

By The Book

Risk Management Information for Private and Charter Schools from The Hartford and Bolton & Company

WITH AN ESTABLISHED INTERNET USE POLICY IN PLACE, AND WITH CAREFUL MONITORING AND SAFEGUARDING TECHNOLOGY, YOU CAN DEVELOP AN ENVIRONMENT THAT ALLOWS ACCESS TO THE INTERNET'S RICH EDUCATIONAL STOREHOUSE, YET MINIMIZES POSSIBLE DANGERS FOR YOUR SCHOOL, STUDENTS AND STAFF.

The Internet, Your Students and You

A tremendous information resource, the Internet has become the preferred research tool for many students. And with the use of personal computers at home so prevalent, it's no wonder that many children learn how to access the Internet before they reach kindergarten.

Unfortunately, there are risks associated with using the Internet – for students, staff and your school. The Internet provides a gateway to information and temptation that can lead to costly, injurious or even deadly consequences.

Denying your students and staff access to the Internet's capabilities is not an option. But you can take steps to better protect your school. This issue of *By The Book* explores possible dangers of the Internet and suggests ways that your school can minimize their impact.

Protecting Your School

Liability – a Serious Risk

One of the most important points to consider about the use of the Internet is liability for your school. What if a staff member or a student uses your facilities to spread a virus, initiate a “spam” attack, or commit a “cyber crime”? What if your students download copyrighted materials, such as music or movies?

Even innocent activities have hidden dangers. Students and teachers who use instant messaging, file sharing, online chat or other peer-to-peer applications can unknowingly put themselves and their schools in jeopardy. Depending on the circumstances, your school could be held liable for the acts – or the results of the acts – of your staff or students, especially if you have not used commonly available safeguards.

Fortunately, there are steps that your school can take that allow students access to the Internet for learning, while helping to safeguard them from undesirable Web sites.

Step 1. Prepare an Internet Use Policy

One of the first steps you can take to help safeguard your school is to develop an Internet Use Policy. This policy should contain guidelines for the proper use of your school's computer network and the Internet, and it should clearly state that the guidelines apply to *anyone* who uses the Internet on your school property, including all staff and students.

When you develop your school's Internet Use Policy, be sure to:

- **State your objective.** Here's an example:
To help safeguard ABC School students and staff when they access the Internet, we created this Internet Use Policy. The policy will serve to inform school staff, students, parents and guardians about the proper – and improper – use of the school's computer network and the Internet on school premises.



BOLTON & Company
INSURANCE BROKERS
& EMPLOYEE BENEFITS CONSULTANTS
...an Assurex Partner





- **Explain the purpose and importance of your school's computer network and Internet access**, i.e., they should be used strictly for school-related educational purposes.
- **Define the rules for proper use – and the penalties for improper use – of the school's computer network and the Internet.** The rules should include your school's provisions for dealing with network etiquette, vandalism and harassment, copyright and plagiarism, and downloading of music, etc.

Make it clear that failure to adhere to these rules may subject users to warnings, usage restrictions, disciplinary actions, or legal proceedings. In addition, you may want to state that access to the school's computers and the Internet is a privilege – not a right.

- **Explain your school's responsibility regarding the computer network, the Internet and privacy.** It's a good idea to include disclaimers that indicate:
 - Although your school does its best to maintain the computer network, it does not guarantee that it will function at all times. In addition, your school provides access to the Internet, but it does not guarantee the accuracy of information found on the Internet.
 - Your school uses filtering software (if you do) but does not guarantee the effectiveness of the filter.
 - Even with the use of logons and passwords, privacy is limited for those who use your computer network to access the Internet.
- **Include any special requirements for using your school's own Web site and for requesting modifications to its content.**
- **Designate school personnel to be responsible for your network and user administration.** Include their names and responsibilities in the policy.

- **Indicate that you will carefully monitor Internet use in your school** (including checking the history of users) and that you will frequently review your school's Internet Use Policy and update it as needed.

Step 2. Choose and Install Filtering Software

This step assumes that you already have a network that is administered appropriately and that has an adequate firewall and virus protection software and hardware. If you use an outside service vendor to host your network, this step applies to them.

Filtering software is by no means foolproof, and choosing one may seem daunting. Although most private schools are not required to comply with

the Children's Internet Protection Act (CIPA), using CIPA-compliant solutions is a good place to start.

This type of software is aimed at complying with CIPA, but many can be modified to meet your school's specific needs. Make sure that the software can be configured to control peer-to-peer applications, such as chat rooms. If you have a Systems' Administrator or a

Network or IT Security person, he or she would be responsible for choosing the software.

Although not specifically endorsed by The Hartford, here are some providers of CIPA-compliant software:

- www.N2H2.com
- www.trillionpartners.com
- www.enclavix.com
- www.vicomsoft.com

Step 3. Publicize and Enforce Your Policy

Communicate to your staff, students and their parents or guardians about your Internet Use Policy and the safeguards you are taking. If any staff member or student violates the policies, make sure you apply the prescribed penalties – consistently, every time.

Protecting Your Students

There is a dark side to the Internet and, despite your best efforts, if students are determined to find it, they will. Consider the following data (2001)

The more control you have over Internet access, the greater protection for your school, staff and students.

from the Cyberspace Research Centre, a British organization:

- One in five British children aged nine to 16 regularly use chat rooms.
- More than half have engaged in sex chat.
- One quarter have received requests to meet face to face.
- One in 10 of these have met face to face.

And, closer to home, 21 percent of the U.S. Internet audience is children between the ages of two and 17 (Nielsen, 9/03). Even more compelling is the following information:

- An estimated 11 million children have access to the Internet. More than half of the nation's classrooms currently have Internet access and those that don't soon will be wired.

The degree to which your attempts are successful in protecting your school and your students will depend in part on how you allow your students to access the Internet.

Levels of Internet Access

The more control you have over Internet access, the greater protection for your school, staff and students. Here are four levels of Internet access. Take a close look and consider what level will work best for your school.

Level 1

If you only allow access to the Internet via school-owned computers that your school controls, you can provide several levels of protection on the individual computers and on the network. This is probably the most effective way to control access and filter content, and it allows you to control where the students access the Internet. A good approach is to have the computers in a common area, such as a classroom or a library. This allows your staff the opportunity to supervise and monitor Internet use.

For boarding schools with dormitories, carefully consider whether or not you will allow students to have personal computers and Internet access in their individual rooms. If you do allow it, make sure students are mature and responsible enough to handle this privilege and inform them that it can be taken away if they abuse it.

Recognizing that this level of security may not be feasible for all schools, there are other ways to control Internet access.

Wireless Services

Many schools are installing wireless networks on their campuses. You should be aware that the security challenges with these types of systems are significantly greater than with wired systems.

For example, consider these potential dangers with wireless services:

- Any stranger within range of your school would have access to the wireless router. Without adequate precautions between the router and your school's servers, any stranger could gain access and cause major disruption.
- Imagine that one of your students goes off campus and uses a "cyber café" wireless service. In doing so, the student makes his or her personal computer vulnerable to more security risks. The student could then carry back to campus any Trojan horse, worm or virus contracted while at the café. Without proper precautions, the undesirable code could then infect the entire school system's network, as well as its users.

If your school has a wireless network, take the following precautions:

1. Obtain the services of an IT security expert who has experience in wireless system security. This is critically important.
2. Specify and verify the software that must be used on student computers.
3. Provide various levels of security on the wireless routers and servers.

Level 2

If you allow a student to access the Internet through your network via their own computer – but you specify and verify the hardware and software – you can gain a reasonable level of control. Make sure that the specified software includes fire-wall, anti-virus and filtering products. In exchange for mandating specific hardware and software, your school probably would have to provide technical support for the student body.

Level 3

If you allow students to access the Internet on their student-owned computers via your school's network – but you do not specify the hardware and software they are using – you are asking for trouble. Even if you have taken significant precautions with the hardware and software on your network, improper or incompatible software on a

student's computer can wreak havoc on your school's computer network.

Level 4

If you allow students to access any Internet Service Provider by dialing on a standard phone system at your school, your network will not be affected. However, you will have no control over how the students use the Internet. This lack of control could subject students to pornography, warez* sites, suicide clubs, and questionable chat rooms. Unfortunately, you won't know about this until it's too late.

* Pronounced "way-riz" or "way-riss," this pirated commercial software has been made available to the public via the Internet. Typically, the pirate has de-activated the copy protection or registration scheme used by the software. It is both illegal to use and distribute. In contrast, shareware and freeware may be freely copied and distributed.

Summary

Your school and your students can benefit from the advantages of the Internet. But it is critical to control Internet access as you would any other tool. There are technologies that can help. Educate your staff and students about the constructive use of the Internet and its dangers.

Managing Your Risk

Since technology is always changing, it's important to frequently review your Internet Use Policy and update it as necessary. The same goes for your software and hardware products. With an established Internet Use Policy in place, and with careful monitoring and safeguarding technology, you can develop an environment that allows access to the Internet's rich educational storehouse, yet minimizes possible dangers for your school, students and staff.

More Protection For Your School

Continue to protect your school, students and staff with The Hartford's insurance program for Private and Charter schools.

To receive The Hartford's *Parent Guide to Managing Internet Access*, receive future issues of *By The Book*, obtain any of our other publications, suggest topics of interest, or learn about the many ways we can work with your school, contact:

Cheryl Bever-McDowell, Account Executive, Private School Practice Group, Bolton & Company
E-mail: cmcdowell@boltonco.com Phone: (626) 535-1428

You'll also find more information about insurance, including tools such as a jargon translator, a risk IQ tester, and a protection match, on the Web at mb.thehartford.com/schoolnews.

By The Book is brought to you by The Hartford.

This document is provided for information purposes only. It is not intended to be a substitute for individual legal counsel or advice on issues discussed within. Readers seeking resolution of specific legal issues or business concerns related to the captioned topics should consult their attorney and/or insurance representative. The Hartford does not endorse the providers of CIPA-compliant software and makes no representations or warranties with respect to the effectiveness of such software. Descriptions with respect to insurance coverages are of a general nature and may vary by company or policy type. Always review the terms of an insurance policy carefully.