

E-Mail, Internet, and Technology Issues

Things You Should Know

1. Read your district's Acceptable Use Policy (AUP), abide by it, and reread it once or twice a year.
2. Assume you have **no** privacy regarding e-mail you send and receive, Internet sites visited, or even computer work done offline on your employer-sponsored system. For more information on privacy see www.epic.org/privacy/ and www.cdt.org/privacy/ .
3. If you have questions about security/privacy issues related to the use of school computers, ask for proper training.
4. Do not give away your password or let others see your password. Change your password often. If you do not have password capabilities, you need to insist on getting them. Your computer should not remain logged-on if you are going to be leaving the room for **any** period of time.
5. An experienced investigator can often access a “deleted” computer file, including deleted e-mail.
6. There is a trail on the computer you are using showing what Internet sites you have accessed. This history is stored permanently on the computer server.
7. If you become aware of inappropriate use of computers, the Internet, or e-mail by students, **immediately** report it to the building supervisor. Keep a record of your report to the supervisor and/or technology coordinator.
8. Be aware that some of the newer software now available allows district network administrators to monitor every keystroke on a computer. This not only leaves e-mail and Internet usage open to scrutiny, but would also allow a district to read every document prepared on a district computer as well. No one should consider anything done on a school computer to be private!
9. All of these recommendations also apply to school-owned laptops that may travel or are able to be checked out of the building. **You are responsible** for the property if it is in your possession.
10. It is recommended that employer-owned computers be used for work-related purposes only—**not** for personal use such as checkbook balancing, making online purchases, game playing, online auction monitoring, etc.
11. Do not save anything in the “Favorites” section of your computer unless it is specifically related to education, curriculum, or professional organizations.



Think Before You Click!

New Cautions!!

With many districts publishing staff e-mail addresses on their Web sites, some new situations have occurred.

Responding to Parental E-mails

1. Remember to be aware of the perceived tone, appropriate word usage, and emotion used when responding to parental e-mails. This is also true when corresponding with other staff members. E-mails may easily be misinterpreted.
2. Don't create a paper trail that could possibly be used against you.
3. It may be better to arrange a time to meet with the parent about the student rather than corresponding via e-mail.
4. ***Do not*** exchange e-mail jokes with parents. If they send them to you, ask them to stop. Refer to your district's Acceptable Use Policy.

Opening E-mails from Unknown Senders

1. When in doubt about the source of an e-mail, ***do not*** open it. Some systems have preview capabilities for e-mails. Utilize that option if it's available.
2. If an e-mail from an unknown sender is opened accidentally, close it immediately and report to your technology coordinator in your district that you are receiving unsolicited e-mails.
3. ***Do not*** open attachments from unknown senders. People have lost their jobs because they opened inappropriate attachments on school-owned equipment.

Remember employer owned computers should be used for work related purposes only.

ISEA Great Education.
It's An Iowa Basic.

Iowa State Education Association
777 Third Street
Des Moines, IA 50309

Reminder—e-mail is a public record. School e-mail constitutes a public record!

Points to consider:

1. E-mail is analogous to regular mail, not to phone calls. Therefore, any e-mail sent or received on a publicly owned computer, such as a school district computer, is a public record.
2. Any e-mail sent *or received* on a school district e-mail account—even if accessed via one’s personal computer—is a public record. Retrieving and responding to “LakeWobegon.k12.ia.us” e-mail at home does **not** change the fact that the e-mail is a public record.
3. Start with the reality that **all** e-mail is a public record. Some items within an e-mail may legally be able to be expunged as “confidential.” An individual district employee shall not make this determination on his/her own. (For example, the name of a specific student usually, but not always, may be kept confidential. If necessary to use a student’s name in e-mail, consider using first name and initial of last name [“Carol G.”].)
4. The public can access public records. There are search engines by which e-mail can be searched by topic or keyword. Keep this in mind when composing an e-mail message. Avoid any comments you would not want attributed to you, whether they are derogatory, off-color, or subject to misinterpretation.
5. Deleting an e-mail from one’s computer does not destroy the record. Deleted e-mail is still a public record, and may be retrieved.
6. The district’s e-mail accounts are property of the school district. Such accounts are not to be used for personal business or non-incidentual personal correspondence.
7. An employee’s password to access the account should never be given to anyone who has no legitimate need for it. If the superintendent or building principal gives approval for a password to be given to a co-worker it should be for a specific purpose and length of time.



Iowa State Education Association
777 Third Street
Des Moines, IA 50309