

# Cyber Safety

*OSDFS Conference 2009*



Linda Sharp  
Project Director  
CoSN



# What's At Risk?



- Student/Staff
  - Safety
  - Privacy
- Public Support
- Legal Liability



# CIPA



- Schools and libraries subject to CIPA may not receive the discounts offered by the E-rate program unless they certify that they have an Internet safety policy and technology protection measures in place. An Internet safety policy must include technology protection measures to block or filter Internet access to pictures that are:
  - Obscene
  - Child pornography
  - Harmful to minors

(for computers that are accessed by minors)



# CIPA



- Schools and libraries must also certify that, as part of their Internet safety policy, they are educating minors about appropriate online behavior, including cyberbullying awareness and response and interacting with other individuals on social networking sites and in chat rooms.
- Schools subject to CIPA are required to adopt and enforce a policy to monitor online activities of minors.



# CIPA



The Internet safety policy must address the following issues:

- Access by minors to inappropriate matter on the Internet and World Wide Web
- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications



# CIPA



The Internet safety policy must address the following issues:

- Unauthorized access including "hacking" and other unlawful activities by minors online
- Unauthorized disclosure, use, and dissemination of personal information regarding minors
- Measures designed to restrict minors' access to materials harmful to minors





- The “Reality”
  - For 7 hours a day we wrap our students in a very protective cocoon from the cyber world.
  - The remaining 17 hours they operate in the same cyber world as adults.
    - No filtering
    - Limited monitoring
    - Limited knowledge



# Safety vs. Security



- **Safety:** *Individual behavior*
- **Security:** *An organizational responsibility*





- Students need to:
  - Recognize online risks
  - Take action to protect themselves
  - Make informed decisions
  - Exhibit safe behavior
  - Understand legal issues



# Three Strategic Areas



- People
- Policy
- Technology



# Educators



- Understand the laws
- Create/adopt policies
- Coordinated planning and accountability
- Provide professional development
- Involve parents
- Educational Purpose



# Educators



- Understand and follow AUPs
- Advocate for ethical and legal use
- Exhibit good “Netiquette”
- Recognize signs and effects of cyberbullying, cyberstalking, etc





- More than half (52%) don't understand how to ensure a website is secure.
- 75% don't feel comfortable discussing cyber-bullying
- Less than 32% are comfortable giving guidance on how to be safe in an online environment, including social networking and cyber predators



2008 National Cyberethics, Cybersafety, Cybersecurity Baseline Study, <http://www.staysafeonline.org>





- 22% are comfortable teaching about cyber bullying, identity theft and other types of cyber crime
- 23% percent feel prepared to teach students how to protect their personal information online



2008 National Cyberethics, Cybersafety, Cybersecurity Baseline Study, <http://www.staysafeonline.org>



# Parent Education



- Stimulate conversations
- Establish guidelines for home
- Provide advice and guidance to students and parents
- Prevent, detect and intervene if their child is victim

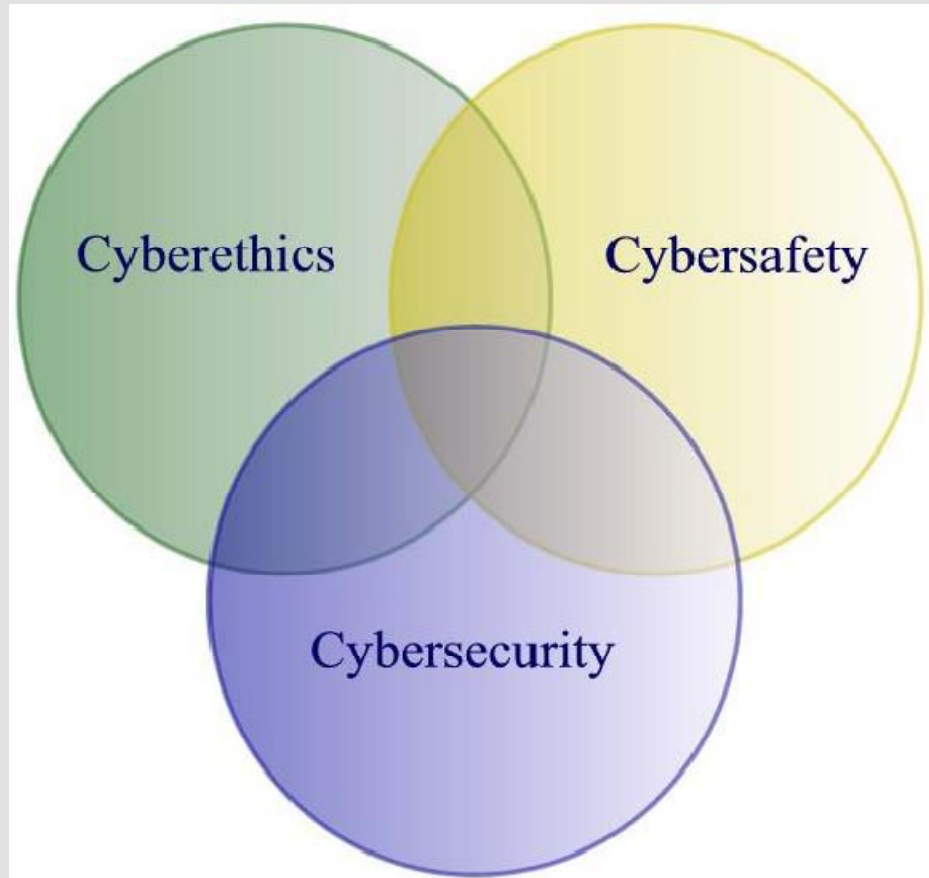


# Focus Areas



- Educators
- Parents
- Students







Linda Sharp

CoSN Project Manager

[linda@cosn.org](mailto:linda@cosn.org)

[www.securedistrict.org](http://www.securedistrict.org)

[www.cosn.org](http://www.cosn.org)



# Sponsors

