



Recommended security manuals for school districts are about 200 pages long. Here are the most critical things, as a teacher in Mankato Area Public Schools, you need to know and practice – in two pages. Please read them carefully.

An increasing amount of critical, confidential data is transmitted and stored electronically in our district. Despite its intangible nature, digital records, communications, and intellectual property, whether owned by the school or you as a professional, is as valuable and important as physical property. Safeguards to protect it are essential and using them is a professional obligation.

High security and high convenience are incompatible. Our district attempts to achieve a sensible balance, placing a high degree of faith in the professionalism of our staff, rather than technological fixes to insure data security. So far, this has worked well.

Passwords

As a teacher in ISD77, you have the responsibility of a variety of passwords including those for SASIxp, Classxp, the Novell network, your e-mail/YODA accounts, progress reports, grade book programs, your screensaver, and your voice mail. All passwords, except for those that are intentionally shared by all staff (Novell, Accelerated Reader, SPED, etc.), should:

- Be unique for each application.
- Be changed on a regular, frequent basis.
- Be composed of both letters and numbers for highest security.
- Be composed of a string of characters not found in a dictionary.
- Be kept in a secure place if written down.
- Never be given to anyone else, especially students
- Never be given to a tech support person who is unknown to you.

Treat passwords with the same care you would a paper grade book, the key to your classroom, or code to your ATM card.

Back-ups

It is *your* responsibility to maintain at least one back-up copy of your grade book data and your self-created school documents (word processing files, presentations, etc.) You should also regularly create a back-up copy of your stored e-mail messages, e-mail address book, calendar, and to-do list.

The district provides online file space on the YODA server for you to do this. You may also choose to use writeable CD-ROM or DVD disks to create copies of your files if your computer is equipped with a writeable CD or DVD drive. These back-up disks should be kept in a secure place, preferably not in your school building.

The district is responsible of creating back-ups of data from district-wide applications (SASIxp, YODA folders, e-mail stored on the server, etc.) but you must create back-ups of your own files. We recommend backing up all files on at least a monthly basis; more often if you are working on a critical project. You need to ask yourself, “What would I lose if my computer’s hard drive were to die right now?”

Viruses

Computer viruses (as well as worms and Trojan horses) are small pieces of computer code that may have the ability to destroy data on your computer or on computer networks. Needless to say, our district takes extreme precautions to protect our computer users from these programs that are spread as e-mail attachments, hidden in programs downloaded from Internet websites, and as macros in word processing and other documents. While our firewall (a computerized filter that screens all data coming into the district) and our spam filter catches many of viruses, new ones are being constantly created and no filter is perfect. Our district to date has been less susceptible to viruses since the majority are written to hurt Windows computers, but viruses also are written for the Macintosh operating system with OSX becoming an increasingly popular target.

As a teacher, you can minimize your exposure to viruses by:

- Never opening an attachment you were not expecting, even from someone known to you. (E-mail addresses can be spoofed.)
- Never download programs from unknown sources on the Internet (or let your children download them).
- Turn the “macro” feature off or turn “macro security” on in word processing and spreadsheet programs.
- Scan your computer regularly using a virus protection program, especially if you have a laptop or desktop computer you use both at home and at school.

Data Privacy

The protection of the privacy of our students is a professional responsibility. This means knowing the laws, district policies and building guidelines about what student information can be shared and with whom. Increasingly this also means indirectly protecting student records and personal information by following the password guidelines listed above. Under no circumstances should library records be displayed that link the student name to specific titles that the student may have used.

We recommend that you use a screen-saver that automatically starts after a short period of inactivity on the computer in your classroom so that screen contents are not easily viewed when you are away from your desk. For added security, a password to quit the screen saver should be set.

Parental permission forms need to be completed prior to posting photographs or student work on the school's website. No students' last names, e-mail addresses, or other identifying information should appear on the school website. Readers wishing to comment on student work that may appear on the district website should do so through a teacher and his/her e-mail account.

Students need to recognize that school provided e-mail accounts, file storage space (YODA, Profile), and login and usage logs may be viewed if necessary. Our district Internet Acceptable Use Policy (524) <www.isd77.k12.mn.us/district/isd77policies/524.pdf> VIII.A states: "Users should expect only limited privacy in the contents of personal files on the school district system." To date, we have only had to exercise the right to view student files when there has been suspicion of wrong doing, rather than employing a continuously running monitoring program. We hope to continue the "only as needed" approach.

Personal Privacy

As e-mail and Internet users, teachers also need to follow guidelines to protect their personal data and privacy. As district employees, we are subject to the same Acceptable Use Policy as are our students, including the "limited privacy" rule. As with students, we only use the "only as needed" approach to viewing staff e-mail and files.

If you use the Internet to purchase goods, sign-up for newsletters, or complete forms or surveys, you will be asked for personal information. Do so at your own risk. Some guidelines:

- Never give your social security number over the Internet. Be very careful to whom you supply your telephone number, e-mail address, mailing address, and other personal information.
- When making a purchase using a credit card on the Internet, make sure the site is reputable and "secure." A secure site's address will begin with *https* rather than simply *http*.
- Limit the "cookies" your Internet browser will accept.
- Maintain two e-mail addresses: one that is used only for business or with those people you know; one for commercial transactions, surveys, etc. The second e-mail address can be a free account from a provider such as Yahoo and can be easily changed if too much spam is being sent to your account.
- When using a Windows computer, regularly run a "spyware" detection program such as the free SpyBot to detect and eliminate hidden programs on your computer.

Hardware Security

Computers and other hardware can also be stolen and damaged through both carelessness and maliciousness.

- Computers should be on a firm surface, well away from desk and table edges to prevent them from being accidentally pushed off.
- Computer cords and cables should be in molding, raceways or cable trays to prevent damage both to the computer and anyone who might trip over them.
- If your computer is a laptop, use a security cable to lock it to your desk if it is left unattended.
- All hardware needs to be purchased through District Media and Technology Services so it can be inventoried and engraved with a school ID.
- If you use your school computer at home or take it to meetings or conferences, be sure your homeowners' insurance covers it if lost or damaged. Take special precautions at airports (especially at security), hotels and in meetings to make sure your computer is not left unattended. Most hotels will provide an in-room safe or a secure area at the desk where you can safely store a laptop computer.
- Under no circumstances should you open (or attempt to open) your computer's case. Touching the wrong gizmo may not only hurt the computer, it may seriously damage you. Let a district technician handle any repairs that require the case to be opened.