Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

SANS GIAC GISO PRACTICAL
Practical Assignment v1.2

GIAC Elementary School District and the Mandate for Student Internet Safety

Patrick W. Luce
March 14, 2003

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

TABLE OF CONTENTS

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

ABSTRACT

This document describes the Information Technology operations for the GIAC Elementary School District (the "District"), and the provisions the District has made to ensure the safety and privacy of its students. The following information is included:

- A description of the general business functions of the District
- An overview of the District's network infrastructure
- A description of the instructional and business operations that rely on the District network
- Analysis of the three most critical risks to the District network and associated mitigation strategies, including:
    a. Exposure of students to harmful Internet content
    b. Unauthorized access to student personal information
    c. Creation of unauthorized points of entry into the District network that bypass District security mechanisms
- An evaluation of an existing Acceptable Use and Internet Safety Policy to be used as the basis for developing an Internet Safety Policy for the District
- An Internet Safety Policy for the District
- A detailed District procedure used to determine if an Internet web site or service is to be blocked from access to the District's network

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

ASSIGNMENT 1: DESCRIBE GIAC ELEMENTARY SCHOOL DISTRICT

Description of GIAC Elementary School District

The GIAC Elementary School District (The "District") is a public school district located in an economically depressed suburb of Los Angeles, California. The District serves seven thousand elementary school students between the ages of four and twelve, all from their local community. The school community is ethnically diverse. The District provides educational services from pre-kindergarten through sixth grade, as well as associated services that include:

- Food services
- After-school day care
- Transportation services to and from school
- Limited medical services, including childhood immunization and hearing/vision testing

The District has eleven school campuses that serve between four and eight hundred students each. The District also has a central office complex ("Headquarters") located near the suburb's civic center. The District employs five hundred employees, including three hundred teachers.

Information Technology (IT) Infrastructure

Network Connectivity

The core of the Information Technology infrastructure of the District is the Wide Area Network (the "Network") that connects the eleven schools to Headquarters and Headquarters to the Internet. The Network serves two primary functions:

1. To provide District employees and students with access to educational resources on the Internet required to implement effective curricula in multiple academic disciplines
2. To provide the District with the ability to conduct day-to-day business in an efficient manner

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

A diagram of the District WAN is shown in figure 1 -1.

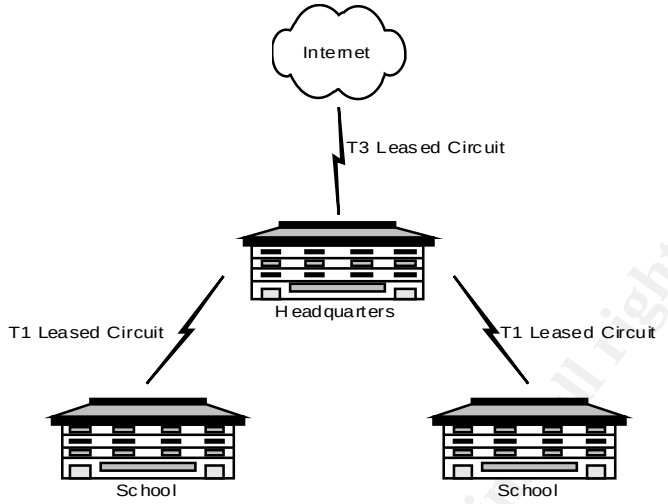

Figure 1-1 District Network Connectivity

Each school and Headquarters has a Local Area Network (LAN) with 10/100BaseT connectivity to all classrooms and offices. All LAN equipment is standardized with Cisco as the manufacturer. A T1 circuit leased from the local telephone company connects a Cisco 2651XM router at each school to a Cisco 3745XM router at Headquarters. A Cisco 7603 router at Headquarters is connected to a separate leased T3 circuit to the Los Angeles County Office of Education (LACOE), which serves as the District's Internet Service Provider. All routers run Cisco IOS version 12.3, and are hardened according to the level -1 benchmark issued by the Center for Internet Security. [1] This benchmark was developed by a consensus of security professionals from a variety of organizations, and is intended to set a minimum standard for "prudent due care." [1]

Network Security

The District has implemented multiple technologies to protect both users and systems from unauthorized and/or malicious access. Due to the young age of students who have direct access to the network, protection from external threats is a primary concern. Therefore, school LANs do not have direct Internet access. All traffic from schools destined for the Internet is sent to Headquarters, which serves as the single point of entry and exit to the Internet. If Internet connectivity to Headquarters fails, Internet access fails to all schools by design. While reducing all Internet traffic to a single access point may potentially reduce availability due to service outages, it also simplifies protection of the Network from hostile external threats.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

A diagram of the District's Network security is shown in figure 1-2.

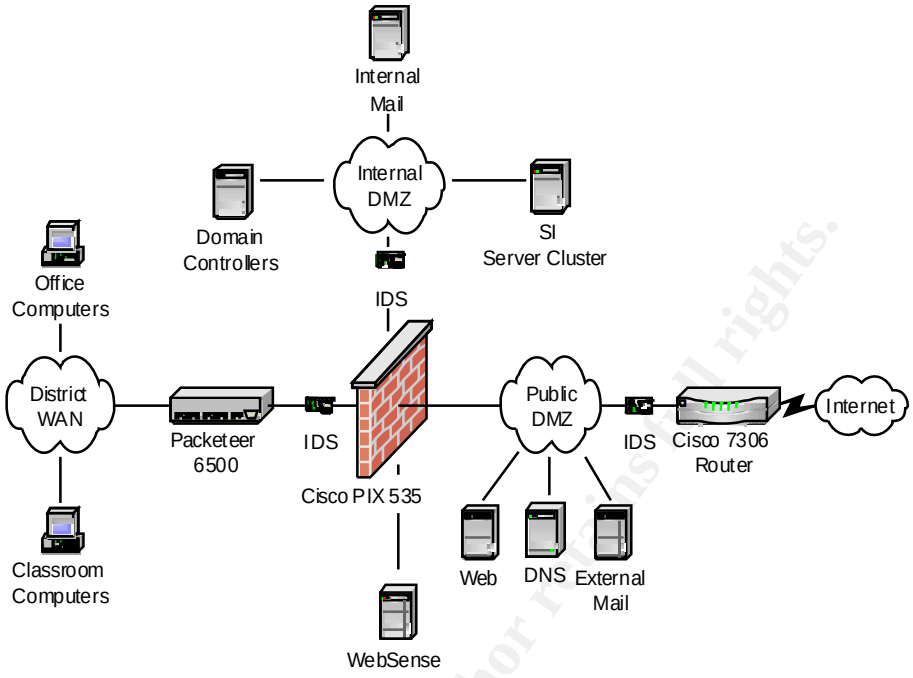

Figure 1-2 District Network Security

The District's perimeter device is a Cisco 7306 Router running Cisco IOS version 12.3. The router has sufficient memory and processing power to support two key features: the Cisco IOS Firewall feature set and the Cisco IOS Intrusion Detection System (IDS). These features integrate intrusion detection and firewall functionality with the Cisco IOS [2] on a single device, which enables the District to minimize hardware costs and associated maintenance while simplifying security administration.

The Cisco 7306 router defines the District's public Demilitarized Zone (DMZ). This DMZ houses servers that require external public access. The public DMZ acts as a security buffer between the public Internet and the District's internal network.

A Cisco PIX 535 Firewall running Cisco PIX Firewall OS version 6.3 with Integrated Intrusion Detection[3] separates the public DMZ from the Internal DMZ and the District's internal network. The Cisco PIX Firewall is hardened according to applicable Level-1 Standards for Cisco IOS routers from the Center for Internet Security.[1] The District also applies additional firewall configuration standards that were developed internally.

The Cisco PIX 535 Firewall connects to a Windows 2000 Server running WebSense Enterprise version 4.4.1. [4] WebSense software filters URL requests originating from within the District and blocks access to web sites that are potentially harmful to students, including but not limited to: pornographic web sites, sites with illegal content, web-based email and chat (many of which are anonymous), and sites

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

advocating violence. The WebSense server can also track and log all URL requests by identifying the requesting computer on the network. The WebSense product also enables the District to create custom filtering lists according to local standards for appropriateness. The WebSense server and the underlying Windows 2000 Operating System are configured according to recommendations provided by WebSense.

The final component of the District's perimeter security is a Packeteer 6500 PacketShaper. [5] The PacketShaper is an application traffic management appliance that sits between the District's internal network and the Cisco PIX 535 Firewall. All traffic between the District's internal network and the Internet passes through the Packeteer appliance. It scans all packets at layers two through seven of the OSI model for a variety of programs and protocols and allows the District to selectively disable programs of concern, such as instant messaging and peer-to-peer applications. Because it can scan at layers even, it detects unauthorized applications that attempt to disguise themselves by communicating on well-known ports such as port 80 or port 21. This greatly enhances the District's ability to prevent potentially harmful services from reaching students.

Enterprise Servers

The public DMZ houses servers that provide information resources to the public Internet. The primary servers in this DMZ are:

1. A DNS server running Bind version 9.2.2. This server fulfills DNS requests from external clients to locate the District's public resources.
2. A web server running Apache version 2.0.44. This server houses the District's public web site.
3. A mail server running Microsoft Exchange 2000. This server hosts Microsoft Outlook Web Access, which enables District students and employees to access District email from external networks. The server also hosts a SMTP relay that forwards inbound email to the District's internal mail server.

Both the DNS server and the web server run on the RedHat version 8.0 Operating System and are hardened according to the Level-1 Benchmarks for Linux from the Center for Internet Security. [6] The mail server runs on the Microsoft Windows 2000 Server Operating System and is hardened according to the Level-1 benchmarks for Windows 2000 v1.1.7 from the Center for Internet Security. [7]

The Internal DMZ contains servers hosting sensitive information that the District must protect from all unauthorized access, whether that access originates from external or internal hosts. All servers in the private DMZ are standardized on the Microsoft Windows 2000 Server Operating System, and are hardened according to the level-1 standards for Windows 2000 Servers as determined by the Center for Internet Security[7], as well as additional hardening standards developed by the District. The most sensitive system is the Student Information (SI) System, which houses confidential student information. The SI system is hosted on a cluster of Windows 2000 Advanced Servers. Other sensitive servers include the District's domain controllers running Microsoft Windows 2000 Active Directory Services and a Windows 2000 Server running Microsoft Exchange 2000. Servers that maintain the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

District's human resource data and financial information are also contained in the private DMZ.

Desktop Systems

Desktops Computers for students and employees are standardized on the Microsoft Windows 2000 Professional Operating System, and hardened according to the Center for Internet Security Level -1 benchmarks.[7]

Business Operations

The District's Network is used for business operations that fall into two general categories: instructional operations and administrative operations.

Instructional Operations

The majority of network usage, both in terms of hardware resources and network bandwidth, is for instructional purposes. A significant amount of this usage is comprised of direct student access to resources on the Internet from desktop computers located in classrooms. Web-based resources are accessed via Microsoft Internet Explorer, which is the District's standard web browser. Instructional resources used by students include:

- Subscription-based curriculum services licensed by the District for general use, such as the Grolier Online Encyclopedia [8] and World Book Online. [9]
- Free reference web sites available to the public that cover a wide variety of academic subjects, such as The Mad Scientist Network [10] and The U.S. Department of the Treasury for Kids. [11]
- Online virtual museums, such as the Smithsonian Institution [12] and the National Gallery of Art [13].

Teachers also access instructional resources on the Internet from desktop computers located in classrooms. In addition to the curriculum-based web sites used by students, teachers also regularly access curriculum support sites that provide lesson plans, instructional resource guides and student assessment tools. Examples include "Microsoft Education Lesson Plans" [14] and "Federal Resources for Educational Excellence." [15]

All teachers and all students in grades four and up have access to District email via Microsoft Exchange 2000 [16], using Microsoft Outlook 2002 as the standard client on all classroom desktop computers. Students use email to communicate with academic experts from a variety of subject areas. Teachers use email to communicate with parents and other educators, as well as to transact District business.

All students and teachers also have classroom desktop access to the Microsoft Office XP Professional desktop suite [17], which provides word processing, spreadsheet and presentation functionality, as well as the Microsoft Outlook 2002 Exchange client.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Administrative Operations

District administrative operations include all tasks relevant to the management of the District that are non-instructional. Examples include accounting and human resource functions that are isolated within Headquarters. The primary administrative operation relevant to instruction is the maintenance and operation of the Student Information (SI) System.

The SI system houses all personal information regarding each student in the District, from their enrollment through the end of their elementary school "career." Information input into the SI system and used daily by District employees includes:

- Personal Data: full name, home address, parent or guardian identification, emergency contact information, home language, immunization records, Federal program eligibility, etc.
- Attendance: daily and cumulative attendance data
- Academic Performance: student report cards, teacher assessment data, standardized test scores, learning disabilities, special education needs, etc.

Information housed in the SI system must be made available to a wide variety of District employees throughout the students' "life cycle" within the District. Examples of required access are as follows:

- Admissions clerks must enter personal data for new students upon matriculation. Access is provided in each school's attendance office.
- School counselors and nurses must have the ability to read and update personal data for students from desktop computers located in school offices.
- Teachers must input and update attendance and academic information for their students from desktop computers located in classrooms.
- Miscellaneous school staff must access specific student data relevant to their position. For example, school transportation employees must have access to home address and parent information, food service employees must have access to Federal lunch program eligibility, etc. This access must be available from offices located within school sites and Headquarters.
- District officials must be able to view individual and summary student data from desktop computers located at Headquarters.

Due to the sensitive nature of information housed within the SI system and several legislative mandates for its security, the District must take great care to provide required access to the SI system in a secure manner.
The District uses a commercial student management package from Chancery Software Limited[18] to house the SI system. The "Chancery SMS 3.0"[19] package is a web-based SI System that runs upon the Microsoft .Net platform. The Chancery package lies on a cluster of servers running on the Microsoft Advanced Server 2000 operating system and integrates the following Microsoft technologies.[20]

- Microsoft Active Directory Services: Provides the underlying authentication for the SI system.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Microsoft Internet Information Server 5.0: Provides the web interface for transactions with the SI system, as well as SSL encryption from user desktops to the server back-end.
- Microsoft SQL Server 2000: Provides the database for the system.

The Chancery SMS package uses role-based security to restrict authenticated and authorized users to specific functions. It also provides an audit trail of all system transactions.[20]

The District uses the inherent abilities of Windows 2000 Active Directory Services to restrict access to the SI System to individually authorized workstations in schools and Headquarters.

District employees at schools and Headquarters also have Internet access from their office desktop computers to perform research tasks relevant to their job description. All office computers also have access to District email via the District's Microsoft Exchange 2000 server[16] and access to the Microsoft Office XP Professional desktop suite[17], which provides word processing, spreadsheet and presentation tools, and the Microsoft Outlook 2002 Exchange client.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

ASSIGNMENT 2: IDENTIFY RISKS

Risk Area 1: Exposure of Students to Harmful Internet Content

The most critical area of risk to the District's network is the exposure of students to harmful content or communications accessed via the Internet. In all aspects of business, IT related or otherwise, the students are the "crown jewels" of the District and must be protected at all costs. There is nothing more devastating to the District than harm to a child, especially if that harm was enabled by an inadequately secured service provided by the District. While the Internet provides instructional resources that are of tremendous educational benefit, it also provides access to resources that could potentially cause permanent physical or psychological harm to children under the District's care. The two most critical risks with respect to student Internet access are the access of pornographic materials and communications with anonymous adults.

The potential for children to reach pornographic materials via the Internet is widely documented and legislated. [21] There is a general consensus that access to pornography is potentially harmful to children in several ways [22], although the extent of harm and the appropriateness of filtering is a topic of consistent debate between legislators and free-speech advocates. [23] However, the risk of children accessing pornographic materials either purposefully or accidentally [a] is extremely high, [24] and the District cannot afford to risk potential harm that could be caused by such access, be it psychological harm to a child or potential legal liability. Moreover, the District is required by Federal law to block access to pornography. The Children's Internet Protection Act (CIPA) mandates that "school… authorities must certify that they are enforcing a policy of Internet Safety that includes measures to … filter Internet access for both minors and adults..." [25] The District receives substantial subsidies for technology via the Federal Schools and Libraries Universal Support Mechanism ("E-rate"). [26] If the District does not implement a filtering technology to restrict access to pornographic sites, it risks losing substantial Federal funding. [b]

Although student access to pornography is a critical issue, the possibility of student access to anonymous communication services is also of particular concern. For example, anonymous email services such as Hotmail allow the potential for an adult to give fictitious information to the host provider, and obtain an account. [27] In the event that an adult using such an account harasses, threatens or stalks a child, that adult may be extremely difficult to trace. While email can be a very effective instructional tool, the ease with which it may be misused along with the high motivation of predators [28] make the risk to students very high. Similar concerns exist

[a] Five years ago, I personally witnessed the trivial and innocent access of questionable materials in a fourth grade classroom. The instructor was teaching the children to bookmark web sites in their browser. He told the students to search "yahoo.com" for their favorite ride at Disneyland. One of the children typed in "Splash Mountain." The first link on the page was to "Flash Mountain," which led to a site with pictures of women exposing themselves while riding on Splash Mountain. As of the date of this document, a search for "Splash Mountain" from yahoo.com still yields the same result.

[b] In November of 2002, there was substantial press coverage that a Federal panel overturned CIPA. Their decision applied only to libraries. School Districts are still required to comply with CIPA.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

for anonymous instant messaging services [29] such as Yahoo Messenger, and peer-to-peer services such as Kazaa, where potentially harmful materials may be traded with anonymous users.[30] In view of the dangers these services present, the District must have a strategy to restrict their introduction to the Network without impeding instructional use of the Internet.

Risk Mitigation

In order to mitigate the risk of exposing students to harmful content from the Internet, the following mitigation strategies are employed:

- The District enforces an Internet Safety Policy.
- The District has implemented WebSense, a commercial filtering solution that prevents all computer systems in the Network from accessing potentially harmful web sites.
- The District has implemented Packeteer, a commercial packet-filtering system that scans all Network traffic to or from the Internet for signatures of services that may include dangerous content. These services are prevented from entering or leaving the Network.
- Both WebSense and Packeteer log attempts to access unauthorized web sites and services. The District reviews the logs regularly and investigates anomalies.
- The District maintains documented procedures for reviewing web sites and services to determine if they are potentially harmful.
- All school officials including administrators, teachers, and instructional aides receive annual training on best practices for proper student supervision when accessing the Internet.

Risk Area 2: Unauthorized Access to Student Information

District employees use the District network to share data that is potentially very sensitive. Several examples include information that is necessary to run any typical business, such as human resource and financial data. However, the most sensitive data that passes across the network for administrative use is confidential student information.

Unauthorized access to student information is a great concern to the District. Student information is protected by a variety of legislation including:

- The Federal Education Rights and Privacy Act [31] (FERPA)
- The Health Information Portability and Accountability Act [32] (HIPAA)
- The California Education Code [33]
- The No Child Left Behind Act [34]
- The USA Patriot Act [35,a]

[a] The USA Patriot act defines rules for disclosing student information as part of a terrorism investigation by the Attorney General of the United States. While not normally associated with school records, its inclusion in the preceding list serves as an example of how pervasive legislative requirements for the protection of student records are.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Unauthorized disclosure of student information could place the District in violation of a number of laws, and could subject the District to potential civil action from parents, as well as potential punitive action from State and Federal agencies. More importantly, the District maintains records that, in the wrong hands, could jeopardize the health or welfare of students. For example, without adequate controls a school could accidentally release the home address of a student to a parent who is prohibited by court order from seeing their child. While the risk of unauthorized access is variable depending upon the particular motivation and opportunity of an intruder, the requirement for legislative compliance and the potential for harm caused by improper release of information make the protection of student information a primary concern.

Risk Mitigation

In order to mitigate the risk of unauthorized access to student records, the following mitigation strategies are employed:

- The District enforces a Student Privacy Policy.
- All access to the SI System is restricted to authorized computers in offices and classrooms that are secured from unauthorized access by directory authentication and physical location.
- The SI System uses role-based security to limit authorized access to "need-to-know" data dependent upon job function.
- Strong password policies for the SI System are enforced, including mandatory periodic password changes.
- All authorized and unauthorized attempts to access the SI System are logged and reviewed, and all anomalies are investigated.
- All transactions between office and classroom computers and the SI system are encrypted using 128-bit SSL.
- All SI servers at Headquarters are physically secured from unauthorized access.
- All SI servers are placed in an internal DMZ to help protect them from unauthorized internal access (within the District) and external access.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Risk Area 3: Unauthorized Network Access Points

The District has implemented a network architecture that allows it to adequately protect students from harmful content and protect student personal information from unauthorized access. However, much of the provided protection depends upon there being one and only one access point to pass information to and from the District's network to the Internet. This access point located at Headquarters has several previously discussed protection measures including:

- A Public DMZ that serves as a buffer between the Internet and the Network
- The WebSense Enterprise Content Filtering Solution that blocks Network access to harmful web sites
- A Packeteer appliance that blocks unauthorized Internet services
- An internal DMZ that protects servers from unauthorized internal and external access

However, there are a variety of inexpensive technologies that may allow District employees and other unauthorized parties to bypass this single access point and create alternative access points to the Internet. In so doing, they could either intentionally or unintentionally expose students to harmful content, or allow intruders into the internal network to attempt to gain unauthorized access to sensitive servers. The risk for these alternative access points is high due to their low cost and simplicity and the high motivation of District employees who feel that Network security measures are "inconvenient". The two most common technologies that present a risk to the District are:

Modems:

- Employees may connect a modem to a Network computer to allow themselves to connect to their classroom or office desktop computer from home. If the modem is not adequately secured, it could provide an access point for intruders.
- Students or employees may bring a laptop with a modem into the District, and connect to a private ISP service via dial-up to bypass security.

Wireless Access:

- Employees may install a wireless access point to enable them to use mobile computers within an office or classroom. If the wireless access point is not secured, it may provide unauthorized access to the Network from within or outside of the District.
- If a home or business that is near Headquarters or a school installs a wireless access point that is inadequately secured, it may provide mobile users within the District to Internet access that bypasses District security.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Risk Mitigation

In order to mitigate the risk of unauthorized access points, the following mitigation strategies are employed:

- The District enforces a Remote Access Policy that mandates that all modems must be authorized and secured according to standard District procedures.
- The District keeps a record of all authorized modems and tests compliance with standard security procedures on a regular basis.
- The District periodically engages in "War Dialing" [36] of all District phone numbers to detect, and subsequently disconnect all unauthorized modems.
- The District enforces a Wireless Access Policy that mandates that all wireless access points must be authorized by the District and secured according to standard District procedures.
- The District keeps a record of all authorized wireless access points, and tests compliance with standard security procedures on a regular basis.
- The District periodically performs an internal network scan to detect, and subsequently remove all unauthorized wireless access points.
- The perimeter of Headquarters and each school is periodically scanned for access to wireless access points not under the District's control. If one is found, the District attempts to work with the owner to secure it properly.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

ASSIGNMENT 3: EVALUATE AND DEVELOP SECURITY POLICY

Evaluate Security Policy

Enforcement of an Internet Safety Policy is the primary risk mitigation strategy to protect students from exposure to harmful content on the Internet. This policy is also required by the Children's Internet Protection Act. [25] An evaluation of the "Acceptable Use and Internet Safety Policy" of the Darke County Educational Service Center is provided below. The full text of the policy is included in this document as Attachment A. The original policy may also be found at http://www.darke.k12.oh.us/parents/AUP.pdf. [37]

The GIAC Elementary School District will use the Darke County policy as a basis to develop its own Internet Safety Policy. Therefore, recommendations for revising the Darke County policy for use by the GIAC Elementary School District follow each section of the evaluation.

The GIAC Elementary School District also maintains an Acceptable Use Policy that is separate from their Internet Safety Policy. Therefore, aspects of the Darke County policy that pertain exclusively to acceptable use and not to safety specifically will not be retained in the GIAC Elementary School District policy.

Overall, the Darke County policy is critically flawed. The evaluation of the policy is divided into the following categories:

- Purpose
- Background
- Scope
- Policy Statement
- Responsibility
- Action
- Additional Concerns

Purpose

The Darke County policy lacks a clearly stated purpose. The title implies the primary purposes of the policy is Acceptable Use *and* Internet Safety, however, the tone of the first section focuses entirely on acceptable use and legal compliance, with no reference to child safety. For example, statements such as "students must take responsibility for appropriate and lawful use of this ... (Internet)...access" imply that legal compliance and/or liability are the District's primary focus. While compliance with legislation is important, it is more important to the parents and to the community to ensure the safety of children. Emphasizing safety as the primary goal would help to establish a more sympathetic tone with the parents of the children the policy is intended to protect.

Recommendations: References exclusive to acceptable use will be omitted. The primary purpose will be explicitly stated to be student safety.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Background

The purpose/background section of the policy does not clearly state the conditions that lead to the need for a policy. If "students must take responsibility for appropriate and lawful use," what laws are of concern to the District? If the policy addresses "Internet Safety," what are the threats from which the District is attempting to shield the students? These issues should be addressed at the beginning of the policy in order to emphasize the need for the policy in the minds of the children's guardians and the public.

Recommendations: The two primary threats that Internet use poses to student safety, access to pornography and anonymous communications, will be explicitly stated.

Scope

With respect to the group of people who are covered under this policy, the scope is explicit. The policy covers students both under and over the age of 18. However, CIPA requires that a school District's Internet Safety Policy apply to both children and adults. This includes employees of the District.

Recommendations: The District's Internet Safety Policy will apply to all Network users regardless of age.

Policy Statement

The policy statements are distributed throughout the document, making it difficult to maintain a cohesive view of the policy's intent. The policy also includes a large number of examples that might be better articulated in a procedure document or a user guide. However, the policy statements that constitute guiding principles are reasonable and valid. For example, the policy states "uses that are considered unacceptable…(are)…uses that violate the law…uses that cause harm…uses that are commercial transactions…" These are valid guiding principles for an Acceptable Use Policy.

Recommendations: All policies and examples that apply solely to acceptable use will be omitted. Policies that end users must follow will be described in one section and examples will be kept to a minimum.

Responsibility

There is no reference to any agent of the DCESC responsible for the creation, review, modification, enforcement, or auditing of the policy. In terms of policy guidance or enforcement, the policy refers in several places to "person(s)" designated by the DCESC. This lack of personal accountability for any action may undermine willingness to comply with the policy and/or the ability of the District to take corrective or punitive action against those who violate the policy.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Recommendations: The District's Internet Safety Policy will clearly state who created the policy, who may modify it, and who is responsible to enforce it.

Action

The policy explicitly details a number of actions that the user is not to perform. The policy also explicitly states positive behavior to exhibit in the "Netiquette" section. However, the statements reflecting judgment of what constitutes acceptable use are ambiguous. Stating that "The DCESC is providing access to computer networks and the Internet for only educational purposes" and "you may consult with the person(s) designated by the DCESC to help you decide if a use is inappropriate" imply a lack of forethought with respect to what educational benefits the network is intended to provide, and a lack of clarity as to who may provide guidance in this area. This ambiguity has the potential to decrease the confidence of parents in the District's ability to protect their children and/or to question the District's ability to enforce the policy fairly or consistently.

Recommendations: The District's Internet Safety Policy will state unambiguous requirements for safe behavior.

Additional Concerns

In addition to the general policy flaws outlined above, items of concern specific to individual sections of the policy are described below.

Section I: Personal Responsibility

This section attempts to hold one user accountable for the actions of another user. Because the primary users are children, this is almost impossible to enforce fairly or consistently. It assumes that children of all ages can be reasonably assumed to understand the nature of the activities another student performs, regardless of both children's age level, cognitive level, or technical savvy. It also serves to raise uncertainty in the minds of the children's guardians as to the adequacy of supervision the DCESC provides. In an environment that caters to children, there is no "peer pressure" or technology that compensates for responsible supervision by properly trained adults.

Recommendations: All references to holding users accountable for other users will be dropped.

Section III-C-3: Acceptable Uses, Netiquette

The third statement in this section contradicts the fundamentally public nature of email. By teaching children to believe that they have an inherent obligation to protect the privacy of an email sent by someone else, it also may give them the expectation of privacy in their own email. With respect to the children's personal safety, it may be more beneficial to teach them that when they send an email, they have no assurance that the receiver will respect their privacy, and they should behave accordingly.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Recommendations: The District's Internet Safety Policy will explicitly prohibit sending personal information that may harm the user or another person.

Section IV-D: Internet Safety, Confidentiality of Student Information

Taken out of context, this section has the potential to raise unfounded concerns with respect to student privacy, and should be eliminated from the policy. The concept of directory information is well defined by FERPA, and should be addressed in a general Student Privacy Policy.

Recommendations: The District's Internet Safety Policy will explicitly prohibit the release of student information without parental consent.

Section IV-E: Internet Safety, Active Restriction Measures

This section appears to be written to address the requirements of CIPA, which states that "no school or library may receive… (Federal E-rate)…discounts unless it certifies that it is enforcing a policy of Internet safety that includes the use of filtering or blocking technology." [38] Emphasizing that such a technology is required by Federal Law may decrease negative reaction to the policy. The section also allows a supervising teacher or school administrator to disable the filtering technology at their discretion. There is inherent danger in allowing an end user to circumvent network security protection for any reason, particularly considering that the protection mechanism is required by law.

Recommendations: The District's Internet Safety Policy will explicitly state legal compliance in the purpose section. Disabling or bypassing District filtering technology will be prohibited.

Section VI: Failure to Follow Policy

As in Section I, the statement, "A user violates this policy by … failing to report any violations by other users that come to the attention of the user" attempts to hold one user accountable for the actions of another.

Recommendations: In the District's Internet Safety Policy, this statement will be omitted.

Section VIII: Updates

This section is vague. The policy should establish clear actions for the maintenance of the policy and the maintenance of the agreement with the guardians of the children covered by the policy.

Recommendations: The District's Internet Safety Policy will clearly state who created the policy, who may modify it, and when they may modify it. Requirements for renewal of the policy agreement will also be clearly stated.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Revise Security Policy

The "Acceptable Use and Internet Safety Policy" of the Darke County Educational Service Center (the "DCESC") is revised in this section. The Acceptable use portions are removed, and the remainder has been edited in order to create an "Internet Safety Policy" for the District that is CIPA compliant.

GIAC Elementary School District
Internet Safety Policy

I. BACKGROUND

The GIAC Elementary School District (the "District") is pleased provide its students with access to the vast array of beneficial instructional resources available via interconnected computer systems within the District and the Internet. Access to the Internet allows connections to valuable educational content located all over the world, including online libraries, virtual museums, and rich media resources.

However, the Internet also provides access to materials outside of the District's control that may be offensive, controversial, or harmful to children under the District's care. The two primary areas of concern for the District are access to pornographic images on the Internet and communication with anonymous Internet users. Therefore, the District must take appropriate action to meet its ethical and legal obligation to protect students from dangerous Internet content. While the District's employees will make reasonable and appropriate efforts to supervise student network and Internet access to ensure appropriate educational benefit, they must have student and parent cooperation in exercising and promoting responsible use of this access in order to ensure the safety of users.

In an effort to help promote the safe use of District network and Internet resources, the District Board of Education created this Internet Safety Policy that must be followed at all times by all users of the District network including students and employees.

II. PURPOSE

The purpose of this document is to establish policies that enable the District to:

1. Ensure the safety of students and employees as they access resources available on the District network and the Internet for educational use
2. Comply with the Children's Internet Protection Act (CIPA), a Federal law that requires the District to: 1) adopt and enforce an "Internet Safety Policy" and 2) establish a filtering or blocking technology that protects students from harmful content on the Internet
3. Determine which information resources on the Internet are potentially harmful to District students
4. Prevent student access to harmful materials on the Internet

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

III. SCOPE

This policy applies to all students enrolled in a school within the GIAC Elementary School District, as well as all children who attend pre-K and after school programs. This policy also applies to all District employees.

IV. POLICIES

All students and staff are to use District network resources and Internet connectivity in a manner that helps to ensure their personal safety and well being. Therefore, the following safety precautions must be followed by all network users at all times:

General Safety

1. Users of the District network must not provide private or personal information that may allow another user on the Internet to have sufficient information to contact them out of school, or cause harm to their well being. All network users must never provide their home address, telephone number, social security number, or other personal information that may be used to contact them or any other party on the Internet. In addition, students must never provide their last name to any party on the Internet. In addition, Users of the District network must not provide private information about any other member of the District community to any other party on the Internet.
2. All Users must not arrange a face-to-face meeting with someone they "meet" on the Internet unless:
   - The user is a student and they receive their parents permission
   - The user is an adult, and the meeting is necessary to transact District business
3. Regardless of age, network users must never agree to meet a person they have only communicated with on the Internet in a secluded place or in a private setting.
4. District employees must obtain express written permission from *both* their immediate supervisor and students' parents to disclose personally identifiable information concerning students via the Internet in any way for any reason. Such disclosure must also conform to all applicable laws and the District Student Privacy Policy.
5. All users must not enable any mechanism that bypasses the District's network security measures in order to access restricted resources on the Internet. Examples include but are not limited to unauthorized computer modems, wireless access points, and proxy services.
6. All students must enroll in a District approved Internet safety curriculum each school year before Internet access is granted for that year.
7. All District employees credentialed to supervise students must have a minimum of four hours of professional development each year that focuses on Internet safety and appropriate Internet use for students.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Active Restriction Measures

The District has installed a combination of technologies that prohibits students from accessing harmful web sites or services from the Internet. In order to maximize the efficiency of these technologies, the following policies are in effect:

1. The Superintendent of Schools must establish a procedure to determine if an Internet web site or service on the Internet is potentially harmful to District students, and should therefore be blocked. This procedure must be reviewed by both the Teacher's Union and the Parent Teacher Student Association, and approved by the Board of Education.
2. The Superintendent of Schools must establish procedures to make a reasonable and appropriate attempt to block those Internet web sites or services that are determined to be potentially harmful to students.
3. In the event that a web site or service on the Internet cannot be blocked by implementing reasonable and appropriate measures within the District's ability, the District Professional Development Committee is to develop appropriate training materials for all District employees to make them aware of the harmful website or service, and instruct them in how to provide adequate student supervision to prevent access to the web site or service.

V. ENFORCEMENT

Privacy

Network and Internet access is provided as a tool for the education of District students and staff. In order to ensure user safety, the District reserves the right to monitor, inspect, copy, review, and store at any time, and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the District and no user shall have any expectation of privacy regarding such materials.

Failure to comply

Use of the District computer network and the Internet is a privilege, not a right.

The principal of each school is responsible for local enforcement of this policy as it pertains to students. Each school principal shall establish local procedures to monitor students for policy compliance. A student who violates this Policy shall, at a minimum, have his or her access to the computer network and Internet terminated, which the District may refuse to reinstate for the remainder of the student's enrollment in school.

The Superintendent of Schools is responsible for enforcement of this policy as it pertains to District employees. An employee who violates this Policy shall, at a minimum, have his or her access to the computer network and Internet terminated, and, at the District's discretion be subject to additional disciplinary action up to and including termination of employment.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Warranties/Indemnification

While the District will make every effort to ensure the safety of students and employees using the District network, the District makes no warranties of any kind, either expressed or implied, in connection with its provision of access to and use of its computer networks and the Internet provided under this Policy. It shall not be responsible for any claims, losses, damages or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any user or his or her parent(s) or guardian(s) arising out of the user's use of its computer networks or the Internet under this Policy. By signing this Policy, a network user is taking full responsibility for his or her use, and the user who is 18 or older, or in the case of a user under 18, the parents(s) or guardian(s) are agreeing to indemnify and hold the School District and all of their administrators, teachers, and staff harmless from any and all loss, costs, claims or damages resulting from the user's access to its computer network and the Internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user. The user or, if the user is a minor, the user's parent(s) or guardians(s) agree to cooperate with the District in the event of the District initiating an investigation of a user's use of his or her access to its computer network and the Internet, whether that use is on a District computer or on another computer outside the District's network.

VI. POLICY RESPONSIBILITY

Students and Employees

Each student or employee who submits to the District, as directed, a properly signed Policy and follows the Policy to which she or he has agreed will have computer network and Internet access during the course of the school year only. Each student and employee must sign and submit this Policy to the District annually. Each student and their parent or guardian, and each employee agree and understand the District may revise this policy as it deems necessary.

The Superintendent of Schools is responsible to review the policy annually, and make recommended changes to the Board of Education. The District may provide notice of any changes to this policy either by posting the revised policy on the District website or by providing written notice to all parents and District employees.

VII. REVISION HISTORY

ADOPTED: March 12, 2003
REVISED:

Legal References:
Children's Internet Protection Act of 2000 (H.R. 4577, P.L. 106-554)
Communications Act of 1934, as amended (47 U.S.C. 254[h], [1])
No Child Left Behind Act of 2001

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

GIAC Elementary School District References:

GIAC Elementary School District Student Privacy Policy
GIAC Elementary School District Acceptable Use Policy
GIAC Elementary School District Remote Access Policy
GIAC Elementary School District Wireless Access Policy

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

STUDENT AGREEMENT

Every student and their parent or guardian must read and sign below:

I have read, understand and agree to abide by the terms of the Internet Safety Policy of the GIAC Elementary School District (The "District"). Should I commit any violation or in any way use my access to the District's computer network and the Internet in an unsafe manner, I understand and agree that my access privileges may be revoked and School disciplinary action may be taken against me.

_____ _____
Student name (PRINT CLEARLY) Home phone

_____ _____
Student signature Date

_____
Address

To be read and signed by parents or guardians of students:

As the parent or legal guardian of the above student, I have read, understand and agree that my child or ward shall comply with the terms of the GIAC Elementary School District's Acceptable Use and Internet Safety Policy for the student's access to the District's computer network and the Internet. I understand that access is being provided to the students for educational purposes only. However, I also understand that it is impossible for the District to restrict access to all offensive and controversial materials and I understand my child's or ward's responsibility for abiding by the Policy. I am therefore signing the Agreement and agree to indemnify and hold harmless the School, the School District and any and all District employees that provides the opportunity for computer network and Internet access against all claims, damages, losses and costs, of whatever kind, that may result from my child's or ward's use of his or her access to such networks or his or her violation of the Internet Safety Policy. Further, I accept full responsibility for supervision of my child's or ward's use of his or her access account if and when such access is not in the School setting. I hereby give permission for my child or ward to access the District's computer network and the Internet.

_____ _____
Parent or Guardian name(s) (PRINT CLEARLY) Home phone

_____ _____
Parent or Guardian signature(s) Date

_____
Address

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

EMPLOYEE AGREEMENT

Every District employee must read and sign below:

I have read, understand and agree to abide by the terms of the Internet Safety Policy of the GIAC Elementary School District (The "District"). Should I commit any violation or in any way use my access to the District's computer network and the Internet in an unsafe manner, I understand and agree that my access privileges may be revoked. I also understand that the District may take additional disciplinary action, up to and including the termination of my employment.

_____ _____

Employee name (PRINT CLEARLY) Office phone

_____ _____

Employee signature Date

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

ASSIGNMENT 4: DEVELOP SECURITY PROCEDURES

This document outlines the steps to be taken by the GIAC Elementary School District to block access to Internet web sites or services that are determined by District procedures to be potentially harmful to students.

GIAC Elementary School District
Internal Procedures
Internet Safety Policy Procedure 1 - A
Procedure to Evaluate Potentially
Harmful Internet Web Sites or Services

As per the requirements of the GIAC Elementary School District Internet Safety Policy, the District is required to comply with the following:

> "The Superintendent of Schools must establish a procedure to determine if a web site or service on the Internet is potentially harmful to District students, and should therefore be blocked. This procedure must be reviewed by both the Teacher's Union and the Parent Teacher Student Association, and approved by the Board of Education."

This document describes the procedures developed by the Superintendent of Schools to be used by the GIAC Elementary School District to determine whether a web site or service on the Internet is to be blocked from access to the District network. Please direct all concerns or inquiries regarding these procedures to the Office of the Superintendent.

The Superintendent has established in this document a three-phase approach to evaluating web sites or services of concern. The three phases are as follows:

1. Establish a review committee (the "Committee") consisting of representatives from District administration, the Teacher's Union, and the Parent Teacher Student Association.
   - The Committee shall receive and evaluate all recommendations to block individual Internet web sites or services of concern. It is important to include teacher representatives in the review process in order to evaluate each site or service from the perspective of how access to that site or service might affect the classroom as a whole. It is also important to include parent representatives in the review process who generally reflect the values of the local community.
2. Allow members of the District and of the local community to submit Internet web sites and services for evaluation by the Committee.
   - It is important for District employees and members of the community to feel secure that the District is responsive to the issue of student safety. Therefore, a procedure must be enforced that allows them to submit their concerns with a minimum of difficulty.
3. Review recommendations for the evaluation of Internet web sites and services in a timely manner.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- The Committee must review requests for the evaluation of potentially harmful Internet web sites or services within a time frame that is commensurate with the importance of protecting students from potential harm.

A step-by-step procedure for each phase of the evaluation process is documented below.

Establishment of the Review Committee

The Superintendent of Schools shall annually appoint a review committee (the "Committee") to review all Internet web sites or services of concern to members of the District community. The following procedure is to be implemented:

1. Before the first school Board meeting of the academic year, the Director of Technology is to appoint an individual from the Office of Technology to be the Committee chair (the "Chairperson").
2. The chairperson is to contact the Teacher's Union president, the Parent Teacher Student Association president, and the Office of the Superintendent to solicit one member from each organization to serve on the Committee. The Chairperson is to outline all Committee responsibilities to each party.
3. The Teacher's Union, the Office of the Superintendent and the Parent Teacher Student Association will each select a member for the Committee using a procedure of their own discretion.
4. The Chairperson is to prepare a Board report that includes the Committee membership and submit the report to the Superintendent of Schools for approval.
5. If the Superintendent approves the Committee membership, he or she is to submit the Board report at the first Board meeting of the academic year. If he or she does not agree to the membership, it is the responsibility of the Superintendent to work with all groups involved to establish Committee membership.

It is the responsibility of the Board Secretary to work with the Director of Technology and the Superintendent to assure that the Committee membership is submitted to the Board of Education at the first Board meeting of the academic year.

Submission of Internet Web Sites or Services of Concern

A simple and convenient mechanism shall exist that enables any District employee or parent to submit a request to evaluate an Internet web site or service of concern. The following procedure is to be implemented:

1. The Director of Technology is to direct the webmaster of the District web site to create a form that is to be conveniently located on the web site, and allows any member of the District community to request that an Internet web site or service be evaluated for potential harm. The form shall require the following information, at a minimum:
    - The first and last name of the requestor
    - The phone number and/or email address of the requestor

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- The school affiliation of the requestor (or in the case of a District employee, the District office)
- The address of the web site in question or a brief description of the Internet service in question
- A text box to enter the reason for the request

2. After the Committee membership has been approved at the first Board meeting of the academic year, the webmaster is to configure the submission form on the web site to email all forms posted to the Chairperson.
3. At the beginning of each semester, the Chairperson is to verify that the submission form is posted on the District website and is operational. He or she will verify correct operation by filling out the form using sample information and submitting it for review.
4. The Chairperson is to attend at least one Teacher's Union meeting and at least one Parent Teacher Student Association meeting each semester in order to remind each group of the existence and location of the submission form, and to provide a short demonstration of its use. The Director of Technology shall be responsible for ensuring the attendance of the Chairperson at the required meetings.

Evaluation of Internet Web Sites or Services of Concern

Upon receipt of the submission form requesting that an Internet web site or service be evaluated, the Committee is to review the site or service for potentially harmful content. The following procedure is to be implemented:

1. The Chairperson shall maintain a review log ("the log") of all web sites and services evaluated by the Committee. The log shall contain the request date, the URL or service, the nature of the request, and the decision to block or unblock each website in question, along with the rationale for the decision.
2. Upon receipt of an email form requesting to evaluate a specific Internet web site or service, the Chairperson is to consult the log. If the site or service has already been reviewed, the Chairperson is to notify the requestor of the previous review and the outcome. If the site has not been reviewed previously, the Chairperson is to proceed to the next step in the evaluation process.
3. The Chairperson is to attempt to visit the web site or access the service, as appropriate from a computer located within the District network to determine if it is already blocked by the current District configuration. [a] If it is currently blocked, the chairperson is to notify the requestor via phone or email, as appropriate.
4. If the web site or service is not currently blocked and it contains or provides access to information that, in the judgment of the Chairperson:
   - Is explicitly pornographic
   - Explicitly advertises access to pornographic or illegal content, including the trading of copyrighted material

[a] The majority of Internet web sites or services that are potentially harmful to students are either already blocked by address filter lists maintained by WebSense or blocked by default peer-to-peer and instant messaging filters maintained by Packeteer. Therefore, it is highly likely that a member of the District community may request that the District block a web site or service that is already blocked.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Explicitly advocates breaking the law or explicitly encourages others to break the law

then the Chairperson is to refer the site or service to the Director of Technology to be blocked immediately. [a] If, in the judgment of the Chairperson, the web site does not meet the above criteria, he or she is to forward the request via email to the other members of the Committee.

5. The members of the Committee shall each review the Internet web site or service individually and determine whether the site is potentially harmful and therefore should be blocked. The Committee members may discuss their reviews in person, via email, or phone, as necessary.
6. If the Committee achieves consensus that the site or service is potentially harmful and should be blocked, the Chairperson is to refer the site or service, along with the Committee's findings to the Director of Technology to block as appropriate.[a] The Chairperson is to enter the site or service and the action taken in the log, and notify the requestor of the Committee's decision along with the rationale for the decision.
7. If the Committee achieves consensus that the site or service should not be blocked, the Chairperson is to enter the site or service and the action taken in the log, and notify the requestor of the Committee's decision and their rationale for leaving the site or service unblocked.
8. If the Committee cannot achieve consensus within three business days, the Chairperson is to forward the request via email to the Superintendent of Schools, along with an explanation of the inability to achieve consensus. The Superintendent shall determine whether the site or service is to be blocked. The decision of the Superintendent shall be final.
9. If the Superintendent determines that the site or service is to be blocked, the Chairperson is to refer the site or service, along with the Superintendent's decision to the Director of Technology to block as appropriate. The Chairperson is to then enter the site or service and the action taken in the log, and notify the requestor of the Superintendent's decision along with the rationale for the decision.
10. If the Superintendent determines that the site or service is not to be blocked, the Chairperson is to update the log and notify the requestor along with the rationale for the decision.

It is the responsibility of the Superintendent of Schools to verify that the evaluation of all Internet web sites and services submitted for review occurs in a timely manner. In the event that the Committee is consistently unable to meet its obligations in a timely manner, the Superintendent may dissolve the Committee and form a new Committee with new membership as per the procedures outlined in this document.

[a] To refer a potentially harmful Internet web site or service to the Director of Technology for blocking, refer to the GIAC Elementary School District Internal Procedures Document, Internet Safety Policy Procedure 1-B: Procedure to Block Harmful Web Sites or Services from the District Network

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

APPENDIX A: ACCEPTABLE USE AND INTERNET SAFETY POLICY FOR THE COMPUTER NETWORK OF THE DARKE COUNTY EDUCATIONAL SERVICE CENTER

Acceptable Use and Internet Safety Policy
for the computer network of the
Darke County Educational Service Center

The Darke County Educational Service Center (DCESC) is pleased to make available to students access to interconnected computer systems within the District and to the Internet, the world-wide network that provides various means of accessing significant educational materials and opportunities.

In order for the DCESC to be able to continue to make its computer network and Internet access available, all students must take responsibility for appropriate and lawful use of this access. Students must understand that one student's misuse of the network and Internet access may jeopardize the ability of all students to enjoy such access. While the DCESC's employees and other staff will make reasonable efforts to supervise student use of network and Internet access, they must have student cooperation in exercising and promoting responsible use of this access.

Below is the Acceptable Use and Internet Safety Policy ("Policy") of the DCESC and the Data Acquisition Site that provides Internet access to the DCESC. Upon reviewing, signing, and returning this Policy, as the students have been directed, each student will be given the opportunity to enjoy Internet access at the DCESC and is agreeing to follow the Policy. If a student is under 18 years of age, he or she must have his or her parents or guardians read and sign the Policy. The DCESC cannot provide access to any student who, if 18 or older, fails to sign and submit the Policy to the DCESC as directed or, if under 18, does not return the Policy as directed with the signatures of the student and his/her parents or guardians. Listed below are the provisions of your agreement regarding computer network and Internet use. If you have any questions about these provisions, you should contact the person that the DCESC has designated as the one to whom you can direct your questions. If any user violates this Policy, the student's access will be denied, if not already provided, or withdrawn and he or she may be subject to additional disciplinary action.

I. PERSONAL RESPONSIBILITY

By signing this Policy, you are agreeing not only to follow the rules in this Policy, but are agreeing to report any misuse of the network to the person designated by the DCESC for such reporting. Misuse means any violations of the Policy or any other use that is not included in the Policy, but has the effect of harming another or his or her property.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

II. TERM OF THE PERMITTED USE

A student who submits to the DCESC, as directed, a properly signed Policy and follows the Policy to which she or he has agreed will have computer network and Internet access during the course of the school year only. Students will be asked to sign a new Policy each year during which they are students at a Darke County school district before they are given an access account.

II. ACCEPTABLE USES

A. Educational Purposes Only. The DCESC is providing access to its computer networks and the Internet for *only* educational purposes. If you have any doubt about whether a contemplated activity is educational, you may consult with the person(s) designated by the DCESC to help you decide if a use is appropriate.

B. Unacceptable Uses of Network. Among the uses that are considered unacceptable and which constitute a violation of this Policy are the following:

1. uses that violate the law or encourage others to violate the law. Don't transmit offensive or harassing messages; offer for sale or use any substance the possession or use of which is prohibited by the student's School District's Student Discipline Policy; view, transmit or download pornographic materials or materials that encourage others to violate the law; intrude into the networks or computers of others; and download or transmit confidential, trade secret information, or copyrighted materials. Even if materials on the networks are not marked with the copyright symbol, you should assume that all materials are protected unless there is explicit permission on the materials to use them.
2. uses that cause harm to others or damage to their property. For example, don't engage in defamation (harming another's reputation by lies); employ another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating or otherwise using his/her access to the network or the Internet; upload a worm, virus, "Trojan horse," "time bomb" or other harmful form of programming or vandalism; participate in "hacking" activities or any form of unauthorized access to other computers, networks, or information systems.
3. uses that jeopardize the security of student access and of the computer network or other networks on the Internet. For example, don't disclose or share your password with others; don't impersonate another user.
4. uses that are commercial transactions. Students and other users may not sell or buy anything over the Internet. You should not give others private information about you or others, including credit card numbers and social security numbers.

C. Netiquette. All users must abide by rules of network etiquette, which include the following:

1. Be polite. Use appropriate language. No swearing, vulgarities, suggestive, obscene, belligerent or threatening language.
2. Avoid language and uses which may be offensive to other users. Don't use access to make, distribute or redistribute jokes, stories or other material which

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

is based upon slurs or stereotypes relating to race, gender, ethnicity, nationality, religion or sexual orientations.

3. Don't assume that a sender of e-mail is giving his or her permission for you to forward or redistribute the message to third parties or to give his/her e-mail address to third parties. This should only be done with permission or when you know that the individual would have no objection.
4. Be considerate when sending attachments with e-mail (where this is permitted). Be sure that the file is not too large to be accommodated by the recipient's system and is in a format which the recipient can open.

IV. INTERNET SAFETY

A. General Warning; Individual Responsibility of Parents and Users. All users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged pupils. Every user must take responsibility for his or her use of the computer network and Internet and stay away from these sites. Parents of minors are the best guide to materials to shun. If a student finds that other users are visiting offensive or harmful sites, he or she should report such use to the person designated by the DCESC.

B. Personal Safety. Be safe. In using the computer network and Internet, do not reveal personal information such as your home address or telephone number. Do not use your real last name or any other information which might allow a person to locate you without first obtaining the permission of a supervisor. Do not arrange a face-to-face meeting with someone you "meet" on the computer network or Internet without your parent's permission (if you are under 18). Regardless of your age, you should never agree to meet a person you have only communicated with on the Internet in a secluded place or in a private setting.

C. "Hacking" and Other Illegal Activities. It is a violation of this Policy to use the DCESC's computer network or the Internet to gain unauthorized access to other computers or computer systems or to attempt to gain such unauthorized access. Any use which violates state or federal law relating to copyright, trade secrets, the distribution of obscene or pornographic materials, or which violates any other applicable law or municipal ordinance, is strictly prohibited.

D. Confidentiality of Student Information. Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian or, if the student is 18 or over, the permission of the student himself/herself. Users should never give out private or confidential information about themselves or others on the Internet, particularly credit card numbers and Social Security numbers. A supervisor or administrator may authorize the release of directory information, as defined by Ohio law, for internal administrative purposes or approved educational projects and activities.

E. Active Restriction Measures. The DCESC, either by itself or in combination with the Data Acquisition Site providing Internet access, will utilize filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors. The DCESC will also

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing such depictions or any other material which is inappropriate for minors.

Internet filtering software or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by students age 17 or older. The term "harmful to minors' is defined by the Communications Act of 1934 (47 USC Section 254[h][7], as meaning any picture, image, graphic image file, or other visual depiction that

- taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
- depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals;
- taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

V. PRIVACY

Network and Internet access is provided as a tool for your education. The DCESC reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the DCESC and no user shall have any expectation of privacy regarding such materials.

VI. FAILURE TO FOLLOW POLICY

The user's use of the computer network and Internet is a privilege, not a right. A user who violates this Policy, shall at a minimum, have his or her access to the computer network and Internet terminated, which the DCESC may refuse to reinstate for the remainder of the student's enrollment in school. A user violates this Policy by his or her own action or by failing to report any violations by other users that come to the attention of the user. Further, a user violates this Policy if he or she permits another to use his or her account or password to access the computer network and Internet, including any user whose access has been denied or terminated. The DCESC may also take other disciplinary action in such circumstances.

VII. WARRANTIES/INDEMNIFICATION

The DCESC makes no warranties of any kind, either expressed or implied, in connection with its provision of access to and use of its computer networks and the Internet

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

provided under this Policy. It shall not be responsible for any claims, losses, damages or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any user or his or her parent(s) or guardian(s) arising out of the user's use of its computer networks or the Internet under this Policy. By signing this Policy, users are taking full responsibility for his or her use, and the user who is 18 or older or, in the case of a user under 18, the parents(s) or guardian(s) are agreeing to indemnify and hold the DCESC, the School, the School District, the Data Acquisition Site that provides the computer and Internet access opportunity to the DCESC and all of their administrators, teachers, and staff harmless from any and all loss, costs, claims or damages resulting from the user's access to its computer network and the Internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user. The user or, if the user is a minor, the user's parent(s) or guardians(s) agree to cooperate with the DCESC in the event of the DCESC's initiating an investigation of a user's use of his or her access to its computer network and the Internet, whether that use is on a DCESC computer or on another computer outside the DCESC's network.

VIII. UPDATES

Users, and if appropriate, the user's parents/guardians, may be asked from time to time to provide new or additional registration and account information or to sign a new Policy, for example, to reflect developments in the law or technology. Such information must be provided by the user (or his/her parents or guardians) or such new Policy must be signed if the user wishes to continue to receive service. If after you have provided your account information, some or all of the information changes, you must notify the person designated by the DCESC to receive such information.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

STUDENT'S AGREEMENT

Every student, regardless of age, must read and sign below:

I have read, understand and agree to abide by the terms of the Acceptable Use and Internet Safety Policy of the Darke County Educational Service Center. Should I commit any violation or in any way misuse my access to the DCESC's computer network and the Internet, I understand and agree that my access privileges may be revoked and School disciplinary action may be taken against me.

_____ _____
Student name (PRINT CLEARLY) Home phone

_____ _____
Student signature Date

_____
Address

User (place an "X" in the correct blank): I am 18 or older ___ I am under 18 ___

If I am signing this Agreement when I am under 18, I understand that when I turn 18 this Agreement will continue to be in full force and effect, and I will continue to abide by the Acceptable Use and Internet Safety Policy.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

_____
Student's Name

To be read and signed by parents or guardians of students who are under 18:

As the parent or legal guardian of the above student, I have read, understand and agree that my child or ward shall comply with the terms of the Darke County Educational Service Center's Acceptable Use and Internet Safety Policy for the student's access to the DCESC's computer network and the Internet. I understand that access is being provided to the students for educational purposes only. However, I also understand that it is impossible for the DCESC to restrict access to all offensive and controversial materials and I understand my child's or ward's responsibility for abiding by the Policy. I am therefore signing the Agreement and agree to indemnify and hold harmless the DCESC, the School, the School District and the Data Acquisition Site that provides the opportunity to the DCESC for computer network and Internet access against all claims, damages, losses and costs, of whatever kind, that may result from my child's or ward's use of his or her access to such networks or his or her violation of the Acceptable Use and Internet Safety Policy. Further, I accept full responsibility for supervision of my child's or ward's use of his or her access account if and when such access is not in the School setting. I hereby give permission for my child or ward to use the building-approved account to access the DCESC's computer network and the Internet.

_____ _____
Parent or Guardian name(s) (PRINT CLEARLY) Home phone

_____ _____
Parent or Guardian signature(s) Date

_____
Address

****

ADOPTED:
REVISED:
Legal References:
Children's Internet Protection Act of 2000 (H.R. 4577, P.L. 106-554)
Communications Act of 1934, as amended (47 U.S.C. 254[h], [1])
Elementary and Secondary Education Act of 1965, as amended (20 U.S.C. 6801 et seq., Part F)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

REFERENCES

[1] Center for Internet Security. "CIS Level -1 / Level-2 Benchmark and Audit Tool for Cisco IOS Routers." Center for Internet Security. March 2003. URL: http://www.cisecurity.org/bench_cisco.html. (10 March 2003).
[2] Cisco Systems. "Cisco IOS Firewall 12.0(5) T and Later Releases, Q&A." Cisco Systems. 2000. URL: http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iofwft/prodlit/fw12t_qp.pdf. (10 March 2003).
[3] Cisco Systems. "Cisco PIX Firewall Software Version 6.3 Data Sheet." Cisco Systems. 2003. URL: http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pix63_ds.pdf. (10 March 2003).
[4] WebSense, Inc. "WebSense Enterprise Overview." WebSense, Inc. 2003. URL: http://www.websense.com/products/about/datasheets/pdfs/websenseoverview.pdf. (10 March 2003).
[5] Packeteer, Inc. "Packeteer's PacketShaper Data Sheet." Packeteer, Inc. 2001. URL: http://www.packeteer.com/PDF_files/packetshaper/PSDS.pdf. (10 March 2003).
[6] Center for Internet Security. "CIS Level -1 Benchmark and Scoring Tool for Linux." Center for Internet Security. April, 2002. URL: http://www.cisecurity.org/bench_linux.html. (10 March 2003).
[7] Center for Internet Security. "Benchmarks and Scoring Tool for Windows 2000 and Windows NT." Center for Internet Security. February 2003. URL: http://www.cisecurity.org/bench_win2000.html. (10 March 2003).
[8] Grolier Publishing Company, Inc. "Grolier Online." Grolier Publishing Company, Inc. 2003. URL: http://go.grolier.com. (10 March 2003).
[9] World Book, Inc. "World Book Online." World Book, Inc. 2003. URL: http://www.worldbookonline.com. (10 March 2003).
[10] MadSci Network. "MadSciNet: The 24-Hour Exploding Laboratory." Washington University Medical School. 2003. URL: http://www.madsci.org. (10 March 2003).
[11] U.S. Department of the Treasury. "U.S. Treasury – For Kids." The U.S. Department of the Treasury. 2002. URL: http://www.treas.gov/kids. (10 March 2003).
[12] The Smithsonian Institution. "Smithsonian Institution." The Smithsonian Institution. 2003. URL: http://www.si.edu. (10 March 2003).
[13] The National Gallery of Art. "National Gallery of Art NGA Kids." National Gallery of Art, Washington D.C. 2003. URL: http://www.nga.gov/kids/kids.htm. (10 March 2003).
[14] Microsoft Corporation. "Microsoft Education Lesson Plans." Microsoft Corporation. 2003. URL: http://www.microsoft.com/education/default.asp?ID=LessonPlans. (10 March 2003).
[15] U.S. Department of Education. "Federal Resources for Educational Excellence." U.S. Department of Education. 7 March 2002. URL: http://www.ed.gov/free/. (10 March 2003).
[16] Microsoft Corporation. "Microsoft Exchange Server: Exchange Server 2000 Product Overview." Microsoft Corporation. 2003. URL: http://www.microsoft.com/exchange/evaluation/overview/default.asp. (10 March 2003.)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

[17] Microsoft Corporation. "Office XP Fast Facts." Microsoft Corporation. 2003. URL: http://www.microsoft.com/office/evaluation/fastfacts.asp. (10 March 2003).
[18] Chancery Software, Ltd. "Chancery Student Management Solutions." Chancery Software, Ltd. 2002. URL: http://www.chancery.com/index.html. (10 March 2003).
[19] Chancery Software, Ltd. "Solutions: Chancery SMS 3.0." Chancery Software, Ltd. 2002. URL: http://www.chancery.com/solutions/features/cancerySMS.html. (10 March 2003).
[20] Chancery Software, Ltd. "Chancery SMS Technology Strategy." Chancery Software, Ltd. 2002. URL: http://www.chancery.com/resources/whitepapers/papers/ChancerySMSTechStrategy.pdf. (10 March 2003).
[21] MacMillan, Robert. "Primer: Children, the Internet and Pornography." The Washington Post. 5 March 2003. URL: http://www.washingtonpost.com/wp-dyn/articles/A39748-2002May31.html. (10 March, 2003).
[22] Rice Hughes, Donna. "How Pornography Harms Children." Donna Rice Hughes. 2001. URL: http://www.protectkids.com/effects/harms.htm. (10 March 2003).
[23] Hopper, D. Ian. "Filtering Law Sparks Fight." The Associated Press. 20 December 2000. URL: http://abcnews.go.com/sections/scitech/DailyNews/library_filters001220.html. (10 March 2003).
[24] Rice Hughes, Donna. "How Children Access Pornography on the Internet." Donna Rice Hughes. 2001. URL: http://www.protectkids.com/dangers/childaccess.htm. (10 March 2003).
[25] Federal Communications Commission. "FCC Form 479: Certification by Administrative Authority to Billed Entity of Compliance with the Children's Internet Protection Act." Federal Communications Commission. September 2002. URL: http://www.sl.universalservice.org/data/pdf/Form479.pdf. (10 March 2003).
[26] Universal Service Administrative Company. "USAC: SL Overview." Universal Service Administrative Company. 2003. URL: http://www.sl.universalservice.org/overview/. (10 March 2003).
[27] Eberhart, Dave. "Hotmail Confusion Fuels Privacy Debate." NewsMax.com. 27 May 2002. URL: http://www.newsmax.com/archives/articles/2002/5/26/165347.shtml. (10 March 2003).
[28] Hock, Paul. "Internet Safety Awareness – Child Predators Part 1." TheGuardianAngel.com. 2 August 2001. URL: http://www.theguardianangel.com/Internet_safety_child_predator.htm. (10 March 2003).
[29] Singer, Michael. "McAfee.com Launches Initiative to Protect Children on the Internet." Jupitermedia Corporation. 2003. URL: http://siliconvalley.Internet.com/news/article.php/3531_725871. (10 March 2003).
[30] Davids, Angela. "DS Online: Tech Bills Updates." Institute of Electrical and Electronics Engineers, Inc. 27 September 2002. URL: http://dsonline.computer.org/techbills/sept02.htm. (10 March 2003).
[31] The Family Policy Compliance Office. "Family Education Rights and Privacy Act (FERPA)." The U.S. Department of Education. 21 October 2002. URL: http://www.ed.gov/offices/OM/fpco/ferpa/. (10 March 2003).
[32] U.S. Department of Health and Human Services. "Office for Civil Rights – Privacy of Health Records." U.S. Department of Health and Human Services. 25 February 2003. URL: http://www.hhs.gov/ocr/hipaa/. (10 March 2003).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

[33] The State of California. "California Education Code." The State of California. 2002. URL: http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=edc&codebody=&hits=20. (10 March 2003).
[34] U.S. Department of Education. "No Child Left Behind." U.S. Department of Education. 2001. URL: http://www.nclb.gov/. (10 March 2003)
[35] United States Congress. "The USA Patriot Act." United States Congress. 2002. URL: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3162enr.txt.pdf. (10 March 2002).
[36] Wikipedia. "War Dialing." Wikopedia. 29 July 2002. URL: http://www.wikipedia.org/wiki/War_dialing. (10 March 2003).
[37] Darke County Educational Service Center. "Acceptable Use and Internet Safety Policy." Darke County Educational Service Center. 2001. URL: http://www.darke.k12.oh.us/parents/AUP.pdf. (10 March 2003).
[38] Universal Service Administrative Company. "USAC: SL Children's Internet Protection Act Requirements." Universal Service Administrative Company. 2003. URL: http://www.sl.universalservice.org/reference/cipa.asp. (10 March 2003).

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.