they were authorized and only for district-related activities. Use of accounts or network access to conduct a personal or commercial enterprise, or to promote or advertise a personal commercial enterprise is prohibited. Transmitting or making accessible offensive, obscene or harassing materials, and transmitting or making

accessible chain letters, etc, are prohibited. Unauthorized mass electronic mailings and newsgroups are prohibited. The intentional or negligent deletion or alteration of information or data of others, intentional or negligent misuse of system resources, intentionally or negligently introducing or spreading computer viruses, and permitting misuse of system resources by others are prohibited.

7. Representing themselves truthfully in all forms of electronic communication. System users must not misrepresent themselves as others in electronic communications.
8. Respecting the privacy of electronic communication. System users must not obtain nor attempt to obtain any electronic communication or information not intended for them.

Guidelines for System Administrator

**System administrator.** Unless otherwise stated, system administrators have the same responsibilities as system users. However, because of their position, system administrators have additional responsibilities and privileges for specific systems or networks. For systems which they directly administer, system administrators are responsible for:

1. Preparing and maintaining security procedures that implement district security policies that address such details as access control, backup and disaster recovery mechanisms and continuous operation in case of power outages.
2. Taking reasonable precautions to guard against corruption, compromise or destruction of computer and network resources. Reasonable precautions for system administrators exceed those authorized for system users. System administrators may also intercept or inspect information en route through a network, under appropriate circumstances.
3. Treating the files of system users as private. It is recognized that a system administrator may have incidental contact with system user files, including electronic mail, in the course of his or her duties. The contents of such files must be kept private. Deliberate access to system user files is authorized only in the event of a suspected security breach, if essential to maintain the system(s) or network(s) for which the system administrator has direct administrative responsibility, or if requested by or coordinated with the system user.
4. Ensuring that district network (e-mail) addresses are assigned to only those affiliated with the operation of Bellefonte Area School District.

5. Limiting access to root or privileged supervisory accounts. In general, only system administrators should have access to such accounts. System users should generally not be given unrestricted access to root or privilege supervisory accounts. As with all accounts, authorization for root or privileged supervisory accounts must be approved in accordance with this policy.

Group E-Mail

Acceptable use of group e-mail to communicate district business to employees, Board members, students or other affiliates of the Bellefonte Area School District is set forth below:

1. The district may, as needed, use group e-mail to communicate with all employees, Board members, students, or other affiliates of the district (or subsets of them) on matters of district business that require immediate notification or that are of a sufficient level of importance to warrant special attention.
2. District personnel may elect to use group e-mail to communicate with students or parents in regard to information of educational value and/or school assignments or programming.
3. The use of any such group e-mails must be approved by the immediate supervisor or should be limited to those matters that affect the majority of the defined group.