CONFIDENTIAL

The ABCs of Privacy Practices for Educators

At Alpha High School, the principal's personal digital assistant was lost during a basketball game. The PDA contained emergency contact information about every student. The business manager at Beta School District had a flash drive with employee financial information stolen. The IT director at Delta School District just discovered that a laptop with unlisted student telephone numbers was compromised. At Gamma School District, the psychologist's records with confidential information and personal student information were accidentally posted on the school's public Web site for at least four months. Could these things happen in your school district?

Over the last year, the number of reported cases of confidential information lost because of stolen laptops, lost USB flash drives, misplaced PDAs, and simple human error has significantly increased. These trends have school districts concerned with issues of violating private information. Laws such as the Family Educational Rights and Privacy Act (FERPA, 1974) and the Child Online Protection Act (COPA, 1998) are not new, but the proliferation of technology makes managing privacy more complicated than it was in the past.

This article addresses essential practices school administrators and teachers should consider for preserving and protecting the information they handle daily. Welcome to the ABCs of privacy practices.

Copyright © 2007, ISTE (International Society for Technology in Education), 1.800.336.5191 (U.S. & Canada) or 1.541.302.3777 (Int'l), iste@iste.org, www.iste.org. All rights reserved.

By Melissa J. Dark, Clewin McPherson, and Joanne Troutner

Asset Identification and Classification

The asset you are trying to protect is private information. Start by identifying the details of what private information needs to be protected. Make a list of the specific pieces of information. Examples might include student health information, free and reduced lunch lists, as well as grades. Think about a typical student registration scenario and the following questions:

- What personally identifiable information does the school district collect?
- Why is the information collected?
- How is this information gathered and stored?
- Who has access to this information and how is it shared?

The next step is classification, which is the process of applying confidentiality requirements to all information. Look at the list of information you created by answering the questions above and mentally walking through student registration. If the information needs to be kept confidential, then it should be marked with a "C." Asset identification and classification is the essential first step to lay the groundwork for deciding what needs to be protected. Once you know *what* needs to be protected, you can begin thinking about *how* to protect it.

Building Privacy Policies

The next step is to develop a privacy policy. A privacy policy is a written statement that articulates how an organization handles the personally identifiable and private information it gathers and uses. The policy should be developed based on two things: (1) answers to the information identification questions and (2) confidentiality requirements (See Table 1 below for an example.)

The privacy policy sanctions allowable uses and thereby delimits what is not allowable. Once this step has been completed, you can select technologies to facilitate allowable uses and prevent unallowable uses. It is important to understand what a technology will and won't do for you in helping protect privacy. This knowledge is crucial for completing the "C" in privacy practices.

Choosing Technologies that Enforce Policies

Though the policies address the types of protection required for information in your school or district, they do not address specific technologies available to protect privacy. Generally speaking, the most effective tools for privacy protection are authentication, access control, and cryptography. Here is a concise look at these options.

Guidelines for Selecting a Good Password

1. More than eight characters in length. Short passwords are easier to crack than long passwords.
2. Combine letters, numbers, and symbols (as allowed), but not:
   - sequential or repeating combinations, such as 12345678, 22222222, abcdefgh, or adjacent letters on your keyboard
   - common words with letters replaced by numbers or symbols, such as MyL0&1n or P@ssw0rd
3. Easy for you to remember and difficult for others to guess, but not:
   - your login name, your spouse's name, or your birthday.
   - words found in the dictionary, in any language. Hackers use sophisticated tools that can rapidly guess passwords based on words in the dictionary, in a variety of languages, and using words spelled backwards.
   - hard-to-remember. Random combinations of letters, numbers, and symbols that must be written down to be remembered, can be misplaced or found by others and used.

TABLE 1

Basis for Developing Privacy Policy

Factors	Type of information collected	People responsible for collecting and storing information	How information will be used	How information will be stored	How disclosure would affect organization
Example	Student names, Social Security Numbers (SSNs), IEPs, test scores, medical records	Teachers, Administrators	Medical information used by nurse; test scores transmitted to a state office	Test scores on network drives, contact information on LAN, emergency contact on PDAs	SSNs have high confidentiality rating; names have lower confidentiality rating

FOLDER©ISTOCKPHOTO.COM/ZCW26 NOTE©ISTOCKPHOTO.COM/PANNONIA

Copyright © 2007, ISTE (International Society for Technology in Education), 1.800.336.5191 (U.S. & Canada) or 1.541.302.3777 (Int'l), iste@iste.org, www.iste.org. All rights reserved.

Creating a Password for Word or Excel Files

- In Microsoft Word or Excel, click on File, then Save As.
- Click on Tools in the upper right corner of the file save dialog box.
- Click on General Options (Excel) or Security Options (Word).
- Enter a password in the box next to Password to open if you wish the file to be completely inaccessible without the password. (You can click on the Advanced button next to the password box to choose a higher level of encryption that is even harder to break into.)
- Enter a password in the box next to Password to modify if it is OK for others to open the file, but you want to restrict who can make changes to the file.
- Click on OK to close the box.
- Select a name and location for your file and click Save.

Authentication & Access Controls: Authentication determines who gets into a specified system (who can log into a network), while access control determines who accesses resources and files. Access control can be provided by the operating system, the network operating system, the database management system, and/or other applications. Access control will verify the identity of the user and then allow or deny access to specific resources or files according to the access control list, which specifies which users have access to what information and resources.

Passwords: Probably the most common and most prolific form of information protection used today are passwords. Everyone has at least one for access to something (e.g., e-mail, bank account, computer access). Passwords are a form of authentication in which users verify their identities by showing they know specific secrets—the passwords. (See Guidelines for Selecting a good password on page 25.)

Passwords can be used in today's Windows environment to protect files from unauthorized access. If your school district allows teachers to store private information on a laptop or thumb drive, then including a requirement in the privacy policy about using passwords to protect those files is a good idea. (See Creating a Password for Word or Excel Files on this page.)

Cryptography: This is the amalgamation of two ancient Greek words—*kryptos* (hidden) and *grafein* (writing). The goal of this "hidden writing" is to enhance confidentiality and secrecy. A secret key is used to turn plain text (text that is readable) to cipher-text (text that is scrambled and cannot be understood). Encryption can be done on a file, folder, directory, or drive level. If a file, folder, or drive is encrypted, it can only be opened by the person who has the key to open it.

Windows Operating System: In this operating system (NTFS), files and folders can be encrypted by the operating system. When a folder or a drive is encrypted, every file contained in that folder or drive is also encrypted. For instructions on how to encrypt a folder in Windows, see Encrypting and Decrypting in Windows on this page.

It should be noted that if the file is moved within a NTFS system, the encryption stays. However, it is important to know that the files/folders are decrypted when sent or transferred to non-NTFS systems. This is an example of how the technology can facilitate unallowable uses.

Office Application: It is also possible to encrypt a file, such as a Microsoft Word or Excel file. This is good because the file can be transported via e-mail or other peripherals without the encryption being removed (the encryption would have been removed if encrypted by the operating system). Think about using this tool when you send grade information, IEP, or discipline reports, or data disaggregated by lunch program status via e-mail to anyone. The encryption is done in the same manner as adding a password to the file, except the complexity of the encryption can be modified under the "Advanced" button.

Third-Party Encryption Tools: These tools allow for the encrypting of files and folders, as well as entire drives. Anyone trying to access the encrypted data will have to have the encryption

Encrypting and Decrypting in Windows

To encrypt:

1. Select the folder you want to encrypt.
2. Right-click the file to be encrypted, and then click Properties.
3. Click on the General tab, click Advanced.
4. Click to check the Encrypt contents to secure data check box. If you click the details button, you can specify the encryption algorithm to use.
5. Click OK, and then click OK again. (Under Windows XP encrypted folders are displayed with a GREEN color)

To decrypt:

1. Use Windows Explorer to browse to the location of the encrypted file that you want to decrypt.
2. Right-click the encrypted file, then click Properties.
3. On the General tab, click Advanced.
4. Click to clear the Encrypt contents to secure data check box, click OK, and then click OK again.

Copyright © 2007, ISTE (International Society for Technology in Education), 1.800.336.5191 (U.S. & Canada) or 1.541.302.3777 (Int'l), iste@iste.org, www.iste.org. All rights reserved.

TABLE 2
Appropriate Privacy Technologies

	Authentication/ Passwords	Access Control	OS Directory/ File Encryption	MS-Office Encryption	Third-Party Encryption Tools
Transmit an individual file	■			■	
Specify access to a folder on a shared drive		■			
Store a database on mobile media	■			■	■
Grades stored on the home directory of a teacher		■	■		
Grades stored on Web-based SIS for access by teachers and parents		■			
Homeroom schedule stored on a portable device (e.g., flash drive or PDA)	■			■	
E-mail test scores to state	■			■	
Move student numbers from one building to another	■			■	
Store test scores with STN numbers on the hard drive	■	■		■	■
Report discipline information to the state for required reports via e-mail	■			■	

tool software and the key. Some third-party encryption tools include:

- To encrypt entire hard drive:
  - PGPdisk
  - SafeBoot
  - Scramdisk
  - TrueCrypt
  - PointSec

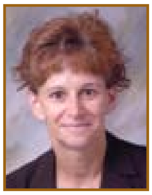
- To encrypt specific folders or files:
  - Crypto Kong
  - Encryptionizer (Windows): Can also be used to encrypt entire databases and servers
  - Icon Lock-iT
  - Pretty Good Privacy (PGP)

Putting It Together

The technologies you choose should be capable of enforcing your privacy policies with regard to the information you are trying to protect and where that information is stored. Information can be stored on a local hard drive, a network drive, a shared drive, a Web site, a flash/thumb drive, a PDA, a portable USB hard drive, a laptop, or a disk (e.g., CD, DVD, Zip). Table 2 shows which technologies might be more appropriate based on the storage medium to protect the confidentiality of the data.

Closing Words

Data privacy is important to any school. The problem is vast but manageable. To get started, begin by identifying the information that is confidential within your school, organization, or district. Follow the ABCs, and the information you have stored on your students can be protected. For more information, visit the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University: http://www.cerias.purdue.edu/education/k-12/securing_k12/.



Dr. Melissa Dark works in the area of information security, with a focus on risk assessment, risk management, and policies in various industry sectors, including education, manufacturing, and government.

Clewin McPherson holds an MS with a focus on Information Security from Purdue University. His research interests include privacy and security issues and their application in industry.

Joanne Troutner is the Director of Media & Technology for the Tippecanoe School Corporation. She writes a regular Internet Resource column for Teacher Librarian, *and owns Creative Computer Enterprises, a consulting firm.*

www.iste.org/LL

Copyright © 2007, ISTE (International Society for Technology in Education), 1.800.336.5191 (U.S. & Canada) or 1.541.302.3777 (Int'l), iste@iste.org, www.iste.org. All rights reserved.