

# Privacy Concerns: Best Practices



November 30, 2007

**Joanne Troutner**  
**Creative Computer Enterprises**  
**Lafayette, IN**  
**[troutner@mindspring.com](mailto:troutner@mindspring.com)**  
**[www.jtroutner.com](http://www.jtroutner.com)**

**PURDUE**  
UNIVERSITY.







## FERPA, CIPA, COPA, HIPAA...

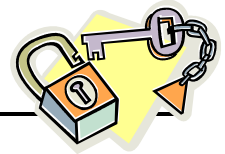
Protecting and defending the growing mountain of critical – and intimate – knowledge about students and staff is not just good academic practice – it’s the law. Or rather, laws. Districts must meet a complex set of federally-mandated obligations to protect data, as outlined below. Each law emphasizes different types of protection; in planning to comply with each law, your district will end up devising a safeguard strategy that blends policy, technology, and administrative practices. (Modified from Steven Miller presentation, NSBA 10/2005)

Law	Law Type	Vulnerability / Threat	Strategic Emphasis	Practices		
				Policy	Technology	Administrative
<b>FERPA</b> Family Education Rights and Privacy Act - 1974	<i>Privacy</i>	<p><i>Twin Vulnerabilities: unauthorized access or disclosure.</i></p> <p><b>Access vulnerabilities:</b></p> <ul style="list-style-type: none"> <li>Confidential data, transmitted over Internet in unencrypted format, is intercepted</li> <li>External intruder hacks in</li> <li>Internal scofflaw steals password or hacks in</li> </ul> <p><b>Disclosure vulnerabilities:</b></p> <ul style="list-style-type: none"> <li>Authorized users fail to follow rules</li> <li>Staff inadvertently reveals protected data in hardcopy format</li> </ul>	<ul style="list-style-type: none"> <li><b>Secure the borders:</b> stop protected information from <b>getting out</b> - and into the wrong hands with regularly updated and maintained firewall, wireless access protections, etc.</li> <li><b>Improve internal network security:</b> Create and enforce authentication and authorization policies and procedures for role-based access to data.</li> <li><b>Encryption:</b> protected data should never be stored or released in an unprotected format. Hardcopy should be in locked cabinets or only given out in sealed envelopes; electronic material should be stored and sent in encrypted format.</li> <li><b>Many players - one playbook:</b> technology won't protect you if authorized staffs don't know the rules about releasing data or leaving logged-in machines unattended. Train and remind everyone about appropriate practices.</li> </ul>	<ul style="list-style-type: none"> <li>Privacy Policies</li> </ul>	<ul style="list-style-type: none"> <li>Encryption for storage and transmission of data</li> <li>Network security</li> <li>Physical security</li> </ul>	<ul style="list-style-type: none"> <li>Educational &amp; Training Awareness Programs</li> </ul>
<b>CIPA</b> Children's Internet Protection Act - 2000	<i>Security</i>	<ul style="list-style-type: none"> <li>Email: Spam</li> <li>Web: pornography, violent or hate sites</li> <li>Other inappropriate content originating outside - or inside - the network</li> </ul>	<ul style="list-style-type: none"> <li><b>All along the watchtower:</b> Reduce the likelihood that inappropriate information will <b>enter</b> your network with appropriately configured filters. In Particular: review spam filtering methodology regularly. However, the law only requires meaningful effort, not perfection, since there is no foolproof technological solution.</li> <li><b>The human element:</b> Be public about the inevitability that some inappropriate material will slip through and train students (and staff) how to deal with it. Make sure everyone knows the district's policies and penalties concerning harassment, use of school resources for inappropriate purposes, etc.</li> </ul>	<ul style="list-style-type: none"> <li>Usage Policies</li> </ul>	<ul style="list-style-type: none"> <li>Email filtering</li> <li>Internet filtering</li> </ul>	<ul style="list-style-type: none"> <li>Educational &amp; Training Awareness Programs</li> <li>Student Online Supervision</li> </ul>
<b>HIPAA</b> Health Insurance Portability and Accountability Act - 1996	<i>Privacy</i>	<ul style="list-style-type: none"> <li>School nurse or athletic department needs health information. Local public health department may request assistance documenting immunization,</li> </ul>	<ul style="list-style-type: none"> <li><b>Get it in writing:</b> A school district can NOT legally be given medical information about a particular person without first receiving HIPAA-required permission. Make sure that parents and staff have given explicit, written permission for you to receive medical data. Once in the district, however, medical info of students falls under FERPA rules.</li> </ul>	<ul style="list-style-type: none"> <li>Privacy Policies</li> <li>Usage Policies</li> </ul>	<ul style="list-style-type: none"> <li>Encryption for storage and transmission of data</li> <li>Network security</li> <li>Physical security</li> </ul>	<ul style="list-style-type: none"> <li>Educational &amp; Training Awareness Programs</li> </ul>
<b>COPA</b> Child Online Protection Act - 1998	<i>Privacy</i>	<ul style="list-style-type: none"> <li>Potentially impacts district web sites or discussion forums that have "open posting" rules.</li> </ul>	<ul style="list-style-type: none"> <li><b>Freedom of Speech:</b> Free speech argument tips a Supreme Court injunction 5-4 (June 2004) against implementation. Stay tuned for changing of the guard.</li> <li><b>Struck down on 3/27/2007</b>—ruling appealed</li> </ul>	<ul style="list-style-type: none"> <li>Privacy Policies</li> </ul>	<ul style="list-style-type: none"> <li>Internet filtering</li> </ul>	<ul style="list-style-type: none"> <li>Educational &amp; Training Awareness Programs</li> </ul>

<b>Information</b>	<b>HD C:/</b>	<b>Web Site</b>	<b>Network Drive H: District Server/</b>	<b>Shared Drives S:/&amp; Collab</b>	<b>Flash/ Thumb Drive</b>	<b>PDA/Palm</b>	<b>Portable USB HD</b>	<b>Disk/CD/Zip Disk</b>
Name/Address								
Unlisted Phone Number								
Student Numbers								
SS Number								
Health Info								
Grades								
Homeroom /Schedule								
Free & Reduced Status								
IEP Info								

<b>Information</b>	<b>HD C:/</b>	<b>Web Site</b>	<b>Network Drive H: District Server/</b>	<b>Shared Drives S:/&amp; Collab</b>	<b>Flash/ Thumb Drive</b>	<b>PDA/Palm</b>	<b>Portable USB HD</b>	<b>Disk/CD/Zip Disk</b>
Attendance								
Emergency Contact Info								
Bus Assignments								
Discipline								
Payroll Info								
Bank Acct Numbers								

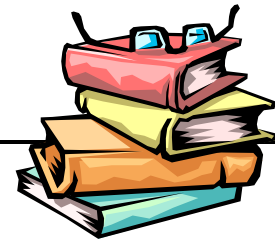
# Security Tools Use



	<b>AU</b>	<b>AC</b>	<b>OSE</b>	<b>MSE</b>	<b>TPE</b>	<b>SSL</b>
Transmit an individual file	<b>X</b>			<b>X</b>		
Specify access to a folder on a shared drive		<b>X</b>				
Store a database of records on mobile media (laptop, PDA, flash drive, etc)	<b>X</b>			<b>X</b>	<b>X</b>	
Grades stored on the home directory of a teacher		<b>X</b>	<b>X</b>			
Grades stored on the web based SIS for access by teachers and parents		<b>X</b>				<b>X</b>
Homeroom schedule stored on a portable device (flash drive / PDA)	<b>X</b>			<b>X</b>		
Transfer STN via email to the state	<b>X</b>			<b>X</b>		
Move STN numbers from one building to another	<b>X</b>			<b>X</b>	<b>X</b>	
Store test scores with STN numbers on the hard drive	<b>X</b>	<b>X</b>		<b>X</b>	<b>X</b>	
Report discipline information to the state for required reports via the web						<b>X</b>
Report discipline information to the state for required reports via email	<b>X</b>			<b>X</b>		
Provide transcript information to colleges and other school districts	<b>X</b>			<b>X</b>		
Share IEPs--confidential individualized education plans for special education students via a shared location on a building network, Internet, between school districts						<b>X</b>

- Authentication (*AU*)
- Access control (*AC*)
- Operating system directory/file encryption (*OSE*)
- MS Office encryption (*MSE*)
- Third-party encryption tools (*TPE*)
- Secure Socket Layer (*SSL*)

# References



## **General references—**

Privacy Workshop for Educators Materials from the NSF funded Privacy Workshops--CERIAS	<a href="http://www.cerias.purdue.edu/education/k-12/securing_k12/">http://www.cerias.purdue.edu/education/k-12/securing_k12/</a>
Electronic Privacy Information Center	<a href="http://www.epic.org/">http://www.epic.org/</a>
Online Privacy Alliance	<a href="http://www.privacyalliance.org/resources/ppguidelines.shtml">http://www.privacyalliance.org/resources/ppguidelines.shtml</a>
Privacy.org	<a href="http://www.privacy.org/">http://www.privacy.org/</a>
The Privacy Place.org	<a href="http://www.theprivacyplace.org">http://www.theprivacyplace.org</a>
The Privacy Rights Clearinghouse	<a href="http://www.privacyrights.org/fs/index.htm#English">http://www.privacyrights.org/fs/index.htm#English</a>
Web Browser Security Settings	<a href="http://www.cert.org/tech_tips/securing_browser">http://www.cert.org/tech_tips/securing_browser</a>
Computer Privacy Annoyances	Dan Tynan ISBN0-596007752
Privacy Lost	David H. Holtzman ISBN 0-7879-8511-2