

# **The IASEP Data Security Protocol for Education**

Copyright © 1999 - 2000 Purdue Research Foundation, Inc. All Rights Reserved.

This is pdf version v. 1 (9/8/00)  
Appendices C and E with references to all fifty states are not included in this pdf  
version. To access Appendix C or E, please view the document online at  
[http://arc.soe.purdue.edu/protocol/home\\_page.htm](http://arc.soe.purdue.edu/protocol/home_page.htm)

This web site constitutes a dynamically changing security protocol. This is only the beginning of its possibilities. It is designed to assist Indiana School Boards, Administrators, and Teachers to implement safe data and information systems. As schools develop policies and encounter changing technological systems, there will be a need for amendments to this document. If school districts would like to share documents that could be used on this site as examples, we would welcome that. **Suggestions, additions, comments, or questions about this protocol should be directed to the webmaster at <securityinfo@purdue.edu>.** Thank you.

The Indiana Assessment System of Education Proficiencies [IASEP] team, along with the Center for Education Research in Information Assurance and Security [CERIAS] at Purdue University, has developed a protocol for policy development for data security for electronically transmitted student assessment data.

The purpose of this protocol is to assist educational organizations that use the IASEP system to protect their valuable information. This site is designed to help policy makers to develop and implement organization-specific original policies whose purposes are to protect and secure access, storage and transmission of student information.

This document is designed as an overall outline of the information protection areas that should be addressed in specific school policies. The chapters include general organizing principles related to specific topics, and Appendices D, E, and G contain samples of policies from Indiana and from other states. The document is sprinkled with links to policies from all over the country that policy makers may view for ideas in generating their own policies. We have also included both federal and state data privacy-related laws. In addition, the bibliography contains links and references to a large number of data security and privacy resources.

This document is intended to be a dynamic, changing instrument that policy makers, teachers, and parents might use to guide them in devising policies and requiring adherence to data privacy and security considerations. As communities complete their data security and privacy policies we would hope that they would be willing to allow us to include them in our sample policies Appendix. And as policy makers address other issues, besides those addressed in these chapters, we would hope that they would share those with us so that we can add those considerations to our chapters. It is this process that will make this a useful dynamic tool for Indiana communities and other communities across the country.

This document is a melding of many resources from federal and state governments, universities, local school districts, and other experts in the field. We have tried to give specific attribution whenever possible. If we have inadvertently missed an attribution, please let us know. We are grateful to all the private and government resources that were available for our use in this document.

## Table of Contents

- Chapters:**
- [1. Introduction](#)
  - [2. General Protocol and Policy Statements](#)
  - [3. Risk Assessment](#)
  - [4. Physical Security Policies](#)
  - [5. Information Security Policies](#)
  - [6. Software Security Policies](#)
  - [7. User Access Security Policies](#)
  - [8. Network and Internet Security Policies](#)
  - [9. Administrative Policies and Procedures](#)
  - [10. Training Protocol](#)

- Appendices:**
- [A. Glossary of Terms](#)
  - [B. Related Federal Laws](#)
  - [C. Related State Laws](#)
  - [D. Related Federal Data Security Policies](#)
  - [E. Related State Data Security Policies](#)
  - [F. Technology Resources](#)
  - [G. Indiana State Requirements and Model Policies](#)
  - [H. Bibliography and Policy Resources](#)

# 1. Introduction

## 1.1 Purpose

The Indiana Assessment System of Education Proficiencies [IASEP] team is currently working with the Center for Education Research in Information Assurance and Security (CERIAS) at Purdue University to develop a prototype for security for electronically transmitted student assessment data. As the IASEP system is distributed across the State, the difficulties with potential PC platform incompatibilities must be addressed.

One solution is to translate the IASEP software to an HTML format for access through the Internet. As we move toward the HTML format for data transmission, it will be critical to create safeguards to ensure the confidentiality and safety of the information that is submitted.

While use of the Internet offers tremendous benefits for the IASEP system, Internet connectivity is dangerous for sites with low security levels.

The Internet suffers from glaring security problems that, if ignored, could have disastrous results for unprepared sites. [The fundamental problem is that the Internet was not designed to be very secure.] Inherent problems with TCP/IP services, the complexity of host configuration, vulnerabilities introduced in the software development process, and a variety of other factors have all contributed to making unprepared sites open to intruder activity and related problems. [NIST at pp. 7-8]

Organizations are, rightly concerned about the security implications of using the Internet:

Will hackers disturb internal systems?

Will valuable organizational data be compromised (changed or read) in transit?

Will the organization be embarrassed? [NIST at p.7]

[And worse yet, will the organization be sued for its lack of security if its system is compromised and confidential data is accessed?]

The purpose of a protocol for security policy development is to assist the educational organizations that use the IASEP system to decide how they are going to protect themselves. This document provides information for policy makers, administrators and school boards, to understand the importance of developing and

implementing organization-specific original policies to protect and secure their organization's data access, storage, and transmission.

A committee consisting of representatives from the Indiana State Department of Education, the IASEP team, and CERIAS has analyzed the system needs and developed corresponding system architectural safeguards. In addition, the same group has been discussing the need for a protocol or policy facilitation document to accompany the IASEP system. It is likely that the IASEP prototype and the protocol for policy development for this system will serve as models for future educational data transmission and storage for many of the evolving electronically-based educational data systems in the State.

This document presents an organizational framework and recommendations for securing information and equipment. It does not presume to dictate local policy, except in the areas where the State of Indiana has already required certain specific policies.

**1.2 General security goals:** The goal of security is to protect information and the system without unnecessarily limiting its utility. At the same time, unauthorized access to critical systems and sensitive information, must be prevented. The purpose of maintaining information in our schools is to help better serve students. In order to do that, the system should not be so secure that authorized users cannot get to the data that they need to do their jobs.

**1.3 Goal of this project:** The goal of this project is to develop a general protocol for the management of all electronic educational data that complies with our state and federal laws. This protocol will contain a variety of resources for educational administrators and teachers.

#### **1.4 Protocol-specific Objectives:**

- 1) Identify current education-related and general data security policies, procedures, guidelines, and standards for review and make these available to IASEP constituents through a protocol document.
- 2) Identify current education-related and general data security state, federal and private laws and regulations for review, and make these available to IASEP constituents through a protocol document.
- 3) Using the laws, policy resources and other data security information collected, develop a protocol document that will assist IASEP constituents to develop data security policies that will affect how data is accessed, entered, stored, transmitted and reported in Indiana.

4) Coordinate with CERIAS, state educational and legal consultants to coordinate with the architectural security work underway with the current IASEP system. Supplement the architectural activities with procedural or policy assistance through a protocol document.

5) Develop a set of schematics to display the information compiled and written so that readers and practitioners can readily visualize and understand how the protocol elements fit together and how they could be used to develop and implement individual school district data security policy plans.

6) Develop a training protocol to disseminate critical information.

**1.5 Intended Audience** -- This protocol is written for school board members, educational administrators, and teachers to assist them to write and implement data security policies for their respective organizations. Every organization is different, so we do not propose specific policies. However, there are enough similarities in organizations and areas of risk that this document will outline the areas that need to be addressed, suggest resources to assist policy-makers, and give examples for consideration.

## **1.6 Major types of policy documents -- Working Definitions**

For purposes of this project, the following terms and their project-specific definitions are being used. Please see Appendix A for additional terms used throughout this document.

**Data or Information** -- In many parts of this document the words "data" and "information" are used interchangeably, although these terms have distinct meanings that will be discussed in later chapters. Data or information refers to records that are directly related to students and maintained by an educational agency or institution or by a party acting for the agency or institution.

<p style="text-align: center;"><b>Type of Document</b></p>	<p style="text-align: center;"><b>Responsible Person or Entity</b></p>
<p><b>Protocol</b> -- a set of recommendations, rules, and laws governing the treatment and formatting of data in an electronic communications system. This includes policy samples and suggestions for overall treatment of data security in individual school districts.</p>	<p><i>This type of document is prepared by persons with statewide perspective to provide overall guidance to policy makers.</i></p>
<p><b>Policy</b> -- Those broad decision making statements made by administrators related to educational data security</p>	<p><i>School boards and school administrators are responsible for the evolution of policies, which provide direction for implementation of more specific measures.</i></p>
<p><b>Security policy</b> -- a collection of statements about the sensitivity of information on a system or LAN, the requirements for how that data must be protected, and the actions to be taken in the event the protection is violated.</p>	<p><i>School boards and school administrators, in conjunction with computer system administrators.</i></p>
<p><b>Standards</b> and <b>guidelines</b> both generally refer to specific technologies and methodologies to be used to secure systems. More specifically, <b>standards</b> refer to the criterion against which the technologies and methodologies are measured.</p> <p><b>Guidelines</b> are guiding principles or courses of action that should be followed when securing systems.</p>	<p><i>School Administrators</i></p>
<p><b>Procedures</b> normally assist in complying with applicable security policies, standards, and guidelines. They are detailed steps to be followed by users, system operations personnel, or others to accomplish particular security-related tasks (e.g., preparing new user accounts and assigning the appropriate privileges).</p>	<p><i>System administrators and individual teachers</i></p>

Some organizations issue overall computer security "manuals," "regulations," "handbooks," or similar documents. These may mix policy, guidelines, standards, and procedures, since they are closely linked. While manuals and regulations can serve as important tools, they are most useful when they clearly distinguish between policy and its implementation (sometimes a difficult process). This promotes flexibility and cost-effectiveness by offering alternative implementation approaches to achieving policy goals.

## **1.7 Methodology, Initial Findings, and Presentation**

The purpose of this section of the data security project is to outline ways to secure IASEP data, hardware, software, network and e-mail components from destruction or corruption. We began by researching federal, state, and private security policies for insight into how to best construct our own document. A web search of private, federal, and state data security laws, regulations, policies, guidelines, and procedures was done. Jennifer Radecki, a part-time graduate research assistant, and Shelly Shinevar, a part-time paralegal student, did the state policy and statutory research, under the direction of Professor Deborah Bennett and the author of the protocol, Candace Elliott Person.

The resources gathered were any policy, protocol, law, guide, document or plan that mentioned or focused on data security in its many forms. As the research progressed, the resources were divided into four categories: data security, physical security, computer/software security, and other (which included network security and e-mail security). The research per state is presented in Appendix C and Appendix E of this document.

General documents, guides and Web sites not affiliated with any state were also collected. These resources can be found in Appendix F and Appendix H. Books and written guides are included for reference. Many of the applicable federal and state laws, regulations and legal procedures pertaining to data security are also summarized in the Appendix B, Appendix D, and Appendix G.

We found that most state Information technology sites had security policies mentioned or slated for creation in the near future. However, the state Department of Education and Educational Technology sites contained very few security policies or plans. Most of the sites did contain links to technology plans, but very few articulated a cohesive system security plan. The focus of most of the technology plans was technology acquisition and set-up and creation of curriculums that would utilize and incorporate technology. Internet Acceptable Use policies and Network Acceptable Use policies,

respectively, were the most prevalent documents found on both the state and education Web sites.

Because we found so few comprehensive security documents on the web, we sent an e-mail letter to the authors of the Web sites researched to request further documentation. Some encouraging responses from the authors of some Web sites gave us additional security material with which to work.

Overall, we found very few education-specific data security policies on the Web. That is not to say that these types of policies are not written. They were just not found on the Web. However, written documents were also not readily shared with us in response to our email request to the Web sites.

There may be several reasons for this finding. First, because of the large push in schools to make the technology available for teachers and students, there has been little time spent on articulating how the technology will be used safely. Secondly, for those educational entities that may have articulated their security policies internally, they may not want them to become public. The reason for this secrecy may be to prevent their systems from being compromised and to preserve the integrity of their systems. A third possibility for finding little data security policies articulated is that educational institutions have not yet had time, or have chosen not to articulate data security policies. This could be because policy formulation can be very time-consuming, and there simply has not been time with the rapid influx of technology. Another reason may be that educational institutions are waiting for direction on their data security formulation.

Whatever the reason for educational institutions not having data security policies in place, this document is designed to assist in that process. Because policy formulation can be very confusing and difficult to perform, it is our intent to make this document and our accompanying web site as user-friendly as possible.

## **1.8 Web Site Development**

We have constructed a web site to disseminate the information gathered to all the constituents involved in the IASEP project. The web site is available to anyone, but especially to the teachers, parents, administrators and staff involved in the IASEP project.

The Web site's design uses a top horizontal table of contents to allow the reader to jump to different sections of the protocol. Movement to the top of the page, to the Purdue home page and to the IASEP are provided through buttons at the bottom of each main chapter page. Each Appendix Index page (i.e. the Appendix C Index) utilizes the same top horizontal table of contents, but has no Purdue or IASEP links. The "daughter" Appendix pages (i.e. the Alabama statutes page within Appendix C) have connections to their respective Index page and to other pages within that Appendix.

This document is a meld of information from all the documents and resources referred in the Appendices. Since this document is intended as a resource manual, we did not want to include extensive amounts of references within the text itself. However, sprinkled throughout the document are we have referred to the major resources from which this document is formed. Those resources are identified either in introductory sentences to a chapter or in bracketed, numbered citations to specific resources.

These citations are linked to Appendix H -- Bibliography & Resources for Internet Security Information.

Draft 5/27/00 v3  
Updated 7/25/00.

## 2. General Protocol & Policy Statements

### 2.1 Policy Underpinnings / Beliefs

- Effective policies must be consistent with other directives, law, organizational culture, guidelines, procedures, and the organization's overall mission. It should also be integrated into and consistent with other organizational policies.
- Good policies are developed for a specifically defined or finite group with similar goals. Consequently, a large organization may need to be divided into components or units in order to clearly articulate policy that will meet the needs of the organization.
- Once the policies are identified they need to be visible in order to be effective. That means that policies will need to be fully communicated throughout the organization. Computer security training and awareness programs can effectively notify system users of security policies.
- Policies need to be introduced in a manner that indicates management's unqualified support and commitment to their implementation.
  - Data security policies are the vehicle for emphasizing management's commitment to these policies and clarifying its expectations for employee performance, behavior, and accountability. [NIST at13]
  - Data security policies are a way for management to demonstrate its belief that information security is important and that employees should pay close attention to securing information. [Wood at 9]
- Data security policies must include provisions to protect the integrity of data in all phases of collection, use, storage, and transmission.
- Data security policies should include all activities to preserve the authenticity and accuracy of information and data through the entire chain of custody.
- Data security policies should also include efforts to ensure validity, integrity and appropriateness for the particular viewer in specified situations.

- Security policies set the stage for privacy. Privacy takes into account who has access to what information and data on school computer systems and the vulnerabilities in the systems throughout the entire process of information collection, use, storage, and transmission.
- The need to protect information and data must be balanced against the need to make the information and data easily accessible to those who are authorized and need to use it.
- Security policies facilitate consistent implementation of controls. They establish a standard and provide the basis to document compliance with system requirements. They also form the basis for disciplinary action if needed.
- Security policies provide a systematic way for an organization to help avoid liability for negligence and breach of fiduciary duty.
- The security system policies should be easy to understand and used to ensure that the system's safeguards are not circumvented.
- A well-articulated data security policy should guide security product selection and implementation.
- Security system information should be disseminated to all persons in the organization, with enough orientation to ensure that everyone understands the purpose of the system, accepts its use by everyone, and then uses it appropriately.

### **3. Risk Assessment**

"In a world of limited budgets, risk assessment provides an organization with the information it requires to accurately prioritize its needs. Options for meeting those needs can then be considered, ranked accordingly, and funded to reflect priority." [NCES. Safeguarding Your Technology: Practical Guidelines for Electronic Education Information Security, p. 13.]

A risk exists when a threat takes advantage of a vulnerability and causes harm to a system. The object of risk assessment is to reduce vulnerabilities and risk and to determine what policies are needed.

The extent of the risk assessment is determined by

- 1) the level of threats an organization faces
- 2) the visibility of the organization to the outside world;
- 3) the sensitivity of the organization to the consequences of potential security incidents;
- 4) legal and regulatory issues. [NIST, p. 15]

It is important to assess all four areas when assembling a policy document, so that it will be applicable to the extent of the risk. If the risks are high, then the extent of the policy document should reflect that. If the risks are low, then general policies may suffice.

#### **3.1 Information Asset Inventory**

An inventory of all information assets is needed to be able to re-establish a system in the event of a disaster. This inventory should include all hardware, software, automated files, databases, and data communications links.

#### **3.2 Data Categorization**

An organization's data must be categorized according to its sensitivity to loss or disclosure. Based on this categorization, appropriate access requirements can be defined.

Owners of the data should assume responsibility for categorization levels, with management review. That means that whoever is responsible for the data or information should categorize various kinds of information that they work with into the level they feel is appropriate. After this original categorization, an overall management review of all categorizations should be done. Any adjustments should be made, using an overall organizational data assessment approach.

All persons who are asked to categorize information should agree on and use the same definitions for data categories. Four specific sensitivity classifications are generally used. Each classification has its own handling requirements. The categories are as follows:

**3.2.1 Sensitive:** Information that requires special precautions to assure the integrity of the information, by protecting it from unauthorized modification or deletion. It is information that requires a higher than normal assurance of accuracy and completeness. Examples of sensitive information include school financial transactions and regulatory actions.

**3.2.2 Confidential:** The most sensitive student information that is intended strictly for use within the school. This information is exempt from disclosure under the provisions of the Freedom of Information Act or other applicable federal laws or regulations. Its unauthorized disclosure could seriously and adversely impact the school, its students and their parents, its teachers and administrators, and the school board. Health care-related information should be considered at least CONFIDENTIAL.

**3.2.3 Private:** Personal information that is intended for use within the school setting. Its unauthorized disclosure could seriously and adversely impact the school district and/or its employees.

**3.2.4 Public:** All other information that does not clearly fit into any of the above classifications. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact the school, its employees, and /or its students or their parents. [Citation]

After all data is categorized, the next step is to assess the potential threats to the data assets from inside and from outside the system.

### 3.3 Asset Inventory

To ensure protection of all information assets each network administrator should maintain an inventory of information systems. This inventory should indicate all existing hardware, software, automated files, databases, and data communications links.

For each information asset, the following information should be detailed:

Type: hardware, software, data  
General support system or critical application  
Designated "owner" of the information  
Physical or logical location  
Inventory item number, where applicable [Guttman, p. 18]

### 3.4 Potential Threats to assets -- Risk Profile Matrix

Once the data or information is identified and categorized, the next step is to look at the data and assess what the potential threat risk to the information. All information is assessed individually according to an agreed upon scale of risk. The following is an example of a Risk Profile Matrix to Assist Administrators in their risk assessment of their system.

#### 3.4.1 Profile Matrix

**Risk Profile Matrix**

Threats	Rating	Visibility	Rating	Score
None identified as active; Exposure is limited	1	Very low profile; No active publicity	1	
Unknown state or multiple exposures	3	Middle of the pack, periodic publicity	3	
Active threats, multiple exposures	5	Lightning rod, active publicity	5	

**Risk Profile Matrix**

Threats	Rating	Visibility	Rating	Score
Consequences		Sensitivity		
No cost impact; well within planned budget; risk transferred	1	Accepted as cost of doing business; no organization issues	1	
Internal functions impacted; budget overrun; opportunity costs	3	Unacceptable business unit management impact; good will costs	3	
External functions impacted; direct revenue hit	5	Unacceptable corporate management impact; business relationships affected	5	
	Total Score			

**Rating:** Multiply Threat rating by Visibility rating. Multiply Consequences rating by Sensitivity rating. Add the two values together and compare to the risk scale below:

2 - 10	Low Risk
11 - 29	Medium Risk
30 - 50	High Risk

Source: Adapted from Barbara Guttman and Robert Gatwill, National Institute of Standards and Technology, U.S. Department of Commerce, Internet Security Policy: A Technical Guide [1998? Draft]  
<http://csrc.ncsl.nist.gov/isptg>

After policy makers decide what level of risk that they are working with, they will then need to decide which defenses are most applicable to their situation and level of risk.

### **3.5 Network Vulnerabilities and Defenses**

The table on the following page illustrates the potential areas of vulnerability that may exist on the Internet, within the State's network, and within a school's Local Area Network (LAN) and/or Wide Area Network (WAN). The vulnerabilities are listed in the first column. The defenses against these vulnerabilities are listed in the second column.

See also another method of risk assessment at the IASEP security page at [http://iasep.soe.purdue.edu/Training\\_info/SecurityThreats.htm](http://iasep.soe.purdue.edu/Training_info/SecurityThreats.htm) This page also has links to scenarios for applying the risk assessment format. Readers might try using both formats to discover which works best for their setting.

After vulnerabilities are assessed and the applicable defenses identified and planned, a set of operating statements about the system are necessary to facilitate the proper operation of the system defenses.

**Network Vulnerabilities and Defenses**

<b>Vulnerability</b>	<b>Defenses</b>
Internet	Firewall
E-mail	Authentication, and/or encryption. Virus scanning software should also be used.
Inappropriate URL Content	URL Content Filtering Products
Web site Security	Web server firewall, Authentication, Intrusion detection
Denial of Service Attack	Authentication, Service filtering, Firewall
Spoofing	Authentication
Sniffing	Encryption
FTP/Telnet	Firewall, Authentication, Administration
Sensitive/Confidential Information traveling the network & Internet	Encryption / Not allowing information to traverse the network or the Internet
Viruses	Virus Scanners for Workstation and E-mail
3rd Party Access	Single Point of Access/ Access Rights
Dial-up Access	Authentication/Access Rights
Unauthorized Access to an Agency	Authentication/Access Rights, Intrusion detection software, Firewall
Unauthorized Access to another Agency from within an Agency	Authentication/Access Rights
Application Level Security	Authentication/Access Rights, Intrusion detection
Secure Remote Access	Authentication, Tokens, Smart Card

Source: Adapted from Table 1, Network Security  
<http://www.its.state.ms.us/et/security/secpaper.htm>

Mississippi Department of Information Technology Services  
 Suite 508  
 301 North Lamar Street  
 Jackson, Mississippi 39201-1495  
 Voice - (601) 359-1395 FAX - (601) 354-6016

## 4. Physical Security Policies & Procedures

The following materials were adapted primarily from the NCES Safeguarding Your Technology document. For more detailed information on this topic, and for a Physical Security Checklist, see Safeguarding Chapter 5 at <http://nces.ed.gov/pub98/safetech/chapter5.html> [28].

**4.1 General Physical Security:** Physical security is an essential part of a security plan. It forms the basis for all other security efforts, including data security.

Physical security refers to the protection of building sites and equipment (and all other information and software contained therein) from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures, and spilled coffee). It requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders." [NCES, p. 55]

Providing this security will require a balancing of what resources are needed and what resources the institution can afford. First, use the risk assessment process identified in Chapter 3 to identify the organization's vulnerabilities. Then use the vulnerabilities list to set priorities on resources needed. Every enhancement of an identified vulnerability in the current system will generally provide more security than previously. Enhance the system to the extent possible, and keep a list of improvements still needed.

**4.2.1** Don't arouse unnecessary interest in secure areas -- minimize use of location signs

**4.2.2** Maximize structural protection. Secured rooms should have full height walls and fireproof ceilings

**4.2.3** Minimize external access. Secure rooms should only have one or two solid, fireproof, and lockable doors. The doors should be observable by security staff. Doors to secure areas should never be left open. Windows should be small and have locks.

**4.2.4** Maintain appropriate locks. Keep doors locked when room is not in use. Maintain secure system for keys and combinations. If there is a breach, each compromised lock should be changed.

**4.2.5** Alternative physical security strategies. When appropriate, consider the use of window bars, anti-theft cabling (with alarm when cable is disconnected from system), magnetic key cards, and motion detectors.

**4.2.6** Be prepared for fire emergencies with appropriate automatic non water fire fighting equipment, and provide appropriate staff training in its use.

**4.2.7** Maintain reasonable climate control in secured rooms, with temperature ranges between 50 and 80 degrees Fahrenheit, with a humidity range of 20 - 80%.

**4.2.8** Minimize nonessential materials that could jeopardize a secure room. Examples of nonessential items include: coffee, food, cigarettes, curtains, reams of paper, and other flammables.

**4.2.9** Dispose of confidential waste carefully and adequately to maintain confidentiality.

**4.2.10** Label confidential information appropriately and ensure suitable security procedures from common carriers when shipping or receiving confidential information.

### **4.3 Equipment Security**

**4.3.1** Keep critical systems separate from general systems.

**4.3.2** Store computer equipment in places that cannot be seen or reached from windows and doors, and away from radiators, heating vents, air conditioners, or other work. Workstations that do not routinely display sensitive information should stored in open, visible spaces to prevent covert use.

**4.3.3** Protect cabling, plugs, and other wires from foot traffic.

**4.3.4** Keep a secure inventory of equipment and peripheral equipment, with up-to-date logs of manufacturers, models, and serial numbers. Consider videotaping the equipment for insurance purposes.

#### **4.3.5 Specific Laptop Security Procedures**

**4.3.5.1** Lock laptops in secure cabinet when not in use.

**4.3.5.2** Secure laptops to desks with cables when unattended.

**4.3.5.3** Provide and use laptop cover locks.

**4.3.6** Log off and lock computers when the operator is not in the vicinity of the computer.

**4.3.7** Use a virus scanner on all computers at all times. Establish a regular schedule for update of virus lists.

**4.3.8** Assign printers to users with similar security clearance levels.

#### **4.4 Equipment Usage**

##### **4.4.1 Laptop Usage**

**4.4.1.1** The primary IASEP purpose for using the laptops is for testing children and writing reports.

**4.4.1.2** Establish a procedure for how peripherals and software applications are to be used on the laptop.

**4.4.1.3** Establish procedures for laptop sharing. Each user should have a separate password.

**4.4.1.4** Establish a procedure for the use of laptops at home or other locations.

**4.4.2** Other hardware will be accompanied by applicable usage and access requirements.

**4.4.3** Establish a system to limit and monitor access to equipment areas.

**4.4.4** Establish a procedure for storing laptops offsite. They should not be placed in car trunks overnight, in cars in extreme hot or cold, or in places where they can be damaged by other moving equipment, such as car jacks.

**4.5 Designated Anti-virus Programs will be used at all times. Programs will be enabled at all times and virus lists will be updated on a designated schedule.**

#### **4.6 Equipment Maintenance**

**4.6.1** Consider the use of maintenance contracts. Keep equipment information, contact and tech support numbers readily available at the computers.

**4.6.2** When computers containing sensitive information are being maintained or repaired, be sure that sensitive data is properly passworded, encrypted, or removed from the computer before maintenance or repair.

##### **4.6.3 Laptop maintenance**

**4.6.3.1** Identify a method of problem detection and reporting.

**4.6.3.2** Establish a schedule for regular computer maintenance and establish a mechanism to contact the Technology department for maintenance.

**4.6.3.3** Provide spare equipment for use when laptops are being repaired or maintained.

**4.7 Equipment labeling. Identify all equipment in overt and covert ways to make unauthorized tampering or use difficult.**

## **4.8 System Backup**

**4.8.1** Procedure to be used to backup system information and applications.

**4.8.1.1** Establish a procedure and schedule of system backup.

**4.8.1.2** Establish overall system backup responsibilities and assign them.

**4.8.1.3** Individuals who use the computers should also have backup responsibilities.

**4.8.1.4** Use a rotation of media (using different disks at each backup and rotating every X days or weeks).

**4.8.1.5** Both onsite and offsite backup storage should be considered and used.

## **4.9 Regulate power supplies to the extent possible.**

**4.9.1** Prepare for electrical power fluctuations by using surge suppressors or electrical power filters and using uninterruptible power sources to serve as auxiliary electrical supplies as backup to critical systems.

**4.9.2** Design electrical systems to better withstand fires, floods, and other disasters.

**4.9.3** Ensure distributed use of outlets by all equipment.

**4.9.4** Use anti-static carpeting and pads, and use anti-static sprays whenever possible.

## **4.10 Addition of new users to the system.**

When new users are added to the system, they will receive and acknowledge receipt of policies related to the use of equipment and accompanying software.

Draft 5-21-00 v3

## 5. Information Security Policies

This Chapter contains information that has been adapted from NIST's Internet Security Policy: A Technical Guide by Barbara Guttman and Robert Bagwill at <http://csrc.nsl.nist.gov/isptg> [13] Materials from Safeguarding Your Technology at <http://nces.ed.gov/pubs98/safetech/> have also been adapted. [30]

**5.1 General Information & Data Protection Policies.** After the school does an assessment of its information security status and a plan set in motion for its security, policy statements about that information are needed. Policies related to a school's handling of information, particularly related to school children, are essential to ensure that the school is in compliance with federal and state laws. A clear and consistent policy related to securing that information at all phases of its collection, use and storage is imperative.

**5.1.1. Confidentiality of information.** One of the most valuable assets of a school is its information, and specifically information related to individuals. This information must be safeguarded. State and federal laws require that information related to individuals be kept secure, confidential, and protected from unauthorized release. The Family Education Rights and Privacy Act of 1974 (FERPA) requires that all individual student records be protected from unauthorized disclosure. See Appendix B.

**5.1.2 Integrity of information.** All confidential and non-confidential system information must be protected from unauthorized creation, modification or deletion of that information. Consequently, policies about who may create, modify and delete this information are critical to provide guidance to all administrators and staff of the organization.

**5.1.3 Availability of information.** All confidential and non-confidential information must be protected from unauthorized access, delay or denial of information.

**5.2 Data or Information Classification.** Data is raw information that lacks any context, and therefore is not meaningful in and of itself. When data is placed in a context, it becomes information. The number 76 lacks meaning standing alone, but when it is associated with the words intelligence quotient, it takes on meaning. All data or information must be classified into the security level necessary for its protection.

**5.2.1 Sensitive information:** Information that requires special precautions to assure the integrity of the information, by protecting it from unauthorized modification or deletion. It is information that requires a higher than normal

assurance of accuracy and completeness. Examples of sensitive information include school financial transactions and regulatory actions.

**5.2.1.1 Collection of sensitive information:** Collection of sensitive student information must be done by authorized persons in a manner that will protect the confidentiality of that information.

**5.2.1.2 Modification of sensitive information:** Only authorized persons may modify any sensitive students records.

**5.2.1.3 Disclosure of sensitive information:** Sensitive information may be disclosed only to those persons with authorization.

**5.2.2 Confidential information:** This is the most sensitive student information that is intended strictly for use within the school. This information is exempt from disclosure under the provisions of the Freedom of Information Act or other applicable federal laws or regulations. Its unauthorized disclosure could seriously and adversely impact the school, its students and their parents, its teachers and administrators, and the school board.

**5.2.2.1 Collection of confidential information:** Collection of confidential student information must be done by authorized persons in a manner that will protect the confidentiality of that information.

**5.2.2.2 Modification of confidential information:** Only authorized persons may modify any confidential students records.

**5.2.2.3 Disclosure of confidential information:** Confidential information may be disclosed only by authorized persons to authorized persons.

**5.2.3 Private information:** The term private data refers to data of a personal nature, which if disclosed to individuals other than those with an authorized "need to know" would be seriously detrimental to an individual or would be an invasion of a person's right to privacy. This applies to information covered by federal or State privacy laws and information ordered private by a court. Its unauthorized disclosure could seriously and adversely impact the student and the school.

**5.2.3.1 Collection of private information:** Collection of private student information must be done by authorized persons in a manner that will protect the confidentiality of that information.

**5.2.3.2 Modification of private information:** Only authorized persons may modify any private students records.

**5.2.3.3 Disclosure of private information:** Private information may be disclosed only to those persons with authorization.

**5.2.4 Public information:** Public information is information that does not clearly fit into the sensitive, confidential or private information classifications. Its unauthorized disclosure may be against policy in some instances, but that disclosure does not seriously or adversely affect the school, its employees, and/or its students.

**5.2.4.1 Collection of public information:** Collection of public information may be done by anyone employed for that purpose.

**5.2.4.2 Modification of public information:** It's always important that information of any kind be accurate and be kept up-to-date. There are potential legal problems with the use of inaccurate information.

**5.2.4.3 Disclosure of public information:** If information is public, it may be generally released upon request without permission, but it must also be released consistent with any applicable policies. It's important to ensure that that information is accurate, up-to-date, or at least contains a disclaimer stating the source of the information and when it was last updated.

**5.3 Transmission of information.** Before any information is transmitted, it is necessary to know its level of sensitivity and the extent to which it can be transmitted according to other policies in place. Policies should identify what persons may access, prepare, and transmit the information, along with any disclaimers that go with the information.

**5.3.1 Copying and printing.** As part of ensuring the privacy of information, copying and printing additional copies of any confidential information should be limited or restricted, except with appropriate permissions.

**5.3.2 Shipping and manual handling of information.** Use caution in sending information in any format. If sending information by U.S. mail or express carriers, be sure that recipient addresses are correct, and include a notice to anyone who is not the recipient related to the confidential nature of the materials and no one by the named recipient should read the materials.

**5.3.3 Transmission by fax or phone.** Great caution should be used in talking about information with anyone on the phone and with transmitting any confidential information by fax. Be sure that the person talking about or sending the information has permission to do so and is the appropriate person to send it. In addition, ensure that the recipient of the information has permission to receive it. All faxes should be accompanied with a cover sheet that contains a warning similar to the following:

Warning: This material is intended only for the individual or entity to which it is addressed. It may contain privileged, confidential information which is exempt from disclosure under applicable laws. If you are not the intended recipient, please note that you are strictly prohibited from disseminating or distributing this material (other than to the intended recipient) or copying this material. If you have received this communication in error, please notify us immediately by telephone and return this material (and all copies) to us by mail at the above address. On request, we will reimburse you for any cost of return. Thank you.

**5.3.4 Transmission via the Internet.** Internet transmission of confidential information is inherently dangerous. There are many ways for this information to be intercepted. Any confidential information sent must be encrypted, using the organization's standard encryption policy. Any accompanying email message should also contain a warning message similar to the one displayed above.

**5.4 Identification and Authentication.** It is important to make sure that all persons using a confidential information system be authorized for its use at the specific level of access that they are allowed. Policies and mechanisms must be implemented to ensure that this occurs at all times. A system for who may access what parts of an information system and at what level will need to be in place before the system may be accessed by those individuals.

**5.4.1 General Identification Policy.** Mechanisms must be in place to establish the identity of any individual attempting to access the information system.

**5.4.2 General Authentication Policy.** Authentication is the act of verifying a user's identity in order to prevent unauthorized use. Authentication can be as simple as a computer ID and password or as complex as one time passwords, challenge response passwords, or physical identification (retinal, voice, image, etc). Schools should establish a consistent method of authentication that fits the facility's needs and which generates a log of all system use.

**5.5 Information Integrity.** Information integrity refers to information that is complete and uncompromised. Administrators should implement policies related to making sure that information remains its original uncompromised condition. In addition, confidential information should be periodically checked to make sure that it has not been compromised.

**5.6 Digital Signatures and Certificates:** Digital certificates are electronic transmissions that allow the recipient to authenticate the identity of the sender via

third party verification from an independent certificate authority. A digital certificate is a code attached to an electronic message that is used to verify that the individual sending the message is really who he or she claims to be. Schools should consider using these forms of verification on each computer when transporting information via the Internet.

**5.7 Intellectual Property rights:** Intellectual property is the tangible or intangible results of research, development, teaching, or other intellectual activity. This includes things such as original written materials, software, trademarks, or product designs. The owner of the specific intellectual property has certain rights to control the use of that property. All staff need to be aware of what constitutes intellectual property and need to be respectful of the owner's rights.

**5.7.1 Assignment of IP rights:** The owner of Intellectual property may be assign his or her rights to others. Staff who write original works as part of their employment may be required to assign those rights to their employer or may keep them, depending on the policy of the employer. If school personnel wish to use copyrighted materials from another, they must first obtain permission to use those materials or an assignment of their rights. This should be in writing and a copy should be kept on file.

**5.7.2 Respect of IP rights:** All software will be registered and used according to the licensing agreements. No one will copy software. All software documentation should accompany each computer. Documentation for portable computers will be placed in specified place.

**5.8 Right to know about secured data:** Parents have a right to know what data is being collected on their children. A procedure for allowing parents to see confidential records will be written and used. See Appendix G for sample forms.

**5.9 Encryption:** Encryption is the process of translating a file into an unintelligible format, or to encode it, via the use of mathematical algorithms or other encoding mechanisms. To open the document, the recipient must have a matching key to decrypt and read the message. While encryption prevents others from reading encrypted documents, encrypted files can be damaged, destroyed, or keys can be lost so that the files are not accessible. This is a risk that policymakers must consider.

**5.9.1** Never send sensitive information in a regular email. Encrypt any messages or information that must be sent via email. See Appendix F for technical resources related to encryption.

**5.9.2** Encrypt all sensitive information on laptops and desktops and any information that is stored on a network server. This includes passwords.

**5.9.3** Any encryption system used should be system-wide, consistent from computer to computer, and keys should be made available to administration

or identified IT staff to ensure that information is not lost. All encryption products used will support a method of making encryption keys available to management or IT staff. See Internet Security Policy: A Technical Guide for more information on encryption pointers. [13]

**5.10 Password policies:** Use consistent required passwords. See the considerations that should be included when assembling a password system in Chapter 7 of this document .

Draft 5/29/00 v.4

## 6. Software Security Policies

**6.1 Reasons for Software Security Policies** -- Software is a valuable resource that allows computers to do what you want them to do. Software can be stolen, copied, and corrupted in many ways. This is an expensive loss. Imported software or viruses can also cause damage to hardware, other software and data.

**6.2 Software security and acceptable use policy.** It is important to keep software secure and under control. A list of acceptable software for the school's systems should be compiled. This is the software that the IT department will support. If school personnel need specific software for their work, permission should be obtained from the IT department or administration.

**6.3 Virus Prevention, Detection, and Removal** -- There are thousands of computer viruses, worms, Trojan horses, and other destructive programs. If they are imported onto a computer they can cause great damage. For that reason computer systems must be protected from these viruses with special anti virus programs that detect and remove these unwanted programs. Every computer should be equipped with a strong anti virus program.

**6.3.1 Regular virus list update** -- New viruses are being created every day. And anti virus program companies are continually developing new lists of viruses and protection from them. For that reason, regular (i.e., weekly) updating of virus lists is imperative.

**6.3.2 Routine use of anti virus program** -- An anti virus program should be running at all times when any school computer is in use. In addition regularly scheduled virus scans should be done or programmed so that the entire system can be screened for viruses.

**6.3.3 Scanning disks used from other systems.** Disks from other systems that are used with school computers should be screened for viruses before use. This can be done automatically by adjusting the anti virus program's setting, or it can be done manually.

**6.4 Controlling Interactive Software.** Interactive software includes games and other programs that require the computer operator to interact with the program in some way. These programs can be installed on a computer or they can be used over an internal or external network, such as the Internet. Some of these programs can be highly useful and therapeutic in a work setting, and others (i.e., some games) can take up valuable disk space and work time, and can introduce malicious code. Policies related to the use of only authorized software should address this kind of software.

## **6.5 Software Licensing**

**6.5.1 All software used must be licensed to the organization or its representative using the software.** Programs may only be used in the way that they are intended. For example, most software is licensed for one computer at a time use. That license should be respected. All licensing information and software documentation should be kept in a secure and readily accessible place.

**6.6 Encryption.** See the encryption discussion in Chapter 5.

Draft 5/29/00 v2

## 7. User Access Security Policies

User access refers to several different concepts. First, it refers to allowing only authorized persons access to a particular computer system or network, and restricting access to any persons or computers without specified levels of security clearance. Secondly, it refers to allowing authorized users access to only the amount of information or portion of the system or network necessary for them to accomplish their designated responsibilities. Policies are required to establish the requisite levels of access to protect confidential, sensitive, and private information and data contained in on a computer system or network.

---

**7.1 System access control** System access control is one of the most important components in any data or information security plan. It is imperative that a school computer system or network be assessed only by authorized persons, and only to the extent that it is necessary and authorized.

**7.1.1** A system is needed for users to identify themselves and prove they are who they claim to be. This system may be as simple as using a password, to the use of a multi-level login or retinal scans. The risk assessment will determine the level of access control needed.

**7.1.2** A log of all network activity, from logon to logoff, needs to be made and retained for auditing and intervention purposes.

**7.1.3** It is the responsibility of top level administrators and information technology directors to establish a system and accompanying policies to ensure that the school computer system or network is used properly. Lines of authority and control need to be clearly defined.

**7.1.4** System access and use security policies and procedures protect:

- a) the system or network itself from intrusion and damage
- b) confidential, sensitive or personal information on the system
- c) each user who might inadvertently or unintentionally gain access to or damage system files

**7.2 Login Process--** The beginning of the process of access control is at the login stage. It is imperative at this stage to inform all authorized and unauthorized users that the system is being monitored and that unauthorized access or use has consequences. In addition, a welcome screen to the system could also imply to

whomever is reading the screen that the user is invited to access the system. Consequently, it is important to convey the proper message to all persons logging onto the computer system or network.

**7.2.1 Warning screens** --There are a many kinds of warning screens used by systems administrators. The major objectives of most are to provide accurate warnings about 1) the need for appropriate authorization to enter and use the system, 2) the continuous monitoring of the system, and 3) potential sanctions for prohibited behaviors or actions. By placing these messages on a introductory screen, readers are presumed to explicitly or implicitly agree to the conditions of authorization, monitoring, and sanctions before continuing on to the next screen. This is presumed whether they read the screen or not. It is there for them to read.

**7.2.2 User agreement** -- Depending on their initial risk assessment, some systems require the reader to agree to the above terms every time they log onto the system, or at least the first time that they access the system and periodically thereafter. If this kind of screen message is used initially or periodically, it's important to have the message readily accessible to any user at any time.

Safeguarding Your Technology at <http://nces.ed.gov/pubs98/safetech/> (p. 86) provides an example of a logon screen warning for a secure computer system or network, which is adapted below:

<p><b>WARNING!</b> This is a restricted network. Use of this network, its equipment, and resources is monitored at all times and requires explicit permission from the network administrator. If you do not have this permission in writing, you are violating the regulations of this network and can and will be prosecuted to the full extent of the law. By continuing into this system, you are acknowledging that you are aware of and agree to these terms.</p>
--

**7.3 Password and User ID process.** Every school should devise a system for identifying specific users and for password acceptance. This will help to ensure greater control of access to system resources and will ensure an appropriate record of system usage. The use of passwords is a very individual issue, but specific rules for their use ensure consistency and greater security.

### **Sample Password Policy Elements Components**

Suggested policy elements for the creation and use of passwords are:

- Include non-alpha characters in the password, such as numbers and punctuation marks
- Use hard to guess password
- Use passwords that are not personal to the user and unique -- no alternating passwords.
- Passwords must be kept in a safe place and not shared with anyone -- no shared accounts
- Individual passwords should be kept private -- no password sharing allowed, no coding them into programs, and no writing them down in obvious places.
- Minimum password lengths should be established (i.e., minimum of 6 alphanumeric characters). If they are too short they will be easier to crack, but if they are too long they'll be hard to remember.
- Passwords should in no way identify or reflect on the user (pet names, birth dates, favorite themes, etc.). Ideally, passwords should be non-words or random character and number combinations.
- Passwords should to be changed periodically (every 1-3 months). The system should automatically require changes at given intervals.
- Use encrypted passwords so only the user will know them. Passwords must be kept safe because if they are lost, information will also be lost.
- Use across-the-network password encryption to prevent passwords from being read by protocol analyzers or others ways.
- Logon IDs and passwords should be suspended if not used for a specified period of time (e.g., 30 days).
- Sessions should be suspended after a specified period of time if system is not in use -- then should require password to be reentered. A password should always be required.
- System administrators should change any pre-set passwords that are built into any software.
- Passwords should never be sent via email to anyone, unless the email is encrypted.
- Passwords need to be masked or obscured on the screen when anyone logs in.
- If users suspect that their password has been compromised, they should change the password immediately.
- Passwords are not available to administrators or IT department.

**7.4 Privileges--** This term refers to the permission that a person receives, by virtue of his or her work position, to enter a specific computer system or network. This is not an absolute right, but rather an earned right that accompanies an employee's job requirements, if s/he meets specific criteria.

**7.4.1 Levels--** Based on its risk assessment, every organization should have designated access privilege levels for every employee. These levels are based on the extent of the computer system or network the employee needs to access to do their job. These levels should be determined when a person is hired by the school system and should be periodically assessed on a regular schedule and checked against audit logs. If employees change jobs within the system, their privileges should be reassessed for the appropriate level of access needed to do their new job. If employees work on an academic year schedule, their privileges should be valid for only that period of time, unless they have permission to use the system during a period when school is not in session.

**7.4.2 Special privileges--** From time to time persons from outside the system or regular employees on special projects may need to access certain portions of a computer system or network. Decisions related to the appropriate level of access assigned to these people, if any, need to be made by top level administrators of the school and the network administrator. This decision making process needs to be documented and clear so employees know the procedure for obtaining special privileges.

**7.4.2.1 Remote users --** Remote use by authorized users should be pre-approved separately from the initial approval process. Remote users should be made aware that remote access will be monitored very carefully and that any transmission of confidential, sensitive, or private information over public phone lines must be encrypted.

**7.4.3 Privileges restrictions--** All persons who have access to a system at any level should be given notice initially and periodically that privileges can and will be restricted or eliminated at any time if they abuse the privilege given to them by their employer. In addition, employees who are not working during the summer or who go on sabbatical should understand that, unless they have special permission, their privileges to the school computer system or network will be restricted.

**7.4.3.1 Log-in times --** Limit users to log-ins during those times when they are actually working. This should be designated initially

when they are given access. Special privileges for remote users may need to be established.

**7.4.3.2 Log-in locations** -- Limit users to only those computers on which they will be working. This also should be designated when they are initially given access to the system or network.

**7.4.3.3 Log-in attempts** -- Set a reasonable number (e.g., three) of attempts to log in before the system suspends the account. Suspending the account will prevent an unauthorized user from retrying to log in later. Legitimate users can always request that their access be reestablished.

**7.4.3.4 Log off requirements** -- Require all authorized users to log off when they leave their work station and to log off and turn off the computer after use. This prevents any unauthorized use when the work station is unattended.

**7.4.3.5 Appropriate Use Agreements** -- All authorized users should be required to sign an appropriate use agreement before they receive access to the system or network.

**7.5 Login system**-- Every computer system or network must have a secure login system. Its purpose is to restrict access to only those individuals who have permission to enter the system or network and only at the level of access that each employee has been assigned by administrators, based on their need to accomplish their job. The login system set up by network administrators needs to be flexible enough to accommodate changes in privilege levels of employees.

---

Resources used to formulate this chapter are primarily the following: NIST's Internet Security Policy: A Technical Guide by Barbara Guttman and Robert Bagwill at <http://csrc.nsl.nist.gov/isptg> [13] and Safeguarding Your Technology at <http://nces.ed.gov/pubs98/safetech/> [30].

---

Draft 7/16/00 v3

## 8. Network and Internet Security Policies

**8.1 Authentication** -- Authentication refers to the many processes of making sure that the persons who log on to a computer system or network are who they say they are. Authentication actually makes decisions based on 'who' was at the source. Authentication can be as simple as a computer ID and password or as complex as one time passwords, challenge response passwords, or physical identification (retinal, voice, image, etc). [NIST Policy, p 33]

**8.1.1 Risk Assessment is a needed first step.** An organization's initial Risk Assessment will provide information on how extensive the authentication process should be. The Risk Assessment step should never be eliminated, since this process is what provides guidance for decision making on authentication systems.

**8.1.2 Authentication Resources** -- There are many resources available that discuss authentication resources in more depth. The following list may be of use:

- Organization for Economic Co-operation and Development. Information, Computer and Communications Policy Committee Working Party on Information Security and Privacy Joint OECD-Private Sector Workshop on Electronic Authentication, Background Paper on Electronic Authentication Technologies and Issues (June 1999)  
<http://www.nzcs.org.nz/nzpkaf/jointoecd.htm>
- Center for Information Technology, National Institutes of Health, Authentication and Encryption Software (May 2000) at  
<http://www.alw.nih.gov/Security/prog-auth.html>
- 

### 8.2 Firewall Administration

**8.2.1 Internet Firewall Policy** - A firewall refers to a special kind of software used to control access into and out of a designated computer network. The purpose a firewall is to protect a computer system from intrusion from outside the system. It will also control the access of users to sources outside the system. Firewalls are an important and essential component to any computer network.

#### 8.2.2 Firewall-related issues

**8.2.2.1 Dial-in numbers** -- Do not publicly list dial-in numbers, since all remote access users should have those numbers.

**8.2.2.2 Automatic answer mode** -- Do not leave a modem on automatic answer mode. This could subject the system to unauthorized and unsupervised system access.

**8.2.2.3 Modem use only from secure locations** -- Modems connected to system machines should always be protected by a firewall or gateway.

**8.2.2.4 Security of external networks** -- External networks to which the school network connects must be secure. If they cannot be verified as secure, precautions such as gateways and firewalls will need to be installed. Install automatic terminal identification, dial-back, and encryption mechanisms to protect transmissions to and from off-site users. [Safeguarding, p. 69]

**8.2.2.5 Internet connections** -- The Internet and other networks provide two ways of communication and access. The internal school system or network must be secured to protect against access from these networks.

**8.2.3 Firewall Resources** -- there are many resources available related to firewalls, including some of the following:

- Center for Information Technology, National Institutes of Health, Firewall Software (December 1999)  
<http://www.alw.nih.gov/Security/prog-firewall.html>

**8.3 System Integrity, security, documentation & incident handling** -- These are all the responsibility of systems administrators. There need to be policies in place to ensure that all these areas are dealt with appropriately.

**8.4 Logs and Audit Trails** (Audit/Event Reporting and Summaries) -- Logs and audit trails must be maintained at all times and stored in a secure place.

**8.4.1 System logs.** Logs should keep track of who is granted access to specific student information, who actually accesses the records, and when access occurs. Other access logs should also be established according to the results of the risk assessment.

**8.4.2 Event Reporting.** A system of performing and reporting event audit results should be implemented to ensure appropriate administrative evaluation and handling of access events. Policies for when and how those audits will be done, and who is responsible for them, should be established initially when a computer network or system is placed in service.

**8.4.3 Network Monitoring Resources** -- Regular monitoring of a computer system or network should be implemented and used regularly. Regular reports should be reviewed by system and school administrators.

- Center for Information Technology, National Institutes of Health, Network and Network Monitoring Software (June 2000)  
<http://www.alw.nih.gov/Security/prog-network.html>

- Center for Information Technology, National Institutes of Health, System Monitoring Software (June 2000) <http://www.alw.nih.gov/Security/prog-monitor.html>

**8.5 Internet and World Wide Web (WWW)** -- The Internet, and specifically Web, have provided great opportunities for students and faculty for educational purposes. However, it has also created numerous security and privacy issues. For that reason, it is essential to have policies that address the use of the Internet, the Web, and email systems.

**8.5.1 Internet Use Policies** -- Internet use policies should be developed to guide teachers, students, staff, and school administrators in their use of the Internet.

**STATE OF INDIANA REQUIREMENTS FOR PUBLIC SCHOOL INTERNET ACCEPTABLE USE POLICIES AND GUIDELINES**

Source: <<http://www.siec.k12.in.us/aup/require.html>>

A. 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 the 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.
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 for a student to 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. Safeguarding personal information, such as name, address, telephone number, etc.

Indiana Department of Education -- Revised November 1995

STATE OF INDIANA RECOMMENDATIONS FOR PUBLIC SCHOOL INTERNET  
ACCEPTABLE USE POLICIES AND GUIDELINES

Source: <http://www.siec.k12.in.us/aup/recomm.html>

A. It is strongly recommended that each public school corporation in Indiana establish an Internet Acceptable Use Policy that is consistent with existing policies for print media, and that the local Internet Acceptable Use Policy include:

1. A brief explanation of the Internet, content that is available via the Internet, and the potential educational value of student access to the Internet.
2. Disclaimer limiting the school corporation's liability relative to:
  - a. Information stored on school corporation diskettes, hard drives or servers.
  - b. Information retrieved through school corporation computers, networks or on-line resources.
  - c. Personal property used to access school corporation computers, networks or on-line resources.
  - d. Unauthorized financial obligations resulting from use of school corporation resources/accounts to access the Internet.
3. Parent/Guardian responsibilities.
4. A description of the privacy rights and limitations of school sponsored/managed Internet accounts.
5. Notification that, even though the school corporation may use technical means to limit student Internet access, these limits do not provide a foolproof means for enforcing the provisions of local Acceptable Use Policies.
6. Notification that all provisions of the policy are subordinate to local, state and federal statute.
7. Notification to parents/guardians that it is possible for students to purchase goods and services via the Internet and that these purchases could potentially result in unwanted financial obligations.

B. It is strongly recommended that each public school corporation in Indiana develop guidelines that:

1. Include suggestions to help parents and students to take full advantage of Internet access from home or public access terminals.
2. Require students of an appropriate age to read and sign (indicating their acceptance of the provisions and agreement to comply) the school corporation's Acceptable Use Policy.
3. Describe appropriate staff use of school corporation Internet resources/accounts.
4. For internal use, assign specific staff with specific security, management and account responsibilities associated with the school corporation's Internet resources and accounts.
5. Include procedures for users to subscribe to Internet services, such as list servers and news groups.

Indiana Department of Education -- Revised November 1995.

## 8.5.2 Acceptable Use Policy Examples

### **Model Acceptable Use Policy Access to Electronic Information, Services, and Networks published by the Indiana Department of Education**

This model meets all the requirements for an AUP for Indiana public school corporations.

Source: <<http://www.siec.k12.in.us/aup/modelaup.html>>

### **{SCHOOL DISTRICT} Policy on District-Provided Access to Electronic Information, Services, and Networks**

Freedom of expression is an inalienable human right and the foundation for self-government. Freedom of expression encompasses the right to freedom of speech and the corollary right to receive information. Such rights extend to minors as well as adults. Schools facilitate the exercise of these rights by providing access to information regardless of format or technology. In a free and democratic society, access to information is a fundamental right of citizenship.

In making decisions regarding student access to the Internet, the {SCHOOL DISTRICT} considers its own stated educational mission, goals, and objectives. Electronic information research skills are now fundamental to preparation of citizens and future employees. Access to the Internet enables students to explore thousands of libraries, databases, bulletin boards, and other resources while exchanging messages with people around the world. The District expects that faculty will blend thoughtful use of the Internet throughout the curriculum and will provide guidance and instruction to students in its use. As much as possible, access from school to Internet resources should be structured in ways which point students to those which have been evaluated prior to use. While students will be able to move beyond those resources to others that have not been previewed by staff, they shall be provided with guidelines and lists of resources particularly suited to learning objectives.

Outside of school, families bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephones, radio, movies, and other possibly offensive media.

Students utilizing District-provided Internet access must first have the permission of and must be supervised by the {SCHOOL DISTRICT}'s professional staff. Students utilizing school-provided Internet access are responsible for good behavior on -line just as they are in a classroom or other area of the school. The same general rules for behavior and communications apply.

The purpose of District-provided Internet access is to facilitate communications in support of research and education. To remain eligible as users, students' use must be in support of and consistent with the educational objectives of the {SCHOOL DISTRICT}. Access is a privilege, not a right. Access entails responsibility. Users should not expect that files stored on school-based computers will always be private. Electronic messages and files stored on school-based computers may be treated like school lockers. Administrators and faculty may review files and messages to maintain system integrity and insure that users are acting responsibly.

#### **The following uses of school-provided Internet access are not permitted:**

- 1.) To access, upload, download, or distribute pornographic, obscene, or sexually explicit material;

- 2.) To transmit obscene, abusive, or sexually explicit language;
- 3.) To violate any local, state, or federal statute;
- 4.) To vandalize, damage, or disable the property of another individual or organization;
- 5.) To access another individual's materials, information, or files without permission; and,
- 6.) To violate copyright or otherwise use the intellectual property of another individual or organization without permission.

Any violation of District Policy and rules may result in loss of District-provided access to the Internet. Additional disciplinary action may be determined at the building level in keeping with existing procedures and practices regarding inappropriate language or behavior. When and where applicable, law enforcement agencies may be involved.

The {SCHOOL DISTRICT} makes no warranties of any kind, neither expressed nor implied, for the Internet access it is providing. The District will not be responsible for any damages users suffer, including--but not limited to--loss of data resulting from delays nor interruptions in service. The District will not be responsible for the accuracy, nature or quality of information stored on District diskettes, hard drives, or servers; nor for the accuracy, nature, or quality of information gathered through District-provided Internet access. The District will not be responsible for personal property used to access District computers or networks or for District-provided Internet access. The District will not be responsible for unauthorized financial obligations resulting from District-provided access to the Internet.

**Parents of students in the {SCHOOL DISTRICT} shall be provided with the following information:**

The {SCHOOL DISTRICT} is pleased to offer its students access to the Internet. The Internet is an electronic highway connecting hundreds of thousands of computers and millions of individual users all over the world. This computer technology will help propel our schools through the communication age by allowing students and staff to access and use resources from distant computers, communicate and collaborate with other individuals and groups around the world, and significantly expand their available information base. The Internet is a tool for life-long learning.

Families should be aware that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate, nor potentially offensive to some people. In addition, it is possible to purchase certain goods and services via the Internet which could result in unwanted financial obligations for which a student's parent or guardian would be liable.

While the District's intent is to make Internet access available in order to further educational goals and objectives, students may find ways to access other materials as well. Even should the District institute technical methods or systems to regulate students' Internet access, those methods could not guarantee compliance with the District's acceptable use policy. That notwithstanding, the District believes that the benefits to students of access to the Internet exceed any disadvantages. Ultimately, however, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. Toward that end, the {SCHOOL DISTRICT} makes the District's complete Internet policy and procedures available on request for review by all parents, guardians, and other members of the community; and provides parents and guardians the option of requesting for their minor children alternative activities not requiring Internet use.

NOTICE: This policy and all its provisions are subordinate to local, state, and federal statutes.



**Sample Acceptable Use Policy  
and Application for Classroom use of the Internet**

Adapted from Kevin Barry, Florida Institute of Technology, Academic & Research Computing Services and originally recommended by the Southern Indiana Education Center.

Source: <http://www.siec.k12.in.us/aup/Acceptable.Use.txt>

**TERMS AND CONDITIONS FOR USE OF INTERNET**

Please read the following carefully before signing this document. This is a legally binding document. Internet access is now available to students and teachers in the \_\_\_\_\_ County School District. The access is being offered as part of a collaborative project involving \_\_\_\_\_ School, the Indiana Department of Education, and \_\_\_\_\_. We are very pleased to bring this access to \_\_\_\_\_ County and believe the Internet offers vast, diverse and unique resources to both students and teachers. Our goal in providing this service to teachers and students is to promote educational excellence in the \_\_\_\_\_ County Schools by facilitating resource sharing, innovation and communication.

The Internet is an electronic highway connecting thousands of computers all over the world and millions of individual subscribers. Students and teachers have access to:

- 1) electronic mail communication with people all over the world.
- 2) information and news from NASA as well as the opportunity to correspond with the scientists at NASA and other research institutions.
- 3) public domain and shareware of all types.
- 4) discussion groups on a plethora of topics ranging from Chinese culture to the environment to music to politics.
- 5) access to many University Library Catalogs, the Library of Congress, CARL and ERIC.

With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting. \_\_\_\_\_ and \_\_\_\_\_ have taken available precautions to restrict access to controversial materials. However, on a global network it is impossible to control all materials and an industrious user may discover controversial information. We, at \_\_\_\_\_ School, and \_\_\_\_\_ firmly believe that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may procure material that is not consistent with the educational goals of this Project.

Internet access is coordinated through a complex association of government agencies, and regional and state networks. In addition, the smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines. These guidelines are provided here so that you are aware of the responsibilities you are about to acquire. In general this requires efficient, ethical and legal utilization of the network resources. If a \_\_\_\_\_ school user violates any of these provisions, his or her account will be terminated and future access could possibly be denied. The signature (s) at the end of this document is (are) legally binding and indicates the party (parties) who signed has (have) read the terms and conditions carefully and understand (s) their significance.

### **Internet - Terms and Conditions**

1) **Acceptable Use** - The purpose of NSFNET, which is the backbone network to the Internet, is to support research and education in and among academic institutions in the U.S. by providing access to unique resources and the opportunity for collaborative work. The use of your account must be in support of education and research and consistent with the educational objectives of the \_\_\_\_\_ County School District. Use of other organization's network or computing resources must comply with the rules appropriate for that network. Transmission of any material in violation of any US or state regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secret. Use for commercial activities \_\_\_\_\_ is generally not acceptable. Use for product advertisement or political lobbying is also prohibited.

2) **Privileges** - The use of Internet is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. (Each student who receives an account will be part of a discussion with a \_\_\_\_\_ teacher pertaining to the proper use of the network.) The system administrators will deem what is inappropriate use and their decision is final. Also, the system administrators may close an account at any time as required. The administration, faculty, and staff of \_\_\_\_\_ may request the system administrator to deny, revoke, or suspend specific user accounts.

3) **Netiquette** - You are expected to abide by the generally accepted rules of network etiquette. These include (but are not limited to) the following:

- a) Be polite. Do not get abusive in your messages to others.
- b) Use appropriate language. Do not swear, use vulgarities or any other inappropriate language. Illegal activities are strictly forbidden.
- c) Do not reveal your personal address or phone numbers of students or colleagues.
- d) Note that electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
- e) Do not use the network in such a way that you would disrupt the use of the network by other users.
- f) All communications and information accessible via the network should be assumed to be private property.

4) **Warranties** - \_\_\_\_\_ and \_\_\_\_\_ make no warranties of any kind, whether expressed or implied, for the service it is providing. \_\_\_\_\_ School and \_\_\_\_\_ will not be responsible for any damages you suffer. This include loss of data resulting from delays, nondeliveries, misdeliveries, or service interruptions caused by it's own negligence or your errors or omissions. Use of any information obtained via \_\_\_\_\_ or \_\_\_\_\_ is at your own risk. \_\_\_\_\_ and \_\_\_\_\_ specifically deny any responsibility for the accuracy or quality of information obtained through its services.

5) **Security** - Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on Internet, you must notify a system administrator or e-mail \_\_\_\_\_. Do not demonstrate the problem to other users. Do not use another individual's account without written permission from that individual. Attempts to login to Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to Internet.

6) **Vandalism** - Vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet, or any of the above listed agencies or other networks that are connected to the NSFNET Internet backbone. This includes, but not limited to, the uploading or creation of computer viruses.

7) **Updating Your User Information** - Internet may occasionally require new registration and account information from you to continue the service. You must notify Internet of any changes in your account information (address, etc). Currently, there are no user fees for this service.

8) **Exception of Terms and Condition** - All terms and conditions as stated in this document are applicable to the \_\_\_\_\_ County School District and the \_\_\_\_\_. These terms and conditions reflect the entire agreement of the parties and supersedes all prior oral or written agreements and understandings of the parties. These terms and conditions shall be governed and interpreted in accordance with the laws of the State of Indiana, and the United States of America.

I understand and will abide by the above Terms and Conditions for Internet. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken and/or appropriate legal action.

User Signature: \_\_\_\_\_ Date: \_\_/ \_\_/ \_\_

\*\*\*\*\*

PARENT OR GUARDIAN (If you are under the age of 18 a parent or guardian must also read and sign this agreement.)

As the parent or guardian of this student I have read the Terms and Conditions for Internet access. I understand that this access is designed for educational purposes and \_\_\_\_\_ has taken available precautions to eliminate controversial material. However, I also recognize it is impossible for \_\_\_\_\_ to restrict access to all controversial materials and I will not hold them responsible for materials acquired on the network.

Further, I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give permission to issue an account for my child and certify that the information contained on this form is correct.

Parent or Guardian (please print): \_\_\_\_\_

Signature: \_\_\_\_\_ Date \_\_\_\_\_

**8.7 Electronic Mail** -- Email is an effective, accepted, and popular means of communication to and from computer users. It is not considered secure unless it is

encrypted. Consequently, any authorized transmission of confidential, sensitive or private information should be encrypted and sent as an email attachment.

**8.7.1 Acceptable Email Usage** -- Acceptable use of email policies should be implemented at the same time an email system is made available to users of a computer system or network. School and system administrators should provide system users with a copy of the policies. Users should be required to sign a statement that they have read and agree to comply with the policies.

**8.7.2 Potential Email Problems** -- The use of email by school computer system users presents potential problems.

**8.7.2.1 Accidents** -- Since security of confidential information is a requirement, any accidental transmission of that information could cause personal and legal consequences. Consequently, it is important to make sure that security accidents do not occur. A procedure should be in place as to how any accidents will be addressed.

**8.7.2.2 Email Threats** -- There are many kinds of threats, both external and internal, can impact an email system. Email use policies need to be communicated to all email system users. Users should be required to sign an acknowledgment that they have read and agree to comply with the policies before they are allowed to use the email system.

**8.7.2.3 Harassment** -- Email systems can be used for harassment of other users. If any users are feeling harassed they need to know the policy for reporting any threats or harassment to school and system administrators. School administrators and school boards can be held liable for these kinds of incidents that are not addressed after they are reported. Consequently, a well-established policy and system of reporting and handling those reports must be in place.

**8.7.2.4 Impersonation** -- Any incidents of a different person pretending to be a user must be reported immediately.

**8.7.2.5 Eavesdropping** -- This occurs when an outside or inside entity gains unauthorized access to a computer system or network for the purpose of intercepting messages or other information or files.

**8.7.2.6 Mail bombing** -- This is a mechanism used to create thousands of email messages which potentially clog a system and cause it to crash.

**8.7.2.7 Junk mail** -- Junk mail takes up space, wastes users' time and generally wastes system resources. The system email policy should address the method that will be used to handle any junk mail.

### **8.7.3 Use of the email system for personal use**

**8.7.4 Email Safeguards** -- All users must be aware of safeguards that are provided by the network for the email system, as well as safety measures that are expected from users.

Users need to understand that all messages sent with or over the school's email system are property of the school and are subject to inspection or monitoring. This policy is for the protection of the users, the school administration, and the school computer network. In the school environment the security of confidential information and the appropriate use of the email system prevails over the privacy interests of the users.

**8.7.4.1 Protection of Email Messages and Systems** -- all email systems should be protected with anti-virus software to ensure that the school computer network is not adversely affected by any viruses or other harmful programs that enter the system via email messages or attachments. Users should also be aware of what is expected from them to assure email safety.

**8.7.4.2 Retention of Email Messages** -- retention of email messages is often one of the best methods to trace offending messages. This information is also used to provide evidence of harassment, theft, viruses, and other security breaches. Users should be instructed to keep any messages that evidence a potential for system security or personal threat. These messages should immediately be shared with systems administrators, according to the method designated in the email security policy.

**8.7.5 Example Email Policy** -- see policies above. In addition, see Appendix E for various state email use policies, including but not limited to the following:

- State of New Jersey Email Use policy --  
<http://www.state.nj.us/cio/policy/emailpolicy.pdf>
- Oregon Public Education Network policy --  
<http://www.open.k12.or.us/sitedocs/serverdocs/deployment/spam.html>
- State of Arizona Email Use policy --  
<http://www.gita.state.az.us/Standards/E-Mail%20Use%20Policy.html>

---

Resources used to formulate this chapter were primarily the following: NIST's Internet Security Policy: A Technical Guide by Barbara Guttman and Robert Bagwill at <http://csrc.ncsl.nist.gov/isptg/> [13] and Safeguarding Your Technology at <http://nces.ed.gov/pubs98/safetech/> [30].

---

Draft 7/9/00 v3

## **9. Administrative Policies & Procedures**

**9.1 Importance of Administrative Policies** -- Policies related to the administration of computer systems and networks are also necessary to ensure that school boards, administrators, teachers, and staff are not found liable for breaches in any data security measures.

**9.1.1 Legal Implications** -- School systems are responsible for the security of all confidential, sensitive, and private information that is entrusted to them and which resides on their computer systems. If this information or data is compromised school boards, administrators, and teachers could be found liable for this information being revealed in any way that is not authorized by statute or the individuals whose information is compromised. This is one of the major reasons for the formulation of data security policies on all levels. See FERPA Fact Sheet link in Appendix B.

**9.1.2 Responsibility of all members of the education team** -- each member of the education team from teachers to school board members have a level of responsibility that they should be aware of, should be trained about, and should respect. Security breaches provide not only legal vulnerabilities, but credibility and trust vulnerabilities.

**9.2 Administrative security** -- Top level administrators must have access to almost any information related to system users, use patterns, audit trails, confidential and other information, and whatever other level of information that will allow them to do their jobs appropriately. Just because administrators are allowed top level access does not mean that they need top level access. Their requirements will also need to be assessed. If they do not need to access confidential and other levels of information on a regular basis, it is best not to allow access until or if it is needed. A method for special access should be established for occasional access needs.

### **9.2.1 Training and increasing awareness**

**9.2.1.1** All persons involved with the computer system and its confidential, sensitive, or private information need training as to the security requirements involved in using the system, their responsibilities, and their level of security clearance. See Chapter 10 of this document for further training information.

**9.2.1.2** Reasonable efforts are imperative to alert both authorized and unauthorized users that the school computer systems are monitored and

that unauthorized access and use of the system will have legal sanctions. See Chapter 7.

**9.2.2 Reporting of security problems** -- Anyone who encounters actual or potential security problems should be reported to the appropriate systems administrators as soon as the problems are detected.

**9.3 Compliance** -- The overall responsibility of administrators is to ensure that there is compliance with all data security policies and to investigate and sanction all breaches of policies.

**9.3.1 How to follow policy** -- All users of a school's computer system or network must be trained to help them understand how to best follow new and well-established data policies. Users are more likely to comply if they understand the reasons for the policies and the consequences of not following them.

**9.3.2 How policy exceptions are handled** -- There may be times when exceptions to established policies will need to be made. It's important to have a procedure in place to handle potential exceptions. For most data security policies, any exceptions must be addressed by top level systems and other administrators. If the exception approval process is outlined clearly there will be no excuse for not following the procedure if needed.

**9.3.3 Consequences of policy noncompliance** -- All users must understand the consequences for not following security policies. Because breaches of some policies can carry with them legal consequences, those policies need to be specifically addressed. Consequences may range from warnings to exclusion from use of the system to expulsion from the job. Clearly defined consequences define the importance of the policies.

**9.4 Periodic Reviews of the System and its use** -- The need for policies may change as the laws, practice, and technology changes. Consequently, there should be a pre-determined time each year to review the computer system or network and to further refine security policies. This will ensure that the most up-to-date procedures are in place.

**9.5 Password Management Policies** -- Password management is one of the first lines of defense to protect a school's data security system. The risk assessment that determines the level of security measures should be done yearly at a pre-determined time. If there is a higher risk in a particular area than previously, different measures may need to be put into place for greater protection of confidential, sensitive or private information.

**9.6 Granting access to confidential data** -- All users must be assessed as to their need for access to confidential, sensitive, and personal data and information. The job description and other assigned duties will define their needs to which level, and what part of the information. No users should be granted any greater level of access than necessary for them to do their jobs appropriately.

**9.7 Data Security Contingency plans** -- Contingency plans for potential breaches are necessary to ensure that there is a reasonable measured response to infractions or major breaches. Initial plans may fail and backup plans will ensure appropriate responses.

Draft 7/16/00 v2

## 10. Training Protocol

### Educational Administrators and School Board Member Responsibilities

#### **Procedures on how to develop protocol / policy**

1. Policies generally cannot be adopted from another source and issued. Policies must be tailored for each specific organization. Factors that need to be addressed vary from organization to organization. These factors include, but are not limited to, the following:

- objectives
- legal requirements
- organizational design
- organizational culture
- prevailing ethics and morals
- extent of worker education
- the information system technology used by the organization [Wood, pp 2-3]

2. Concepts behind information security policies are similar from organization to organization or school district to school district. Consequently, there are essential ideas that should go into all information security policy statements. See examples in Appendices D, E, and H for examples.

3. One of the best ways to become familiar with the policy factors from #1 above is to do a risk assessment or analysis to determine the organization's unique information security needs. Each of these needs will then be addressed in a policy. [Wood, p 798] An example of network vulnerabilities and defenses charts is displayed in Chapter 3 .

4. Clarify roles and responsibilities related to information security and policy generation. This includes responsibility for issuing and maintaining policies. Identify management staff who will approve the final information security document.

5. Collect and read all existing internal information security awareness materials. List the underlying messages that they contain. Do a brief internal survey to gather ideas that the staff believe should be included in the policy document [Wood, p 798].

6. Identify the persons to receive the policies, their computer knowledge and receptivity to security messages. Decide what orientation or training efforts should be conducted before security policies are issued. Id.

**Training Goals** [Source: Safeguarding, p. 109]

1. Raise levels of awareness of user groups of all information security issues.
2. Make sure that users are aware of local, state, and federal laws and regulations related to confidentiality and security.
3. Explain overall organizational security policies and procedures.
4. Stress that security is a team effort and that each person has an important role in helping to meet security goals and objectives.
5. Train staff to perform the specific security responsibilities of their positions.
6. Alert staff that security all activities will be monitored.
7. Review consequences that accompany breaches in security policies and procedures.
8. Assure staff that reporting potential and actual security breaches and vulnerabilities is their responsibility and is necessary to remedy situations.
9. Convey to users that creating a secure trustworthy system is achievable, and every user plays a part to ensure the realization of this goal.

**Training Resources**

Indiana Assessment System of Educational Proficiencies, Training Manual (June 1999)

I.A.S.E.P. Teacher Resource page  
[http://iasep.soe.purdue.edu/Training\\_info/welcome.htm](http://iasep.soe.purdue.edu/Training_info/welcome.htm)

National Cooperative Education Statistics System & National Center for Education Statistics, Safeguarding Your Technology: Practical Guidelines for Electronic Education Information Security, Chapter 10  
<http://nces.ed.gov/pub98/safetech/>

Charles Cresson Wood, Information Security Policies Made Easy, Version 7 (Sausalito, Ca. October, 1999).

Draft 7/16/00 v2

## **Appendix A: Glossary of Terms**

### **Access**

To approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system or computer network. [KS]

### **Adequate Security**

Security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

### **Agency Confidential Data**

Data which if disclosed to individuals other than those with a specific "need to know" would result in substantial harm to the agency or the State.

### **Application**

The use of information resources (information and information technology) to satisfy a specific set of user requirements.

### **Architectural Security**

Measures taken to guard against adverse occurrences to a structure of networks, computers or programs.

### **Audit**

An independent review and examination of system records and activities in order to test for accuracy of system controls, to ensure compliance with established policy and operational procedures and to detect breaches in security.

### **Authentication**

The process of verifying valid users or processes; the act of requiring the 'person' requesting access to a network, LAN, or system to identify themselves through one or more identification schemes. Screening only makes decisions based on source and destination addresses. Authentication makes decisions based on 'who' was at the source. Authentication can be as simple as a computer ID and password or as complex as one time passwords, challenge response passwords, or physical identification (retinal, voice, image, etc). [NIST Policy at 33, KS]

### **Computer**

An electronic device which performs work using programmed instruction and which has one or more of the capabilities of storage, logic, arithmetic or communication

and includes all input, output, processing, storage, software or communication facilities which are connected or related to such a device in a system or network. [KS]

**Computer Crime**

- (a) Willfully and without authorization gaining or attempting to gain access to and damaging, modifying, altering, destroying, copying, disclosing or taking possession of a computer, computer system, computer network or any other property;
- (b) Using a computer, computer system, computer network or any other property for the purpose of devising or executing a scheme or artifice with the intent to defraud or for the purpose of obtaining money, property, services or any other thing of value by means of false or fraudulent pretense or representation; or
- (c) Willfully exceeding the limits of authorization and damaging, modifying, altering, destroying, copying, disclosing or take possession of a computer, computer system, computer network or any other property. [KS]

**Computer Network**

The interconnection of communications lines, including microwave or other means of electronic communication, with a computer through remote terminals, or a complex consisting of two or more interconnected computers. [KS]

**Computer Program**

A series of instructions or statements in a form acceptable to a computer which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer system. [KS]

**Computer Security Policy**

The documentation of computer security decisions. Managers face hard choices when making computer security decisions. These choices involve organizational strategy, competing objectives, resource allocation, protecting technical and information resources and guiding employee behavior. [NIST policy]

**Computer Software**

Computer programs, procedures and associated documentation concerned with the operation of a computer system. [KS]

**Computer System**

A set of related computer equipment or devices and computer software which may be connected or unconnected. [KS]

**Computerized Data**

Data in a form suitable for processing by computers.

**Confidential Information**

The most sensitive student information that is intended strictly for use within the school. This information is exempt from disclosure under the provisions of the

Freedom of Information Act or other applicable federal laws or regulations. Its unauthorized disclosure could seriously and adversely impact the school, its students and their parents, its teachers and administrators, and the school board. Health care-related information should be considered at least CONFIDENTIAL. [NIST]

### **Confidentiality**

A person's obligation not to disclose or transmit information to unauthorized parties. Confidentiality extends to information about individuals and organizations. "In schools, districts, or state education agencies, that usually means establishing procedures that limit access to information about students or their families. This access extends to the school officials who work directly with the students, agency representatives who serve as evaluators or auditors, or individuals who act on behalf of authorized education officials." [Primer for Privacy, I-4]

### **Critical Data**

Computerized data without which normal business operations would be significantly disrupted or seriously impaired. This includes vital records and data necessary for the life, health, welfare, or safety of citizens.

### **Data**

Raw information that lacks the context to be meaningful. When data is placed in a context, it becomes information.

### **Data Custodians**

Persons responsible for storing, processing, distribution, and communicating computerized data.

### **Data Users**

Persons who have access privileges to computerized data.

### **Dissemination**

The school - initiated distribution of information to the public. Not considered dissemination within the meaning of this Circular is distribution limited to government employees or agency contractors or grantees, intra- or inter-agency use or sharing of government information, and responses to requests for agency records under the Freedom of Information Act (5 U.S.C. 552) or Privacy Act.

### **Digital certificate**

An attachment to an electronic transmission that allows the recipient to authenticate the identity of the sender via third party verification from an independent certificate authority.

### **Digital Signature**

A code attached to an electronic message that is used to verify that the individual sending the message is really who he or she claims to be.

### **Directory Information**

The part of the education record which "includes personal information about a student that can be made public according to a school system's student records policy. Directory information may include a student's name, address, and telephone number, and other information typically found in school yearbooks or athletic programs." [Council of Chief State School Officers (written by Policy Studies Associates, Inc.), printed by National Center for Education Statistics for the National Forum on Education Statistics. (January, 1997)]

### **Disclosure**

"[P]ermitting access to, revealing, releasing, transferring, disseminating, or otherwise communicating all or any part of any individual record orally, in writing, or by electronic or any other means to any person or entity." [Primer for Privacy I-4] The terms disclosure and release may be used interchangeably.

### **Educational Record**

Includes "a range of information about a student that is maintained in schools in any recorded way, such as handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche . . . . Personal notes made by teachers and other school officials that are not shared with others are not considered education records. Additionally, law enforcement records created and maintained by a school of district's law enforcement unite are not education records." [Council of Chief State School Officers (written by Policy Studies Associates, Inc.), printed by National Center for Education Statistics for the National Forum on Education Statistics. (January, 1997)]

### **Educational Records**

Those records that are directly related to a student and maintained by an educational agency or institution or by a party acting for the agency or institution. [34 CFR 99.3 identifies several types of records that are not educational records.] [Young, IN]

### **Encryption**

The process of translating a file into an unintelligible format, or to encode it, via the use of mathematical algorithms or other encoding mechanisms. To open the document, the recipient must have a matching key to decrypt and read the message.

### **Firewall**

A computer or other communications device used to control access to/from a network or computer. The firewall shields a system from potential attacks by unauthorized individuals. [KS]

### **Government Information**

Information created, collected, processed, disseminated, or disposed of by or for the State or Federal Government.

### **Government Publication**

Information which is published as an individual document at government expense, or as required by law. (44 U.S.C. 1901)

### **Guidelines**

[Written statements designed] to assist users, systems personnel, and others in effectively securing their systems. The nature of guidelines, however, immediately recognizes that systems vary considerably and imposition of standards is not always achievable, appropriate, or cost-effective. An organization guideline may, for example, be used to help develop system-specific standard procedures. Guidelines are often used to help ensure that specific security measures are not overlooked, although they can be implemented, and correctly so, in more than one way.

### **Information**

Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. Raw data that has taken on meaning by being placed in a context.

### **Information Dissemination Product**

Any book, paper, map, machine-readable material, audiovisual production, or other documentary material, regardless of physical form or characteristic, disseminated by an agency to the public.

### **Information Life Cycle**

The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

### **Information Management**

The planning, budgeting, manipulating, and controlling of information throughout its life cycle.

### **Information Resources Management**

The process of managing information resources to accomplish agency missions. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and information technology.

### **Information System**

A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

### **Information System Life Cycle**

The phases through which an information system passes, typically characterized as initiation, development, operation, and termination.

### **Information Security Officer**

A person who is responsible for reviewing the implementation of state and departmental policies and standards regarding the security of information pertaining to his respective agency.

### **Information Technology**

The hardware and software operated by an agency or by a contractor of an agency or other organization that processes information on behalf of the government to accomplish a governmental function, regardless of the technology involved, whether computers, telecommunications, or others. It includes automatic data processing equipment [as defined in Section 111(a)(2) of the Federal Property and Administrative Services Act of 1949].

### **Intellectual Property**

The tangible or intangible results of research, development, teaching, or other intellectual activity. This includes things such as original written materials, software, trademarks, or product designs.

### **The Internet**

"The international formal Department of Defense data network formed during the late 60's and early 70's. This network interconnects millions of computers worldwide. The protocol used on this network is strictly TCP/IP. There is a standardized naming and addresses policy for any site connected to this network." [KS]

### **Major Application**

An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

### **Non-Records**

All identical copies of forms, records, reference books, and exhibit materials which are made, or acquired, and preserved solely for reference use, exhibition purposes, or publication and which are not included within the definition of a record. [Young, IN]

### **Non-Repudiation**

Proof of origin of data, proof of original content, proof of delivery, and proof of original content received. This ensures that a message or transaction was initiated by

the identified sender and received by the identified receiver. It protects against later denying responsibility for involvement in a communication. [Miller]

### **Organizational Standards**

These specify uniform use of specific technologies, parameters, or procedures when such uniform use will benefit an organization. Standardization of organization-wide identification badges is a typical example, providing ease of employee mobility and automation of entry/exit systems. Standards are normally compulsory within an organization.

### **Personal Records**

"1.) All documentary materials of a private or non-public character which do not relate to or have an effect upon the carrying out of the constitutional, statutory, or other official or ceremonial duties of a public official, including: diaries, journals, or other personal notes serving as the functional equivalent of a diary, or journal which are not prepared or utilized for, or circulated or communicated in the course of, transacting government business; or

2.) Materials relating to private political associations, and having no relation to or effect upon the carrying out of constitutional, statutory, or other official or ceremonial duties of a public official and are not deemed public records." [Young, IN]

### **Policy**

Policy is written at a broad level. Therefore, organizations also develop standards, guidelines, and procedures which offer users, managers, and others a clearer approach to implementing policy and meeting organizational goals. Standards and guidelines specify technologies and methodologies to be used to secure systems. Procedures are yet more detailed steps to be followed to accomplish particular security-related tasks. Standards, guidelines, and procedures may be disseminated throughout an organization via handbooks, regulations, or manuals.

### **Privacy**

"Privacy is a uniquely personal right that reflects an individual's freedom from intrusion. Protecting privacy means ensuring that information about individuals is not disclosed without their consent. A student's right of privacy . . . [w]hile confidentiality . . . refers to restricting disclosure of information to authorized individuals only, privacy refers to protection from personal intrusion." [Primer for Privacy I-4]

### **Private Data**

This refers to data of a personal nature, which if disclosed to individuals other than those with an authorized "need to know" would be seriously detrimental to an individual or would be an invasion of a person's right to privacy. This applies to information covered by federal or State privacy laws and information ordered private

by a court. Its unauthorized disclosure could seriously and adversely impact the student and the school.

### **Procedures**

These normally assist in complying with applicable security policies, standards, and guidelines. They are detailed steps to be followed by users, system operations personnel, or others to accomplish a particular task (e.g., preparing new user accounts and assigning the appropriate privileges).

### **Property**

This includes, but is not limited to, financial instruments, information, electronically produced or stored data, supporting documentation and computer software in either machine or human readable form and any other tangible or intangible item of value. [KS]

### **Protocol**

A set of conventions governing the treatment and especially the formatting of data in an electronic communications system. (Webster's Ninth New College Edition)

### **Public Information**

All information that does not clearly fit into the sensitive, confidential or private information classifications. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact the school, its employees, and/or its students.

### **Record**

All documentation of the informational, communicative or decision-making processes of state government, its agencies and subdivisions made or received by any agency of state government or its employees in connection with the transaction of public business or government functions, which documentation is created, received, retained, maintained, or filed by that agency or its successors as evidence of its activities or because of the informational value of the data in the documentation, and which is generated on: 1) paper or paper substitutes; 2) photographic or chemically-based media; 3) magnetic or machine readable media; 4) any other materials, regardless of form or characteristics. [Young, IN]

### **Records**

All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the government or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of the data in them. Extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included. (44 U.S.C. 3301)

### **Records Management**

The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations. (44 U.S.C. 2901(2))

### **Retention Schedule**

A set of instructions prescribing how long a record series shall be kept. [Young, IN]

### **Router**

A communications device that 'decides' which path or circuit collections of data (packets) should be sent. Decisions are made based on what is the 'best' path to send a packet to its destination address. Best can be determined by many factors such as line speeds, cost of service (leased versus phone lines), and other factors. [KS]

### **Security Policy**

A collection of statements about the sensitivity of information on a system or LAN, the requirements for how that data must be protected, and the actions to be taken in the event the protection is violated. [KS]

### **Sensitive Information**

Information that requires special precautions to assure the integrity of the information, by protecting it from unauthorized modification or deletion. It is information that requires a higher than normal assurance of accuracy and completeness. Examples of sensitive information include school financial transactions and regulatory actions. [NIST, p.20]

### **Services**

They include, but are not limited to, computer time, data processing and storage functions and other uses of a computer, computer system or computer network to perform useful work. [KS]

### **Supporting Documentation**

This includes, but is not limited to, all documentation used in the construction, classification, implementation, use or modification of computer software, computer programs or data. [KS]

### **Telnet**

A TCP/IP application that enables PC's to 'emulate' or mimic the function of a terminal across a TCP/IP network (such as the Internet) for accessing a remote computer. [KS]

Draft 5/12/00; modified 6/12/00.

## **Appendix B: Related Federal Laws**

Family Educational Rights and Privacy Act (FERPA)  
<http://web.indstate.edu/soe/iseas/ferpa.html>

## **Appendix C: Related State Laws**

To access Appendix C, please view the document online at  
[http://arc.soe.purdue.edu/protocol/home\\_page.htm](http://arc.soe.purdue.edu/protocol/home_page.htm)

## **Appendix D: Related Federal Data Security Policies**

The following resources are examples of data security policies on a broader scale:

1. National Institute of Standards and Technology [NIST], Computer Security Resource Clearinghouse, Federal Requirements and Policy Examples (May 4, 2000), <http://csrc.ncsl.nist.gov/policies/welcome.html>
2. The National Security Telecommunications and Information Systems Security Committee [NSTISSC], Library of Data Security Policy Documents (March 7, 2000), <http://www.nstissc.gov/html/library.html>
3. Organization of Economic Co-operation and Development [OECD], "Guidelines on the Protection of Privacy and Transborder Flows of Personal Information" (January 5, 1999), <http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM>
4. OECD, "Guidelines for the Security of Information Systems," (July 1, 1997), [http://www.oecd.org//dsti/sti/it/secur/prod/e\\_secur.htm](http://www.oecd.org//dsti/sti/it/secur/prod/e_secur.htm)
5. OECD, "Implementing the OECD Privacy Guidelines in the Electronic Environment: focus on the Internet," (October, 1997) <http://www.oecd.org//dsti/sti/it/secur/prod/reg97-6e.pdf>
6. OECD, "Inventory of Instruments and Mechanisms Contributing to the Implementation and Enforcement of the OECD Privacy Guidelines on Global Networks," (May 11, 1999) [http://www.olis.oecd.org/olis/1998doc.nsf/4cf568b5b90dad994125671b004bed59/0663f1ef6343f3a78025677d00529a52/\\$FILE/05E95540.ENG](http://www.olis.oecd.org/olis/1998doc.nsf/4cf568b5b90dad994125671b004bed59/0663f1ef6343f3a78025677d00529a52/$FILE/05E95540.ENG)
7. OECD, "Practices to Implement the OECD Privacy Guidelines on Global Networks," (September, 1998) [http://appli1.oecd.org/olis/1998doc.nsf/4cf568b5b90dad994125671b004bed59/ac229791c57176e3c12566e3003e051c/\\$FILE/12E81114.ENG](http://appli1.oecd.org/olis/1998doc.nsf/4cf568b5b90dad994125671b004bed59/ac229791c57176e3c12566e3003e051c/$FILE/12E81114.ENG)

## **Appendix E: Related State Policies**

To access Appendix E, please view the document online at  
[http://arc.soe.purdue.edu/protocol/home\\_page.htm](http://arc.soe.purdue.edu/protocol/home_page.htm)

## **Appendix F: Data Security & Technology Resources**

1. Faulkner & Gray, "Guide to Health Data Security" (2000),  
<http://www.faulknergray.com/health/ghs.htm>
  
2. Rothstein Catalogue on MIS Disaster Recovery,  
<http://www.rothstein.com/data/cg040001.htm>  
and <http://www.rothstein.com/data/cg230001.htm>
  
3. Harvard University, Information Security Handbook (November, 1991),  
<http://all.net/books/document/Harvard.html>
  
4. Department of Defense, "Trusted Computer System Evaluation Criteria,"  
(August 15, 1983), <http://www.alw.nih.gov/Security/FIRST/papers/criteria/tcsec.txt>
  
5. Online Privacy Alliance, "Guidelines for Online Privacy Policies," (2000),  
<http://www.privacyalliance.org/resources/ppguidelines.shtml>
  
6. Computer Information & Networking Services, "Computer Network and Usage  
Policies," (May 8, 2000), <http://cins.colstate.edu/policies/index.htm>
  
7. Charles Cresson Wood, Information Security Policies Made Easy (7th ed.),  
<http://www.baselinesoft.com/>
  
8. Center for Information Technology, National Institutes of Health,  
Computer Security Information Table of Contents (January 1999)  
<http://www.alw.nih.gov/Security/tcontents.html>

## **Appendix G: Indiana State Requirements and Model Policies**

[160-4-7-.06 Confidentiality of Personally Identifiable Information](#)

[Education Records](#)

[State of Indiana Requirements for Public School Internet Acceptable Use Policies and Guidelines](#)

[State of Indiana Recommendations for Public School Internet Acceptable Use Policies and Guidelines](#)

[Model Acceptable Use Policy published by the Indiana Department of Education](#)

[Sample Acceptable Use Policy and Application for Classroom use of the Internet](#)

[Rule 8: Confidentiality of Information \(with appendices\)](#)

## **160-4-7-.06 Confidentiality of Personally Identifiable Information**

(Identifier Code: IDDF (6))

(1) Identification and Location Procedures.

(a) Notice to Parents.

1. Each local school system (LSS) shall provide adequate public notice to fully inform parent(s)/guardian(s) regarding the requirements related to the identification, location and evaluation of students with disabilities. This includes giving public notice published or announced in newspapers or other media, or both, prior to conducting any major identification, location or evaluation activity. Provision for such notice shall be described annually in each LSS comprehensive plan.

2. Such notice shall be given in native languages appropriate to population groups served by the LSS.

3. Each LSS shall provide adequate public notice to fully inform parent(s)/guardian(s) that personally identifiable information is maintained on students who are eligible for special education services.

4. Information that could identify an individual student shall not be maintained beyond the local level collecting it and shall not be held by any state-level agency except to the extent necessary to carry out the provisions of this rule.

5. The parent(s)/guardian(s) maintain(s) the right to inspect any and all data that are subject to collection and to appeal the accuracy of any such information. The access of unauthorized persons to personally-identifiable data without parent/guardian consent is forbidden.

6. One person in each local agency shall have responsibility for persons having access to these data. The parent(s)/guardian(s) shall be notified and asked to consent to submission prior to entering any personally-identifiable data for this collection.

7. Each LSS shall provide adequate public notice to all parent(s)/guardian(s) concerning the policies and procedures which the LSS follows regarding storage, disclosure to third parties and retention and destruction of personally identifiable information. The notice shall include a description of all the rights of parents and students regarding the confidentiality of personally identifiable information and access to records, including the

rights under Section 438 of the General Education Provisions Act and Part 99 of Title 34 of the Code of Federal Regulations.

8. A statewide news release shall be sent annually to all state and local newspapers with a description of the Child Find program and an address and telephone number of a contact person for further information.

(b) Confidentiality Requirements.

1. Access Rights. Each public agency shall permit the parent(s)/guardian(s) to inspect and review any education records relating to his/her/their children which are collected, maintained or used by the agency.

(i) The public agency shall comply with a request without unnecessary delay and before any meeting regarding an IEP or hearing relating to the identification, evaluation or placement of the child, and in no case more than 45 days after the request has been made.

2. The right to inspect and review education records includes:

(i) The right to a response from the participating agency to reasonable requests for explanations and interpretations of the records;

(ii) The right to request that the agency provide copies of the records containing the information if failure to provide those copies would effectively prevent the parent(s)/guardian(s) from exercising the right to inspect and review the records; and

3. The right to have a representative of the parent(s)/guardian(s) inspect and review the records.

(i) Each public agency shall presume that the parent(s)/guardian(s) has/have the authority to inspect and review records relating to his/her/their child unless the agency has been advised that the parent(s)/guardian(s) does/do not have the authority under applicable state law governing such matters as guardianship, separation and divorce.

4. Records of Parties Obtaining Access. Each public agency shall keep a record of parties obtaining access to data collected or maintained (except access by the parent(s)/guardian(s) and authorized employees of the education agency), including the name of the party, the date access was given and the purpose for which the party is authorized to use the data.

5. Records on More Than One Child. If any record includes data on more than one student, the parent(s)/guardian(s) of those students shall have the right to inspect and review only the data relating to their child or be informed of that specific data.

6. List of Types and Locations. Upon request, the agency shall provide the parent(s)/guardian(s) a list of the types and locations of data collected, maintained or used by the agency.

7. Fees. Upon request, parent(s)/guardian(s) may obtain copies of data for a duplication fee; however, if they provide ample evidence of inability to pay such fee, the data shall be provided free of charge. The participating agency shall not charge a fee to search for and retrieve information. Access to such data, if requested, is the right of each parent/guardian and shall not be denied by the public agency due to physical limitations or geographical locations.

(c) Amendment of Records.

1. The parent(s)/guardian(s) who believe(s) that data collected or maintained is/are inaccurate or misleading or violates the privacy or other rights of the student may request that the local school system amend the data.

2. The agency shall decide whether to amend the data in accordance with the request within a reasonable period of time of receipt of the request not to exceed 30 school days.

3. If the agency decides to refuse to amend the data in accordance with the request, it shall inform the parent(s)/guardian(s) of the refusal and advise the parent(s)/guardian(s) of the right to a hearing.

(d) Results of Hearing.

1. If, as a result of the hearing, the agency decides that the information is inaccurate, misleading or otherwise in violation of the privacy or other rights of the student, it shall amend the information accordingly and so inform the parent(s)/guardian(s) in writing.

2. If, as a result of the hearing, the agency decides the data are accurate and not misleading or otherwise in violation of the privacy or other rights of the student, it shall inform the parent(s)/guardian(s) of his/her/their right to place in the record it maintains on the student, a statement commenting on the data and setting forth their reasons for disagreeing with the decision of the public agency.

3. Any explanation placed in the records of the student shall be maintained by the public agency as part of the records of the student as long as the record or contested portion thereof is maintained by the agency. If the records of the student or the contested portion thereof, is disclosed by the public agency to any party, the explanation shall also be disclosed to the party.

(e) Consent.

1. Every effort shall be made to ensure that: the parent(s)/guardian(s) has/have been fully informed of the information in his/her/their native language; the parent(s)/guardian(s)

understand(s) and agree(s) in writing to the release of information and records shall be sent; and the parent(s)/guardian(s) understand(s) that the granting of consent is voluntary.

2. Signed informed parental/guardian consent shall be obtained before disclosure of data to anyone or in any manner other than:

(i) to parent(s)/guardian(s) or eligible students;

(ii) To school officials, including teachers within the LSS or legally constituted cooperating agencies, e.g., Psychoeducational Programs, Regional Educational Service Agencies (RESAs) or shared services, when access has legitimate educational purposes;

(iii) In connection with a student's application for or receipt of financial aid;

(iv) With the written approval of the local school superintendent, to organizations conducting a study on behalf of an education agency to develop, validate or administer predictive tests, to administer student aid or to improve instruction and will be available only to those conducting the study with all personally-identifiable data destroyed when they are no longer needed for the purpose of the study;

(v) To accreditation agencies;

(vi) In compliance with a judicial order;

(vii) To authorized state or federal representatives evaluating or auditing federally-supported educational programs;

(viii) To the Office for Civil Rights;

(ix) To officials of other schools or school systems in which the student seeks or is eligible to enroll, upon condition that the student's parent(s)/guardian(s) be notified of the transfer, receive a copy of the record if desired and have an opportunity for a hearing to challenge the content of the record;

(x) To a Department of Human Resources (DHR) facility for the purpose of making appropriate educational decisions;

(xi) For any use or purpose other than meeting a requirement under this part.

(f) Safeguards.

1. The local school superintendent or designee shall ensure the confidentiality of any personally-identifiable data.

2. All persons collecting or using personally-identifiable data shall receive instruction regarding Georgia Department of Education (GDOE) policies and procedures for use of data.

3. The public agency shall maintain for public inspection a current list of the names and positions of employees within the local school system who may have access to personally-identifiable data. This list shall include teachers and administrators directly involved in the educational interest of the student and others as designated in writing by the superintendent under guidelines established by the local board of education.

4. Whenever educational records of a student are released, the public agency shall:

(i) Maintain a record of those who have had access to the educational records and for what purpose (except for teachers and administrators in the local school);

(ii) Provide access to these records to the parent(s)/guardian(s) or eligible students;

(iii) Specify in writing that persons receiving such records shall not permit access by third parties without the written consent of the parent(s)/guardian(s) or eligible student.

(iv) Transfer personally-identifiable data used in making and maintaining placement in special education programs to another local school system which the student plans to attend. The parent(s)/guardian(s) or eligible student shall be informed and, upon request, receive a copy of all information transmitted.

(v) Protect the confidentiality of personally-identifiable information at collection, storage, disclosure and destruction stages.

(g) Destruction of Data.

1. The public agency shall establish a procedure for destruction of data, inform parent(s)/guardian(s) that personally-identifiable information collected, maintained or used in the provision of a free appropriate public education is no longer needed to provide educational services to the student. These procedures shall be in accordance with Family Educational Rights and Privacy Act (FERPA) and Georgia Records Act.

2. The information shall be destroyed at the request of the parent(s)/guardian(s). However, a permanent record of a student's name, address and telephone number, grades, attendance record, classes attended, grade level completed and year completed may be maintained without time limitation.(h) Student's Rights. Whenever a student with a disability has attained 18 years of age, all rights contained in this part shall be transferred from the parent(s)/guardian(s) of the student to the student upon taking into consideration the student's age and type and/or severity of disability.

(i) Enforcement. The GDOE shall ensure that these policies and procedures are followed and that the requirements of these rules are met through the Program Review Process.

Authority O.C.G.A. § 20-2-152; 20-2-168; 20-2-1160.

Adopted: September 8, 1994      Effective: October 9, 1994

DOE:  
Office of Special Service  
Division for Exceptional Students

## **Education Records (from the Mauve Manual)**

### Contents:

[I. Definitions](#)

[II. Rights of a Parent and An Eligible Student](#)

[III. Custody and Protection of Education Records](#)

[IV. Access to Education Records](#)

[V. Disclosure of Education Records to Third Parties](#)

[VI. Correction of Education Records](#)

[VII. Copies of Education Records](#)

[VIII. Release of Directory Information](#)

[IX. Education Record Retention Requirements](#)

[Attached Document: Annual Notice to Parents and Students of Their Rights Concerning Education Records](#)

### **I. Definitions**

A. Education Records. Education records are those official records, files, and data directly related to a student and maintained by the school corporation. Such records encompass all the material kept in the student's cumulative folder and include such information as general identifying data, records of attendance and of academic work completed, records of achievement, results of evaluative tests, health data, disciplinary records, test protocols, and individualized education programs. Education records are the property of the school corporation. Access to and correction of education records is governed by this policy.

1. Exclusions. Education records do not include the following:
  - a. Data which relates to a student or groups of students but by which the student(s) cannot be identified.
  - b. Records kept in the sole possession of the maker and which are not accessible or revealed to other persons. Such records may include grade books, notes on student work, transcripts of interviews, counselors' notes, and memory aids.
  - c. Privileged communications made under IC 20-6.1-6-15 and information required to be furnished to law enforcement or social services agencies relating to suspected child abuse or neglect under IC 31-6-11.

B. Parent. Parent is a parent of a student and includes natural parent, a guardian, or an individual acting as a parent in the absence of a parent or guardian. The term includes the custodial and noncustodial parent of a student.

C. Student. Student is any individual who is or has been in attendance at the school corporation.

D. Eligible Student. Eligible student is a student who has reached eighteen (18) years of age or is attending a post-secondary education institution.

E. Disclosure. Disclosure is to permit access to, release of, transfer of, or communication of, education records or personally identifiable information from education records to any party by any means, including oral, written, or electronic means.

F. Personally Identifiable Information. Personally identifiable information is information by which it is possible to identify a student with reasonable certainty including, but not limited to, the following:

1. The name of a student, a student's parent, or any other family member.
2. The address of a student.
3. A personal identifier such as a student's social security number.
4. A list of personal characteristics, including disability designation.

## **II. Rights of a Parent and An Eligible Student**

A. Rights of a parent. The rights afforded to a parent under this policy shall be given to either parent, including a custodial and noncustodial parent, unless the school corporation has been provided with evidence of a court order or other legally binding document relating to such matters as divorce, separation, or custody that specifically revokes these rights.

B. Rights of an eligible student. The rights afforded to a parent under this policy shall transfer to a student when the student becomes an eligible student, as defined in this policy, unless the student has been adjudicated incompetent by a court or the type and severity of the student's disabling condition would make a transfer inappropriate.

## **III. Custody and Protection of Education Records**

A. Place records are kept. Education records will generally be maintained in the cumulative record folders either in the administrative offices of the school corporation, in the special services office, or in the school in which the student is currently enrolled. With the consent of the superintendent or the superintendent's designee, a portion of

education records may be kept in other places for reasons of effective school administration. Upon request, a list of the types and locations of education records will be provided to a parent or eligible student.

B. Control of the records. Education records shall be under the immediate control of the person in charge of the building where the education records are maintained. This person shall be responsible for carrying out this policy.

C. Record of access to education records. Each individual student cumulative folder, and each student record maintained separate from the folder, shall contain as part thereof a written form upon which any person examining such records shall indicate the following:

1. The identity of such person.
2. The specific record examined.
3. Purpose of the examination.
4. The date on which, or in the case of a person whose job within the school corporation system requires repeated examination, the period of time over which such examinations were made.

No such record need be kept when the disclosure was a to a parent or eligible student, school staff members with legitimate educational interest, a party with a written consent from the parent or eligible student, or a party seeking directory information.

#### **IV. Access to Education Records**

A. Right of access. A parent, a student, or an eligible student has the right to inspect and review the education records of such student or any part thereof. A representative of the parent or eligible student may also inspect and review such student's education records upon the written consent of the parent or eligible student.

B. Manner of exercising such rights. Such right shall be exercised by presenting a written request to the office of the superintendent or the superintendent's designee. The request shall specify the specific education records which the parent, student, or eligible student wishes to inspect or examine. In the event the school cannot determine the exact records as described, the designated school employee shall immediately contact the parent, student, or eligible student by letter or otherwise, to determine the desired scope of education records to be inspected.

Compliance with all requests to access education records must occur without unnecessary delay and in no case more than forty-five (45) days after a request has been made. If requested, a parent or eligible student must be given access to the student's education

records before any meeting regarding an individualized education program or pending due process hearing.

All inspections of education records shall be made during regular business hours. A school official shall be present during any such inspection to assist in the interpretation of the records.

C. Records involving more than one student. Where the records requested include information concerning more than one student, the parent, student, or eligible student shall either receive for examination that part of the record pertaining to the student of the parent or the student making the request, or where this cannot reasonably be done, be informed of the contents of the part of the record pertaining to the student of the parent or the student making the request.

## **V. Disclosure of Education Records to Third Parties**

A. Disclosure without the consent of the parent or eligible student. The education records of any student shall be available to the following persons, or in the following situations, without the consent of the parent or eligible student:

1. School officials within the school corporation who have legitimate educational interests. Officials with legitimate educational interests are those individuals who, at the time of access, are directly involved in the development and/or delivery of educational services to the student.
2. Officials of another school, school corporation, or institution of postsecondary education where the student seeks or intends to enroll. The parent or eligible student will not be notified of the disclosure of education records to another school, school corporation, or institution of post-secondary education where the student seeks to attend or enroll. The parent or eligible student may receive a copy of the record that was disclosed upon request.
3. Officials of another school, school corporation, or educational agency where the student is enrolled or receiving services. The parent or eligible student will not be notified of the disclosure of education records to another school, school corporation, or educational agency where the student is enrolled or receiving services. The parent or eligible student may receive a copy of the record that was disclosed upon request.
4. Authorized representatives of the Comptroller General of the United States, the Secretary of the Department of Education, and authorized employees of the Indiana Department of Education, provided, however, that except where collection of personally identifiable data is specifically authorized by federal law, any data or copies collected by such officials with respect to individual students shall not include information which would permit the personal identification of any student or their parents.

5. Organizations conducting studies for, or on behalf of, the school corporation for the purpose of developing, validating, or administering predictive tests, and improving instruction.
6. Accrediting organizations in order to carry out their accrediting functions.
7. Parents of a dependent student, as defined in section 152 of the Internal Revenue Code of 1954.
8. Appropriate state or local officials in health or safety emergency where such officials need the information immediately to deal with a serious threat to the health or safety of students or other individuals.
9. Where such information is furnished in compliance with a judicial order and pursuant to any lawfully issued subpoena, upon the condition however, that a parent or eligible student is notified of all such orders or subpoenas as soon as reasonably possible after they are received, and in any event no less than 24 hours before disclosure.

B. Disclosure with consent. Education records may be furnished to any other person only with the written consent of the parent or eligible student.

Such written consent shall specify the records to be released, the reasons the records are to be released, and to whom. To the extent reasonably possible, the school corporation shall release information to persons on the condition that such persons will maintain the confidentiality of the information and will not reveal or disseminate the information to other persons.

## **VI. Correction of Education Records**

A parent or eligible student shall have an opportunity for a hearing to challenge the content of the student's education records to ensure that they are not inaccurate or misleading or otherwise in violation of the rights of privacy or the constitutional rights of the student. If the parent or eligible student believes that such records should be corrected or deleted, the parent or eligible student shall advise the superintendent or the superintendent's designee, who shall provide the parent or eligible student an informal conference. If the school corporation agrees to amend the contents of the records, the change shall occur within ten (10) business days of the date the request is received. The school corporation shall provide the parent or eligible student with notification of the change and a copy of the amended contents if the parent or eligible student requests.

In the event no agreement is reached, the parent or eligible student shall have an opportunity for a hearing to correct or delete the record by filing a statement of the relief requested and a hearing shall be held thereon, and appeals taken, in the same manner as a charge brought under IC 20-8.1-5-14 or, in the case of a student with disabilities, 511 IAC 7-8-1 (p).

## **VII. Copies of Education Records**

Copies of education records may be provided to a parent or eligible student at no charge where such a person is unable because of distance or other valid reason to personally inspect and review the education record. Fees for all other copies shall be assessed by the superintendent or the superintendent's designee. No fees may be assessed for the search or retrieval of education records.

## **VIII. Release of Directory Information**

The school corporation may release certain "directory information," which means information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed and which includes, but is not limited to, the student's name, address, parents' names and their home and work telephone numbers, major field of study, participation in official recognized activities and sports, height and weight of members of athletic teams, dates of attendance, awards received, motor vehicle description (including license plate number), hair and eye color, race, sex, date of birth, height, weight, grade level, and other similar information, without consent to media organizations (including radio, television, and newspapers), colleges, civic or school-related organizations and state or local governmental agencies.

A parent or eligible student who desires to object to disclosure of any or certain of the categories of directory information should request form (Denial of Permission to Release Certain Directory Information Without Prior Written Consent) from the superintendent's office. An objecting parent or eligible student may use this form to deny consent for release of all directory information, or the parent or eligible student may selectively deny consent by circling those categories of directory information the parent or eligible student does not wish released.

Building principals shall ensure that parents and eligible students are informed of their right to object to the release of directory information and that they have fourteen (14) calendar days from the date of receipt of the Annual Notice to Parents and Students of Their Rights Concerning Education Records in which to file an objection.

## **IX. Education Record Retention Requirements**

The school corporation shall maintain all student's education records for at least five (5) years after the student leaves the school corporation. However, a permanent record of directory information may be maintained without time limitation.

For students with disabilities, the parent or eligible student shall be notified when personally identifiable information is no longer needed to provide educational services to the student. This information shall be destroyed at the request of the parent or eligible student.

**Legal Reference:**

20 U.S.C. 1232(g)  
20 U.S.C. 1415(b)(1)(A)  
34 CFR Part 99  
34 CFR §300.129  
34 CFR §§300.560-300.574  
IC 20-1-1-6  
IC 20-1-6-2.1  
IC 20-10.1-22.4  
511 IAC 7-8-1

511 IAC 7-3-17  
511 IAC 7-3-21  
511 IAC 7-3-41  
34 CFR §300.221

Date Adopted: \_\_\_\_\_

## **Annual Notice to Parents and Students of Their Rights Concerning Education Records**

To Parents and Students:

Education records are governed by federal and state laws and regulations. The requirements of these laws and regulations are contained in school board policy # \_\_\_\_\_, entitled Education Records. Generally, this policy provides for the following:

- (1) Records are confidential and may be disclosed only as provided in the policy.
- (2) The policy concerns both elementary and secondary student education records.
- (3) Parents and students have a right to examine their student's education records at reasonable times.
- (4) Before education records are disclosed to third parties, the school requires a signed and dated written consent of either: (1) a parent of a student who is less than 18 years of age and not attending a post-secondary educational institution; or (2) a student who is at least 18 years of age or attending a post-secondary institution (an eligible student).
- (5) Certain persons may examine education records without a parent's or eligible student's consent, as provided in the above paragraph. These include school officials who have legitimate educational interests; officials of another school, school corporation, or institution of post-secondary education where the student seeks or intends to enroll; and officials of another school, school corporation, or other educational agency in which the student is enrolled or receiving services. This school corporation forwards education records to these agencies without prior notification to the parent or eligible student.
- (6) Directory information will be released to media organizations (including radio, television, and newspapers), colleges, civic or school related organizations, and state or local government agencies without the consent of a parent or eligible student. Directory information includes the student's name, address, parent home and work telephone number, major field of study, participation in official recognized activities and sports, height and weight of members of athletic teams, dates of attendance, awards received, motor vehicle description (including license plate number), hair and eye color, race, sex, date of birth, height, weight, grade level, and other similar information which would not generally be considered harmful or an invasion of privacy if disclosed. A parent or eligible student may object to disclosure of any of the categories of directory information by filing form (Denial of Permission to Release Certain Directory Information Without Prior Written Consent) from the principal's office no later than fourteen (14) calendar days from the date of receipt of this notice.

Very truly yours,

## **State Of Indiana Requirements For Public School Internet Acceptable Use Policies And Guidelines**

Source: <<http://www.siec.k12.in.us/aup/require.html>>

A. 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 the 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.
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 for a student to 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. Safeguarding personal information, such as name, address, telephone number, etc.

Department of Education -- Revised November 1995

## **State Of Indiana Recommendations For Public School Internet Acceptable Use Policies And Guidelines**

Source: <http://www.siec.k12.in.us/aup/recomm.html>

A. It is strongly recommended that each public school corporation in Indiana establish an Internet Acceptable Use Policy that is consistent with existing policies for print media, and that the local Internet Acceptable Use Policy include:

1. A brief explanation of the Internet, content that is available via the Internet, and the potential educational value of student access to the Internet.

2. Disclaimer limiting the school corporation's liability relative to:

A. Information stored on school corporation diskettes, hard drives or servers.

B. Information retrieved through school corporation computers, networks or on-line resources.

C. Personal property used to access school corporation computers, networks or on-line resources.

D. Unauthorized financial obligations resulting from use of school corporation resources/accounts to access the Internet.

3. Parent/Guardian responsibilities.

4. A description of the privacy rights and limitations of school sponsored/managed Internet accounts.

5. Notification that, even though the school corporation may use technical means to limit student Internet access, these limits do not provide a foolproof means for enforcing the provisions of local Acceptable Use Policies.

6. Notification that all provisions of the policy are subordinate to local, state and federal statute.

7. Notification to parents/guardians that it is possible for students to purchase goods and services via the Internet and that these purchases could potentially result in unwanted financial obligations.

B. It is strongly recommended that each public school corporation in Indiana develop guidelines that:

1. Include suggestions to help parents and students to take full advantage of Internet access from home or public access terminals.

2. Require students of an appropriate age to read and sign (indicating their acceptance of the provisions and agreement to comply) the school corporation's Acceptable Use Policy.

3. Describe appropriate staff use of school corporation Internet resources/accounts.

4. For internal use, assign specific staff with specific security, management and account responsibilities associated with the school corporation's Internet resources and accounts.

5. Include procedures for users to subscribe to Internet services, such as list servers and news groups.

Department of Education -- Revised November 1995.

**Model Acceptable Use Policy published by the Indiana Department of Education**

This model meets all the requirements for an AUP for Indiana public school corporations.

Source: <<http://www.siec.k12.in.us/aup/modelaup.html>>

**{SCHOOL DISTRICT} Policy on District-Provided  
Access to Electronic Information, Services, and Networks**

Freedom of expression is an inalienable human right and the foundation for self-government. Freedom of expression encompasses the right to freedom of speech and the corollary right to receive information. Such rights extend to minors as well as adults. Schools facilitate the exercise of these rights by providing access to information regardless of format or technology. In a free and democratic society, access to information is a fundamental right of citizenship.

In making decisions regarding student access to the Internet, the {SCHOOL DISTRICT} considers its own stated educational mission, goals, and objectives. Electronic information research skills are now fundamental to preparation of citizens and future employees. Access to the Internet enables students to explore thousands of libraries, databases, bulletin boards, and other resources while exchanging messages with people around the world. The District expects that faculty will blend thoughtful use of the Internet throughout the curriculum and will provide guidance and instruction to students in its use. As much as possible, access from school to Internet resources should be structured in ways which point students to those which have been evaluated prior to use. While students will be able to move beyond those resources to others that have not been previewed by staff, they shall be provided with guidelines and lists of resources particularly suited to learning objectives.

Outside of school, families bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephones, radio, movies, and other possibly offensive media.

Students utilizing District-provided Internet access must first have the permission of and must be supervised by the {SCHOOL DISTRICT's} professional staff. Students utilizing school-provided Internet access are responsible for good behavior on -line just as they are in a classroom or other area of the school. The same general rules for behavior and communications apply.

The purpose of District-provided Internet access is to facilitate communications in support of research and education. To remain eligible as users, students' use must be in support of and consistent with the educational objectives of the {SCHOOL DISTRICT}. Access is a privilege, not a right. Access entails responsibility. Users should not expect that files stored on school-based computers will always be private. Electronic messages and files stored on school-based computers may be treated like school lockers.

Administrators and faculty may review files and messages to maintain system integrity and insure that users are acting responsibly.

The following uses of school-provided Internet access are not permitted:

- 1.) To access, upload, download, or distribute pornographic, obscene, or sexually explicit material;
- 2.) To transmit obscene, abusive, or sexually explicit language;
- 3.) To violate any local, state, or federal statute;
- 4.) To vandalize, damage, or disable the property of another individual or organization;
- 5.) To access another individual's materials, information, or files without permission; and,
- 6.) To violate copyright or otherwise use the intellectual property of another individual or organization without permission.

Any violation of District Policy and rules may result in loss of District-provided access to the Internet. Additional disciplinary action may be determined at the building level in keeping with existing procedures and practices regarding inappropriate language or behavior. When and where applicable, law enforcement agencies may be involved. The {SCHOOL DISTRICT} makes no warranties of any kind, neither expressed nor implied, for the Internet access it is providing. The District will not be responsible for any damages users suffer, including--but not limited to--loss of data resulting from delays nor interruptions in service. The District will not be responsible for the accuracy, nature or quality of information stored on District diskettes, hard drives, or servers; nor for the accuracy, nature, or quality of information gathered through District-provided Internet access. The District will not be responsible for personal property used to access District computers or networks or for District-provided Internet access. The District will not be responsible for unauthorized financial obligations resulting from District-provided access to the Internet.

Parents of students in the {SCHOOL DISTRICT} shall be provided with the following information:

The {SCHOOL DISTRICT} is pleased to offer its students access to the Internet. The Internet is an electronic highway connecting hundreds of thousands of computers and millions of individual users all over the world. This computer technology will help propel our schools through the communication age by allowing students and staff to access and use resources from distant computers, communicate and collaborate with other individuals and groups around the world, and significantly expand their available information base. The Internet is a tool for life-long learning.

Families should be aware that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate, nor potentially offensive to some people. In addition, it is possible to purchase certain goods and services via the Internet which could result in unwanted financial obligations for which a student's parent or guardian would be liable.

While the District's intent is to make Internet access available in order to further educational goals and objectives, students may find ways to access other materials as well. Even should the District institute technical methods or systems to regulate students' Internet access, those methods could not guarantee compliance with the District's acceptable use policy. That notwithstanding, the District believes that the benefits to students of access to the Internet exceed any disadvantages. Ultimately, however, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. Toward that end, the {SCHOOL DISTRICT} makes the District's complete Internet policy and procedures available on request for review by all parents, guardians, and other members of the community; and provides parents and guardians the option of requesting for their minor children alternative activities not requiring Internet use.

NOTICE: This policy and all its provisions are subordinate to local, state, and federal statutes.

## **Sample Acceptable Use Policy and Application for Classroom use of the Internet**

Adapted from Kevin Barry, Florida Institute of Technology, Academic & Research Computing Services and originally recommended by the Southern Indiana Education Center.

Source: <http://www.siec.k12.in.us/aup/Acceptable.Use.txt>

### TERMS AND CONDITIONS FOR USE OF INTERNET

Please read the following carefully before signing this document. This is a legally binding document. Internet access is now available to students and teachers in the \_\_\_\_\_ County School District. The access is being offered as part of a collaborative project involving \_\_\_\_\_ School, the Indiana Department of Education, and \_\_\_\_\_. We are very pleased to bring this access to \_\_\_\_\_ County and believe the Internet offers vast, diverse and unique resources to both students and teachers. Our goal in providing this service to teachers and students is to promote educational excellence in the \_\_\_\_\_ County Schools by facilitating resource sharing, innovation and communication.

The Internet is an electronic highway connecting thousands of computers all over the world and millions of individual subscribers. Students and teachers have access to:

- 1) electronic mail communication with people all over the world.
- 2) information and news from NASA as well as the opportunity to correspond with the scientists at NASA and other research institutions.
- 3) public domain and shareware of all types.
- 4) discussion groups on a plethora of topics ranging from Chinese culture to the environment to music to politics.
- 5) access to many University Library Catalogs, the Library of Congress, CARL and ERIC.

With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting. \_\_\_\_\_ and \_\_\_\_\_ have taken available precautions to restrict access to controversial materials. However, on a global network it is impossible to control all materials and an industrious user may discover controversial information. We, at \_\_\_\_\_ School, and \_\_\_\_\_ firmly believe that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may procure material that is not consistent with the educational goals of this Project.

Internet access is coordinated through a complex association of government agencies, and regional and state networks. In addition, the smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines. These guidelines are provided here so that you are aware of the responsibilities you are about to acquire. In general this requires efficient, ethical and legal utilization of the network resources. If a \_\_\_\_\_ school user violates any of these provisions, his or her account will be terminated and future access could possibly be denied. The signature (s) at the end of this document is (are) legally binding and indicates the party (parties) who signed has (have) read the terms and conditions carefully and understand (s) their significance.

#### Internet - Terms and Conditions

1) Acceptable Use - The purpose of NSFNET, which is the backbone network to the Internet, is to support research and education in and among academic institutions in the U.S. by providing access to unique resources and the opportunity for collaborative work. The use of your account must be in support of education and research and consistent with the educational objectives of the \_\_\_\_\_ County School District. Use of other organization's network or computing resources must comply with the rules appropriate for that network. Transmission of any material in violation of any US or state regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secret. Use for commercial activities \_\_\_\_\_ is generally not acceptable. Use for product advertisement or political lobbying is also prohibited.

2) Privileges - The use of Internet is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. (Each student who receives an account will be part of a discussion with a \_\_\_\_\_ teacher pertaining to the proper use of the network.) The system administrators will deem what is inappropriate use and their decision is final. Also, the system administrators may close an account at any time as required. The administration, faculty, and staff of \_\_\_\_\_ may request the system administrator to deny, revoke, or suspend specific user accounts.

3) Netiquette - You are expected to abide by the generally accepted rules of network etiquette. These include (but are not limited to) the following:

- a) Be polite. Do not get abusive in your messages to others.
- b) Use appropriate language. Do not swear, use vulgarities or any other inappropriate language. Illegal activities are strictly forbidden.
- c) Do not reveal your personal address or phone numbers of students or colleagues.
- d) Note that electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.

e) Do not use the network in such a way that you would disrupt the use of the network by other users.

f) All communications and information accessible via the network should be assumed to be private property.

4) Warranties -- \_\_\_\_\_ and \_\_\_\_\_ make no warranties of any kind, whether expressed or implied, for the service it is providing. \_\_\_\_\_ School and \_\_\_\_\_ will not be responsible for any damages you suffer. This include loss of data resulting from delays, nondeliveries, misdeliveries, or service interruptions caused by it's own negligence or your errors or omissions. Use of any information obtained via \_\_\_\_\_ or \_\_\_\_\_ is at your own risk. \_\_\_\_\_ and \_\_\_\_\_ specifically deny any responsibility for the accuracy or quality of information obtained through its services.

5) Security - Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on Internet, you must notify a system administrator or e-mail \_\_\_\_\_. Do not demonstrate the problem to other users. Do not use another individual's account without written permission from that individual. Attempts to login to Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to Internet.

6) Vandalism - Vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet, or any of the above listed agencies or other networks that are connected to the NSFNET Internet backbone. This includes, but not limited to, the uploading or creation of computer viruses.

7) Updating Your User Information - Internet may occasionally require new registration and account information from you to continue the service. You must notify Internet of any changes in your account information (address, etc). Currently, there are no user fees for this service.

8) Exception of Terms and Condition - All terms and conditions as stated in this document are applicable to the \_\_\_\_\_ County School District and the \_\_\_\_\_. These terms and conditions reflect the entire agreement of the parties and supersedes all prior oral or written agreements and understandings of the parties. These terms and conditions shall be governed and interpreted in accordance with the laws of the State of Indiana, and the United States of America.

I understand and will abide by the above Terms and Conditions for Internet. I further understand that any violation of the regulations above is unethical and may constitute a

criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken and/or appropriate legal action.

User Signature: \_\_\_\_\_ Date: \_\_\_/\_\_\_/\_\_\_

\*\*\*\*\*

PARENT OR GUARDIAN (If you are under the age of 18 a parent or guardian must also read and sign this agreement.)

As the parent or guardian of this student I have read the Terms and Conditions for Internet access. I understand that this access is designed for educational purposes and \_\_\_\_\_ has taken available precautions to eliminate controversial material. However, I also recognize it is impossible for \_\_\_\_\_ to restrict access to all controversial materials and I will not hold them responsible for materials acquired on the network.

Further, I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give permission to issue an account for my child and certify that the information contained on this form is correct.

Parent or Guardian (please print): \_\_\_\_\_

Signature: \_\_\_\_\_ Date \_\_\_\_\_

## **Rule 8 Confidentiality of Information**

### **511 IAC 7-8-1 Confidentiality Policy and Procedures**

- A. The public agency has in place written policy and procedures regarding how the public agency maintains confidentiality of all educational records collected, maintained, or used. The policy and procedures include:
1. How the parent, or parent's representative, may inspect and review educational records including the procedures the parent must follow to inspect records;
  2. The circumstances under which the public agency believes it may legitimately deny a request for a copy of those records;
  3. A schedule of fees, if any, to be charge for copies of records;
  4. A list of the types and locations of educational records maintained by the public agency, and the titles and addresses of the officials responsible for the records;
  5. A statement that personally identifiable information will not be released from an educational record without the prior written and dated consent of the parent, except as provided in number one (1) above;
  6. A statement indicating whether the public agency has a policy of disclosing personally identifiable information under number one (1) above and, if so, the public agency's criteria for determining:
    - a. which parties are school officials; and,
    - b. what constitutes a legitimate educational interest;
  7. A statement that a record of disclosures will be maintained and that a parent may inspect and review that record.
  8. A list of the types of personally identifiable information that the agency has designated as directory information.
  9. A statement that the public agency permits a parent to:
    - a. Request correction of the student's records in whole or in part;
    - b. Obtain a hearing to contest information in the student's records; and,
    - c. Add statements to the record;
  10. A statement that the policy is available to the parent upon request.
- B. A public agency shall permit the parent, or parent's representative, to inspect and review the educational records of the parent's children ages birth to eighteen (18) collected, maintained or used by the public agency. All rights under this rule pass to the student and become concurrent with the parent's rights when the student reaches age eighteen (18), unless the student has been adjudicated incompetent.
- C. The public agency shall permit the parent, custodial and noncustodial alike, to inspect and review the student's records unless the public agency has received written notice that a court order has terminated or restricted the parent's authority to access the student's records under applicable state law governing matters such as, but not limited to, guardianship, separation, and divorce.

D. The public agency shall comply with a request from a parent to inspect and review the records:

1. Without unnecessary delay;
2. Before any meeting regarding an individualized education program or due process hearing concerning identification, evaluation, or placement of the student; and
3. In no case more than forty-five (45) days after the request is made.

E. The right to inspect and review educational records includes:

1. The right to explanations and interpretations of the records by the public agency;
2. The right to receive copies of the records from the public agency if failure to provide those copies would prevent the parent from exercising the right to inspect the records;
3. The right to have a representative of the parent inspect and review the records; and
4. The right to receive a copy of the student's educational record from the public agency for use in a contemplated or pending due process hearing.

F. The public agency may charge a fee for copies of records, not to exceed actual cost of duplication, that are made for a parent unless the payment of the fee prevents the parent from exercising the right to inspect and review the records. The public agency may not charge a fee to search for or to retrieve information.

G. If an educational record includes information on more than one student, the parent has the right to inspect and review only the information relating to the parent's child, or to be informed of that specific information.

H. The public agency shall maintain for public inspection a current listing of the names and positions of those employees within the public agency authorized the access personally identifiable information.

I. The public agency shall keep a record of each access to, and disclosure of, personally identifiable information from the educational record of each student, except when the access or disclosure has been by or to parents or authorized public agency employees. The record shall be kept with the educational record as long as the educational record is kept. The access and disclosure record shall include:

1. The name of the person gaining access to the record or receiving personally identifiable information from the record;
2. The date of access or disclosure; and,
3. The reason the person is gaining access to the record.

J. The public agency shall provide the parent upon request a list of the types and locations of educational records collected, maintained or used by the public agency.

K. Except as specified in subsection (L) below, written and dated parental consent shall be obtained before personally identifiable information is disclosed to anyone other than the parent or authorized employees of the public agency, or before the information is used for any purpose other than those specified in Rule 8. The consent shall specify the following:

1. The records that may be disclosed;
2. The purpose of the disclosure; and,
3. The person or class of persons to whom the records may be disclosed.

L. The public agency may request a due process hearing when the parent refuses consent for disclosure of information.

M. The public agency may allow access to, or disclose information from, an educational record without parental consent under any of the following conditions:

1. The access or disclosure is to authorized public agency employees whom the agency has determined to have legitimate educational interests;
2. The public agency policy includes notice that the agency forwards educational records to another public agency in which the student intends to or has enrolled.
3. The access or disclosure is to federal or state education authorities for audit, evaluation, or accreditation purposes, or for the enforcement of, or compliance with, legal requirements related to federal and state supported education programs;
4. When a student is enrolled in more than one (1) public agency or receives services from more than one (1) public agency, the agencies involved may disclose to each other information from the student's records.
5. The access or disclosure is to an organization conducting a study for or on behalf of federal or state education agencies or institutions for any of the purposes listed in 511 IAC 7-8-1 (I), providing the organization protects the confidentiality of the educational record and destroys all copies in its possession when the record is no longer needed for the purpose for which the study was conducted.

Acceptable purposes of studies are:

- a. developing, validating, or administering predictive tests;
  - b. administering student aid programs; and,
  - c. improving instruction,
6. The access or disclosure is necessary to comply with a judicial order or lawfully issued administrative or judicial subpoena, provided the public agency make a reasonable effort to notify the parent or the eligible student of the order or subpoena in advance of the access disclosure; and,
  7. The access or disclosure is to appropriate parties in a health and safety emergency if the disclosure is necessary to protect the health and safety of the student or other individuals.

N. The public agency shall, upon request, provide the parent with a copy of the information which has been disclosed.

O. A parent who believes that information in educational records collected, maintained, or used is inaccurate misleading, or violates the privacy or other rights of the student may request the public agency that maintains the record to amend the information. The request shall be in writing, dated, and specify the information that the parent believes is inaccurate, misleading, or violates the student's privacy or other rights.

P. If the public agency agrees to amend the information as requested, the public agency shall:

1. Amend the information within ten (10) business days of the date the request is received;
2. Notify the parent in writing that the change has been made; and,
3. Provide a copy of the amended information upon the parent's request.

Q. If the public agency refuses to amend the information as requested, the parent shall be so informed in writing within ten (10) business days of the date the request is received, including notification of the parent's right to a hearing to challenge the information in the student's education record. The parent shall be informed of procedures related to the hearing, including:

1. The parent shall submit a written request for a hearing that specifies the information to be challenged and the reasons the parent believes the information to be inaccurate, misleading, or in violation of the student's privacy or other rights.
2. The public agency shall convene a hearing within fifteen (15) business days after the request for the hearing is received. The parent shall be provided written notice of the hearing date, time and location, and name, and title of the hearing officer at least five (5) business days before the hearing;
3. The hearing may be conducted by any person, including an official of the public agency, who does not have a direct interest in the outcome of the hearing;
4. The parent shall be given a full and fair opportunity to present evidence relevant to the issues. The parent may, at the parent's expense, choose one (1) or more persons to represent or assist the parent including an attorney.
5. The hearing officer shall notify the parent of the hearing decision in writing within ten (10) business days of the date of the hearing. The decision shall be based solely on the evidence presented at the hearing and shall include a summary of the evidence and the reasons for the decision;
6. If the hearing officer determines the information in question is inaccurate, misleading, or otherwise in violation of the privacy or other rights of the student, the public agency shall amend the information accordingly, inform the parent in writing of the amendment, and provide the parent a copy of the amended information if requested;
7. If the hearing officer determines the information is not inaccurate, misleading, or otherwise in violation of the privacy or other rights of the student, the public agency shall inform the parent in writing of the right to place in the student's record a statement commenting on the contested information or stating any reason for disagreeing with the decision;

8. Statements placed in the record by the parent shall be kept by the public agency in the student's record as long as the record or contested portion of the record is kept by the public agency. If the student's record or the contested portion is disclosed by the public agency to any party, the parent's statement must also be disclosed by the public agency; and,
  9. The public agency shall notify the parent of any local process for initiating appeal or review of the hearing officer's decision, including the right to seek judicial review in a civil court with jurisdiction.
- R. The public agency shall establish and maintain procedures to protect the confidentiality of personally identifiable information at collection, storage, disclosure, and destruction stages. These procedures include, but are not limited to, those previously described and:
1. Appointment of one (1) official in each building or administrative office who is responsible to insure the confidentiality provisions are followed; and
  2. Training or instruction regarding the confidentiality provisions for all persons collecting or using personally identifiable information.
- S. The public agency informs the parent in writing when personally identifiable information is no longer needed to provide educational services to the student. The information is destroyed at the request of the parent. A permanent record of the student's name, address, telephone number, grades, attendance record, programs and related services provided, and the year the student exited from special education may be maintained without time limitation.
- T. The public agency maintains a student's educational record for at least five (5) years after the student exits from the special education program.
- U. A public agency may maintain and store a student's educational record in any manner, provided:
1. The manner of maintenance and storage does not abridge any rights previously stated; and
  2. The educational record can be reviewed and copies made if needed.

A public school corporation is required to have a policy and procedures regarding confidentiality. (Please reference Appendix 8-1-A for an example of such procedures.) Within this policy, the public school corporation must have a statement regarding who is permitted to access personally identifiable information and the criteria it uses to determine which parties are school officials with a legitimate educational interest. A SCHOOL OFFICIAL is defined as a person who has direct input into the development and/or implementation of a child's educational program. This direct input establishes a "LEGITIMATE EDUCATIONAL INTEREST." The following school employees would be considered school officials and would have access to personally identifiable special educational information:

- Building Principal
- Assistant Building Principal

- Counselor(s)
- Special Education Personnel
- Dean(s)
- All General Education Teachers who have direct input into the student's educational program
- Home School Advisor(s)
- Multidisciplinary Evaluation Team Members
- Designated Clerical Staff.

It is recommended that a listing of those school officials who have access be posted near the location of the special education records. Please reference Appendix 8-1-B for an example of a Procedure for Accessing Student Records.

Other professional and paraprofessionals who provide services for the student on a routine basis may gain access to educational records through the teacher of record as appropriate.

Key Considerations for other individuals claiming a legitimate educational interest: Have them complete appropriate documentation and submit it to the special education director or designee(s) for approval to view the educational records. Please reference Appendix 8-1-C for an example of an Educational Interest form.

Upon approval, have them review the files with the directory or his designee who can interpret and/or explain the records.

**Training to Ensure Confidentiality Protections:**

A school official must be appointed and trained to ensure that confidentiality procedures are followed. The person charged with that responsibility is generally the administrator of the building where the records are kept. This person may designate another individual to implement the procedures established to maintain confidentiality.

The training include all confidentiality provisions. Documentation of the training must be maintained, including the following information:

- Dates
- Areas covered
- Names of personnel in attendance
- Facilitator
- Retraining should occur when there is a change in the designated person or amendment to the regulations. The retraining should also be documented.

**Caution:**

The Family and Educational Rights and Privacy Act (FERPA) requires that all rights of parents regarding educational records **transfer** to the student at age eighteen (18). The present language of Article 7 indicates that those rights become **concurrent** with the parent's rights. The planning district must be aware that a legal challenge to Article 7's interpretation may result in preemption by the federal regulation. (This requirement does not apply to the minor adjudicated legally incompetent.) Each student's file should contain a Record of Inspection as a means of documenting who has reviewed the

student's file. Please reference Appendix 8-1-D for an example. Also, please reference Appendix 8-1-E for an example of a procedure for release of confidential information to other agencies.

### **Appendix 8-1-A Sample Confidentiality Procedures**

Special Services permits a parent to inspect and review any education records relating to his/her child (aged birth to eighteen (18)) which are collected, maintained or used by the school pertaining to Article 7. All rights listed within this section pass to the child upon reaching age eighteen (18).

The school shall comply with a request without unnecessary delay and before any meeting regarding an individualized education program or hearing relating to the identification, evaluation, or placement of the child, and in no case more than 45 calendar days after the request has been made. The right to inspect and review education records includes:

- a. The right to a response from the school to reasonable requests for explanations and interpretations of the records;
- b. The right to request the school to provide copies of the records containing the information; and
- c. The right to have a representative of the parent inspect and review the records.

Special Services presumes a parent has authority to inspect and review records relating to the child unless the school has been specifically advised the parent does not have the authority under applicable State law governing such matters as guardianship, separation, and divorce.

Each school shall maintain, for public inspection, a current listing of the names and positions of those employees within the school who may have access to personally identifiable information.

Special Services keeps a record of persons obtaining access to education records collected, maintained, or used under Article 7 (except access by parents and authorized employees of the school), including the name of the person, the data access was given and the purpose for which the person is authorized to use the records.

If any education record includes information on more than one child, the parent of a child shall have the right to inspect and review only the information relating to parent's child or to be informed of the specific information. Special Services will provide a parent, on request, a list of types and locations of education records collected, maintained, or used by the school.

Special Services may charge a fee for copies of records, not to exceed actual cost of duplication, which are made for a parent unless the parent is unable to pay the fee. Special Services will not charge a fee to search for or to retrieve information.

A parent who believes information in education records collected, maintained, or used is inaccurate or misleading or violates the privacy or other rights of the child, may request the school which maintains the information to amend the information. Special Services

will decide whether to amend the information in accordance with the request. If Special Services decides to refuse to amend the information, the school will inform the parent of the refusal, and advise the parent of the right to a hearing. The school will, on request, provide an opportunity for a hearing to challenge information in education records to insure that it is not inaccurate, misleading, or otherwise in violation of the privacy or other rights of the child.

If, as a result of the hearing, it is determined the information is inaccurate, misleading, or otherwise in violation of the privacy or other rights of the child, the school will inform the parent of the right to place in the records maintained on the child a statement commenting on the information or setting forth any reasons for disagreeing with the decision. Any explanation placed in the child's records must be maintained by the school as part of the child's records as long as the record or contested portion is maintained by the school. If the child's records or the contested portion is disclosed by the school to any party, the explanation must also be disclosed by the school to the party.

Any hearing conducted as a result of the school's refusal to amend information in a child's record at the request of the parent must be conducted according to the procedures outlined in the regulations implementing the Family Educational Rights and Privacy Act of 1974 (ESEA Title VI, Part 99).

Parental consent must be obtained before personally identifiable information is disclosed to anyone other than officials of the school collecting or using the information or before the information is used for any purpose other than meeting a requirement of State education regulations.

A school may not release information from education records to another school without parental consent unless the transfer of records is initiated by the parent or child at the sending school or the school's confidentiality of information notice and policy includes a statement that the school forwards education records on request to a school in which a student seeks or intends to enroll. The sending school shall provide the parent, upon request, with a copy of the records which have been transferred. If the child is enrolled in more than one school or receives services from more than one school, written consent of the parent is not required for the school to disclose information from the student's records to each other.

Special Services will protect the confidentiality of personally identifiable information at collection, storage, disclosure, and destruction stages. One official at each school shall have the responsibility for insuring the confidentiality of any personally identifiable information. All persons collecting or using personally identifiable information must receive training or instruction regarding policies and procedures related to the confidentiality of information.

Special Services will inform the parent when personally identifiable information which has been collected, maintained, or used is no longer needed to provide educational services to the child. The information must be destroyed at the request of the parent. A

permanent record of a child's name, address, and telephone number, grades, attendance record, classes attended, grade level completed and year completed may be maintained without time limitation.

Special Services in compliance with Section 99.34 of the Family Educational Rights and Privacy Act hereby gives notice to the following policy regarding transfer of school records: Education records will be forwarded, upon request, to a school in which a student seeks or intends to enroll, after reasonable attempt to notify parent at the parent's last known address.

**Appendix 8-1-B**  
**Sample Procedure Access To Student Records**

The following are the established confidentiality policy and procedures of the X School District as required by federal and state regulation for the provision of special education. These policy and procedure statements are effective as of August 24, 1992.

Federal Regulatory Requirements: 34 CFR Part 99; 34 CFR 300.129; 34 CFR 300.221; 34 CFR 300.560-.574

State Regulatory Requirements: 511 IAC 7-3-17; 511 IAC 7-3-21; 511 IAC 7-3-41; 511 IAC 7-8-1; State Statutory Authority: IC 20-1-1-6; IC 20-1-6-14.

Each building will post, near the special education files, the Record of Access form.

The parent/parent representative may inspect the educational records relating to their child.

A Record of Inspection of Student Records form shall be maintained in each student's folder.

While the parent/parent representative is inspecting the record, the principal's designee shall be present to help interpret information.

If the parent/parent representative requests a copy of their child's records, a Consent of Mutual Exchange of Information form must be signed and sent to the Director of Special Education's office.

The Director of Special Education shall make available to the parent/parent representative the child's records as soon as possible and/or within ten days.

A student may request his/her own records once they reach eighteen (18) years of age.

**Appendix 8-1-C**  
**Sample Educational Interest**

Date: \_\_\_\_\_  
Student Name: \_\_\_\_\_  
D.O.B.: \_\_\_\_\_  
Social Security #: \_\_\_\_\_  
Person Requesting Access: \_\_\_\_\_  
Relationship to Student's Educational  
Program: \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
Educational Interest:  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_ Approved

\_\_\_\_\_ Denied

\_\_\_\_\_  
Signature (Director/Designee)

\_\_\_\_\_  
Date

THIS FORM REMAINS IN EFFECT FOR ONE YEAR FROM THE  
APPROVAL/DENIAL DATE.



**Appendix 8-1-E**  
**Sample Release Of Confidential Information To Other Agencies**

The following are the established confidentiality policy and procedures of the X School District as required by federal and state regulation for the provision of special education.

These policy and procedure statements are effective as of August 24, 1992. Federal Regulatory Requirements: 34 CFR Part 99; 34 CFR 300.129; 34 CFR 300.221; 34 CFR 300.560-.574

State Regulatory Requirements: 511 IAC 7-3-17; 511 IAC 7-3-21; 511 IAC 7-3-41; 511 IAC 7-8-1; State Statutory Authority: IC 20-1-1-6; IC 20-1-6-14.

If the parent requests copies of information, the parent should complete the Permission to Release Information form. The original request should be forwarded to the Director of Special Education. The Director's office will be responsible for mailing release forms and/or records.

The complete procedure shall not take more than ten days. The district will act upon release requests as quickly as possible.

\*Per Article 7, it is no longer necessary to require parental signature on release requests; however, we will continue to utilize this procedure.

## **Appendix H -- Bibliography & Resources for Internet Security Information**

1. American National Standards Institute (ANSI), 11 West 42nd Street, 13th Floor, New York NY 10036 USA; phone (212) 642-4900 or (212) 764-3274; fax (212) 398-0023, <http://www.ansi.org>
2. Brown University, A Survey of Selected Computer Policies form Institutions of Higher Education [http://www.brown.edu/Research/Unix\\_Admin/cuisp](http://www.brown.edu/Research/Unix_Admin/cuisp)
3. California Department of Education, K-12 Network Technology Planning Guide, Chapter 9, Security and Authentication  
<http://www.cde.ca.gov/ftpbranch/retdiv/k12/ntpg/ch09.html>
4. Commonwealth of Kentucky, Department of Information Systems, Security Manual (Rev. December 1992)
5. Computer Professionals for Social Responsibility (CPSR), P.O. Box 717, Palo Alto CA 94302 USA; (650) 322-3778; fax (650) 322-4748, <http://www.cpsr.org/>
6. Computer Security Institute (CSI), 600 Harrison St., San Francisco CA 94107 USA; (415) 905-2200; fax (415) 905-2218, <http://www.gocsi.com/>
7. Electronic Privacy Information Center (EPIC), 666 Pennsylvania Ave. SE, Suite 301, Washington DC 20003 USA; phone (202) 544-9240; fax (202) 547-5482, <http://www.epic.org/>
8. Raymond Elliott, et. al., Information Security in Higher Education, Association for the Management of Information Technology in Higher Education (CAUSE), Professional Paper Series #5
9. European Parliament Directive 95/46/EC on the Protection of Individuals with regard to the processing of personal data and on the free movement of such data, <http://lrc.law.warwick.ac.uk/jilt/dp/material/directiv.htm>

10. Family Educational Rights And Privacy Act (FERPA), 20 U.S.C. 1230 et seq., and Federal Regs. at 34 CFR 99, <http://web.indstate.edu/soe/iseas/ferpa.html>
11. Fla. State Technology Charter to Create and Implement safeguards to insure Information resource integrity, and accurate and timely delivery of information to qualified users.
12. Full Disclosure – <http://www.fulldisclosure.org/>
13. Barbara Guttman and Robert Bagwill, National Institute of Standards and Technology, U.S. Department of Commerce, Internet Security Policy: A Technical Guide [1998? Draft] <http://csrc.ncsl.nist.gov/isptg/>
14. Darcy Hopko (CERIAS) -- Confidentiality Reminders -- parents' rights, when parent consent is required, legal definitions of "educational record," "personally identifiable information," and critical pointers
15. Indiana Department Of Education, State Requirements and Recommendations for Public School Internet Acceptable Use Policies and Guidelines (11/95)  
<http://www.siec.k12.in.us/aup/require.html> and  
<http://www.siec.k12.in.us/aup/recomm.html>
16. Information Infrastructure Task Force, Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information, Final Version (June 6, 1995), [http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin\\_final.html](http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html)
17. Information Systems Security; Auerbach Publications; CRC Press; 2000 Corporate Blvd. NW, Boca Raton, FL 33431 USA; phone (800) 272-7737,  
<http://www.crcpress.com/>
18. International Computer Security Association (ICSA), 12379-C Sunrise Valley Drive, Reston VA 20191-3422; phone (703) 453-0500; fax (703) 620-6540,  
<http://www.icsa.net>
19. Iowa Access, Internet Security & Information: Exchange Issues and Concerns  
<http://www.iowaccess.org/main/projects/3/mod7.html>

20. Iowa Department of Education, Project EASIER,  
<http://www.state.ia.us/educate/programs/easier/>
21. William W. Lowrance, HHS Consultant, Privacy and Health Research,  
<http://aspe.os.dhhs.gov/admsimp/PHR.htm#Contents>
22. Kevin C. McDowell, Indiana Department of Education, Divulging School Records:  
Confidentiality Concerns
23. Milken Exchange on Education Technology, Indiana Profile (1998)  
<http://206.117.127.97/statepolicy/stateprofile.taf?stateid=5>
24. Milken Exchange on Education Technology, Learning Technology Policy Counts:  
State-by-State Survey Results (1999)  
<http://www.mildenexchange.org/policy/statepolicy.html>
25. Stephanie Miller (CERIAS), Security Policy Pointers, Overall Security Architecture  
(dataflow chart ), What can go wrong during the data flow process (Understanding  
threats)
26. Stephanie Miller (CERIAS), Masters Thesis, Using the Techniques of a Security  
Assessment to Guide Technology Development in Education (December, 1999).
27. Mississippi Department of Information Technology Services, Network Security, Suite  
508, 301 North Lamar Street Jackson, Mississippi, 39201-1495; Voice - (601) 359-  
1395 FAX - (601) 354-6016, <http://www.its.state.ms.us/et/security/secpaper.htm>
28. Missouri Research Education Network (MOREnet), MOREnet Security Services  
Policies, version 1.2 (1998) <http://www.more.net/security/secpol.html>
29. National Center for Education Statistics, Education Data Confidentiality: Two  
Studies, NCES 94-635 (1994), [http://nces.edu.gov/pubs97/p97527/lk\\_2stuf.htm](http://nces.edu.gov/pubs97/p97527/lk_2stuf.htm)

30. National Cooperative Education Statistics System & National Center for Education Statistics, Safeguarding Your Technology: Practical Guidelines for Electronic Education Information Security, <http://nces.ed.gov/pub98/safetech/>
31. National School Boards Association, ITTE (Education Technology Programs Department), Legal Issues & Education Technology: A School Leader's Guide (April, 1999) <http://www.nsba.org/itte/legalpub.html>
32. National School Boards Association, ITTE (Education Technology Programs Department), Leadership & Technology: What School Board Members Need to Know (October, 1995) <http://www.nsba.org/itte/leadtech.html>
33. National School Boards Association, ITTE (Education Technology Programs Department), Plans & Policies for Technology in Education: A Compendium (March, 1995) <http://www.nsba.org/itte/planpol.html>
34. State Government News; Council of State Governments, 2760 Research Park Drive, P.O. Box 11910, Lexington, KY 40578-1910 USA; phone (606) 231-1925, fax (606)244-8001, <http://www.statesnews.org/>
35. State of Arkansas, Department of Information Systems, Security Document version 4.0 [http://www.dis.state.ar.us/WG/Architecture/A\\_SPA/A\\_drafts/SecV3.1.htm](http://www.dis.state.ar.us/WG/Architecture/A_SPA/A_drafts/SecV3.1.htm)
36. State of Massachusetts, Network Security <http://www.its.state.ms.us/et/security/secpaper.htm>
37. State of Oregon, Guideline For Developing An Agency Information systems security Policy
38. State of Nevada, Department of Information Technology, Policies, Standards and Procedures <http://www.state.nv.us/doit/psp/index.htm> and [http://www.state.nv.us/doit/psp/toc\\_9.htm](http://www.state.nv.us/doit/psp/toc_9.htm)
39. State of Texas, Department of Information Resources, Information Resources Security and Risk Management Policy, Standards, and Guidelines (1995), <http://www.state.tx.us/ftp/pub/irpolicy.txt>

40. U.S. Dept. of Education, National Center for Education Statistics, Protecting the Privacy of Students Records, NCES 97-527, by Oona Cheung, Barbara Clements, and Ellen Pechman, Washington, D.C: January, 1997, <http://nces.ed.gov/pubs97/p97527/>
  
41. U.S. Dept. of Education, National Center for Education Statistics, Protecting the Privacy of Students Records, NCES 97-859R, by Policy Studies Associates, Inc. Under contract to the Council of Chief State School Officers, Washington, D.C.: Revised, March, 1997,  
<http://privateschool.about.com/education/privateschool/gi/dynamic/offsite.htm?site=h>  
<http://nces.ed.gov/>
  
42. Nancy Willard, A Legal and Educational Analysis of K-12 Internet Acceptable Use Policies (1996) [http://www.erehwon.com/k12aup/legal\\_analysis.html](http://www.erehwon.com/k12aup/legal_analysis.html)
  
43. Charles Cresson Wood, Information Security Policies Made Easy, Version 7 (Sausalito, Ca. October, 1999).
  
44. Noraleen A. Young, Indiana Department of Education & Clay Community School Corporation, Care of Public School Records: A Record Creator's Guide (September 1995).

Draft 5/21/00 v5