Internet Security in Education

Jim Johnson
Director of Instructional & Information Technology Services
Bayh College of Education
Indiana State University
Email: jim.johnson@indstate.edu

Why is Internet Safety Important?

- Protect our students
- Empower our students
- Teach proper and safe online behavior
- Train educators to know the benefits and dangers of Internet tools

Internet Security Policies

- CIPA and E-rate Policy
- Acceptable Use Policy
  - Students
  - Faculty and Staff
- Network and Computer Policy

Children's Internet Protection Act Requirements

- Schools are required to have an Internet safety policy
- Must have technology protection measures. that block or filter Internet access to pictures that are: (a) obscene, (b) child pornography, or (c) harmful to minors
- Schools subject to CIPA are required to adopt and enforce a policy to monitor online activities of minors.
- Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing:
  - (a) access by minors to inappropriate matter on the Internet;
  - (b) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
  - (c) unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
  - (d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and
  - (e) measures restricting minors' access to materials harmful to them.
- Schools and libraries are required to certify that they have their safety policies and technology in place before receiving E-rate funding.
- An authorized person may disable the blocking or filtering measure during any use by an adult to enable access for bona fide research or other lawful purposes.

Acceptable Use Policy

- Each public school corporation in Indiana MUST adopt an Internet Acceptable Use Policy which*:
- 1. Describes general instructional philosophies and strategies to be supported by Internet access in schools.
- 2. Describes the process for governing local Internet system security, user accounts and user privileges.
- 3. Describes sanctions to be taken when violations of the policy occur.
- 4. Makes specific reference to prohibiting the use of school corporation Internet resources/accounts:
  - a. To access, upload, download or distribute pornographic, obscene or sexually explicit material.
  - b. To transmit obscene, abusive or sexually explicit language.
  - c. To violate any local, state or federal statute.
  - d. To vandalize, damage or disable the property of another person or organization.
  - e. To access another person's materials, information or files without the implied or direct permission of that person.
  - f. To violate copyright, or otherwise use another person's intellectual property without their prior approval or proper citation.

* Source: Indiana Department of Education

Acceptable Use Policy (cont.)

- 5. Requires that parents be notified that their students will be using school corporation resources/accounts to access the Internet, and provides parents the option to request alternative activities not requiring Internet access.
- 6. Requires the permission of and supervision by the school's professional staff before a student may use a school account or resource to access the Internet.
- 7. Indicates that the educational value of student Internet access is the joint responsibility of students, parents and employees of the school corporation.
- 8. Makes the school corporation's Internet policies and procedures available for review by all parents, guardians, staff and members of the community.

- B. Each public school corporation in Indiana MUST provide staff and student Internet users guidelines for:
  - 1. Responding to unsolicited on-line contact.
  - 2. Safe-guarding personal information, such as name, address, telephone number, etc.

Acceptable Use Policy Notes

- Lays out what the school expects
- Provides some protection for the school
- Tells students and parents what the Internet rules for the school are
- Explains important of copyright
- Sets the groundwork of cooperation between students, educators, parents and community
- Needs to be signed by students and staff
  - Have a separate but similar policy for staff

Computer Use Guidelines

- Use a document to put the AUP in plain terms
- This is used to give explicit details as to what is appropriate use of the computers, email and communication tools and network storage and usage
- This is where violations can be discussed if any of the policies are broken

Internet Safety Training

- This is a requirement for funding and a good idea anyhow!
- Train everyone!
  - Students, Faculty, Staff, Parents, School Board and General Community
  - Help all stakeholders understand what is out there and no be afraid
- i.Safe program
  - www.isafe.org

i.Safe Internet Safety Program

- Provides videos, curriculum and online training for all stakeholders
- Schools can choose a package to meet their needs
- Very easy to train
- i.Safe E-rate curriculum
- Schools can also piece together their own program

Internet Content Filtering

- Required by law if you receive federal funding
- This can be a good friend or a burden
- Learn if and how your school's filtering product can be customized and best utilized
- Determining categories to block and unblock
- Set policy for how individual web sites get blocked or unblocked
- Get input from students, parents and community as well as teachers & the board

Protecting Your Technology

- Anti-Virus
- Anti-Malware
- SPAM filtering – Good luck!
- Protecting your servers – firewall, etc.
- Computer Lab management
  - Computer imaging – Ghost, Clonezilla
  - Teaching and monitoring software – NetOp Vision 6
  - System protection – Deep Freeze
- Laptops, Netbooks and other mobile tech

Accounts & Passwords

- Try to use easy to remember account names like lastnamefirstname
- Try to link all accounts to the same username and password
- Do not write passwords down and store them under keyboards or on sticky notes attached to the monitor!
- Do not share account information or give students a teacher's password
- Social engineering is the easy way in!
- Don't leave your accounts logged in, especially where students can get access
- Use a strong password policy like minimum of 8 characters including numbers and uppercase letters that are not common words, easily guessed personal information
- Requiring changing passwords every 90-180 days

Social Media Policy

- Something new to blend into teaching is the use of social networking sites
  - Facebook, Twitter, etc.
- We can't ignore it!
- There are educationally appropriate sites
  - Edublogs, Edmodo, Ning, school's own sites
- As part of Internet Safety training help students understand how to protect themselves at home and how to use it at school

Social Media Policy

- Students already know how to use this technology and want to use it
- This provides a great communications platform for parental involvement too
- Schools and Universities are using Facebook for information passing daily
- Again, get input from your stakeholders and test out these sites and education everyone – don't be afraid of opening these types of sites

Web Sites to Visit

- www.facebook.com
- www.edmodo.com
- www.ning.com
- www.edublogs.org
- www.joomla.org
- www.wordpress.com www.wordpress.org
- www.faronics.com
- www.isafe.org
- www.netop.com
- www.symantec.com/norton/ghost
- www.clonezilla.org

Questions?

THANKS FOR COMING!

Jim Johnson
Email: jim.johnson@indstate.edu
Phone: 812-237-2921