Network Policy for Catholic Schools

Technology is an integral component of education in the 21st century. As internet-based resources are becoming more important in the educational setting, access to these resources has to be managed effectively. First, school administration must implement safety procedures to secure the computer network from outside and inside threats, such as viruses and malware.

Second, schools must take steps to prevent inappropriate content from being accessible in our schools through the use of firewalls and monitoring. Lastly, schools must establish clear policies and procedures for student, staff and faculty use of the school's information technologies.

Protecting Against Computer Viruses: Anti-Virus Software

A computer virus is a small software program that spreads from one computer to another, interfering with computer operation. A computer virus may corrupt or delete data on a computer, use an e-mail program to spread the virus to other computers, or even delete everything on the hard disk. Anti-virus software protects your computer and network against viruses by scanning files or your computer's memory for certain patterns that may indicate an infection. The patterns it looks for are based on the signatures, or definitions, of known viruses. Because virus authors are continually releasing new and updated viruses, **it is critical that schools ensure all anti-virus software is kept up to date**.

In addition, hackers work hard to infiltrate computers through bugs and loopholes in popular software. In response, software developers create "patches" to close the existing loopholes, once discovered, and distribute these patches electronically via software updates. For this reason, when updates to Windows or Office applications are suggested, it is important to take the time to download them.

Keep Your Systems Up-to-Date: Automatic Updates

Enable automatic updates on all systems. This will ensure that all updates are applied to your systems when they are released by Microsoft and Apple.

Keeping Informed About New Viruses

Many anti-virus packages include an option to automatically receive updated virus definitions. Because new information is added frequently, it is a good idea to take advantage of this option. Resist believing email chain letters that claim that a well-known anti-virus vendor has recently detected the "worst virus in history" that will destroy your computer's hard drive. These emails are usually hoaxes. You can confirm virus information through your anti-virus vendor or through resources offered by other anti-virus vendors.

Roman Catholic Archdiocese of Boston
66 Brooks Drive, Braintree, MA 02184
Office of Risk Management: www.rcabrisk.org
Catholic Schools Office: www.abcso.org

Firewalls

A firewall is a device or set of devices designed to permit or deny network transmissions. It is used to protect networks from unauthorized access while at the same time permitting legitimate communications to pass. It filters content **based on a set of rules** that can limit the types of sites, the types of data and the time of day that data is accessed. Because the Internet is in a constant state of change, firewall manufacturers are constantly updating the data used to determine and implement these rules.

Firewall Monitoring

A firewall monitoring service provides weekly management reports, which should be reviewed on a regular basis. Any issues that are identified should be addressed immediately. When reviewing these reports, start by asking the following questions:

- Is the firewall being updated and maintained?
- Is network being used during normal school hours or is there activity at other times?
- Are sites being used that are not necessary in a school environment?
- Is there a high percentage of "blocked" Internet requests?
- Are the types of content being blocked a cause for concern?

CIPA and FERPA

Schools should be mindful of regulations related to children, the Internet and education. The Children's Internet Protection Act (CIPA) is a federal law that addresses concerns about access to offensive content over the Internet on school and library computers. The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy of student education records. While Catholic schools may be exempt from certain aspects of these laws, it is good practice to follow the laws nonetheless. For example, CIPA states that schools should have an Internet safety policy that includes technology protection measures, which is both common sense and good practice for all schools.

To learn more about CIPA, go to: http://www.fcc.gov/guides/childrens-internet-protection-act

To learn more about FERPA, go to: http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Establishing Clear Policies and Procedures for Students, Staff and Faculty

In the context of school settings, the Internet should be used as an educational tool and not for any other purpose. If inappropriate material occurs on a school network, it is possible that the school may be held liable for damages resulting from students' access to this material. For this reason, it is mandatory that schools monitor logs of access in order to keep track of the web sites visited by students as a measure to restrict access to materials harmful to minors. Any unauthorized access (including so-called "hacking") and other unlawful activities by minors are prohibited by the Archdiocese of Boston, and student violations of such policies may result in disciplinary action.

For more information on policies and procedures for Internet use by students, staff and faculty, please see,"Cyber Security and Social Networking Policies for Catholic Schools."