ace westchester

Pennsylvania School Boards Association
psba
INSURANCE TRUST

ACE Privacy Protection℠
PSBA Insurance Trust Policy
Privacy and Network Liability

In this privacy-conscious world, any school can be affected by a breach of sensitive parent, student or employee information.

ACE Privacy Protection℠ PSBA Insurance Trust Policy approaches traditional network liability with an innovative new alternative. This next generation policy focuses on privacy liability arising out of lost computer equipment, network security breaches and human errors. It even covers schools from mistakes made by outside service providers.

ACE Privacy Protection℠ PSBA Insurance Trust Policy also includes an identity theft response fund, broad network liability and other enhancements including internet media liability and cyber extortion which are available by endorsement.

If your school district answers "yes" to any of the following questions, the ACE Privacy Protection℠ PSBA Insurance Trust Policy may be the answer:

1. Do you obtain Social security numbers, drivers' license numbers, bank account numbers, credit/debit card numbers, or medical history (athletic programs)?
2. Do you sell, share information with third parties, or put parents/families in touch with vendors/third parties, such as school lunch programs, yearbook distributors, school ring vendors, etc.?
3. Do you allow school-owned laptop computers, BlackBerry® smartphones, PDAs, etc., to be removed from school premises? And do you require these devices to be secured/encrypted?
4. Do you sell, donate, or recycle computers? Do you recycle paper?
5. Do you post sensitive data directly on you Internet Web site system, i.e. provide access to student grades?
6. Do you post students' pictures on your website?

Three Reasons Every School Needs the ACE Privacy Protection℠ PSBA Insurance Trust Policy

- ***Increasingly stringent laws and regulations*** enacted over the past decade have elevated a school's duty of care for how it safeguards personal information. The failure to comply with legal and regulatory obligations places a school's reputation at enormous risk. Many companies historically sought to keep security breaches quiet. With state identity theft notification laws making it illegal to sweep privacy breach events under the rug, keeping quiet is not an option.

- ***Advances in Technology*** have made safeguarding employee, parent and student trust, and school reputations from privacy breaches far more difficult. Technology has made it easier to store, transport, steal and simply lose sensitive information. Today, an employee can store the equivalent of an entire pickup truck of printed social security numbers, credit card numbers, or health records on the USB flash drive in his pocket.

- ***In an era of global outsourcing,*** business/risk managers should recognize that privacy risks do not end at corporate firewalls. Any school that entrusts third parties to handle its sensitive data - including employee benefit firms, consultants and yearbook or class ring vendors - ultimately bears the burden of any privacy breach stemming from the outsourced operation. The school may have required its service provider to carry privacy coverage but it does not pass off its responsibility to protect its students, parents or employees data. If your employees, students or parents are affected by a data breach, your school is obligated to respond, regardless of who made the error.

ACE Privacy Protection℠ PSBA Insurance Trust Policy: Coverage Overview

Privacy Liability

- Covers loss arising out of the school's failure to protect sensitive personal or corporate information in any format.
- Provides coverage for regulatory proceedings brought by a government agency alleging the violation of any state, federal, or foreign identity theft or privacy protection legislation.

Network Security Liability

- Covers liability of the school arising out of the failure of network security, including unauthorized access or unauthorized use of schools systems, a denial of service attack, or transmission of malicious code.

Internet Media Liability

- Covers infringement of copyright or trade mark, invasion of privacy, libel, slander, plagiarism, or negligence arising out of the content on the school's internet website.

Identity Theft Response Fund

- Covers expenses as required by law to notify students or parents whose sensitive personal information has been breached, as well as expenses to obtain legal, public relations or crisis management services to restore the school's reputation.

Cyber Extortion

- Covers extortion monies and associated expenses arising out of a criminal threat to release sensitive information or bring down a network unless consideration is made.

Policy Coverage Highlights

- Limits available up to $10 million
- Privacy coverage includes:
  - Personal information in any format
  - Breaches not restricted to a network event
  - Customer and employee information
- Broad form network security grant replaces specified perils
- Crisis management and notification expenses are not subject to a post-discovery time restriction
- Regulatory proceeding coverage extends to both Privacy and Network Liability
- Consumer Redress Fund applies to full Privacy and Network limits of liability
- Definition of damages includes a consumer redress fund awarded from a regulatory proceeding and punitive and exemplary damages (most favorable jurisdiction language)
- Definition of insured includes leased employees, temporary employees, volunteers, substitute teachers and independent contractors
- Fraud and profit exclusions triggered only if there is an adverse adjudication, admission, plea or finding of fact against the insured
- Severability of insured provided under multiple exclusions

Benefits

- Admitted Coverage
- Superior claims experience and handling
- Partnership with leading network assessment firm

What Controls Should A School District Have in Place?

The following does not outline all controls and procedures that your school district may require. These are the minimum controls and procedures you should have in place and why:

- **A designated individual, with school district wide responsibility.** This person will ensure the district is in compliance with privacy legislation and data protection laws (HIPAA, State Privacy legislation or similar laws) and data protection laws.
  - *Why? Someone in a position of responsibility within the school district needs to know what State and Federal laws apply so the school district is in compliance. For example, if medical records are obtained by the nurse or student athletes are required to submit medical records, the school district is bound by HIPPA legislation.*

- **A policy that requires encryption of electronic records/data files** for laptops, blackberries, desktop computers.
  - *Why? Encryption makes it difficult for data to be accessed*

- **A procedure detailing the proper destruction of data residing on systems or devices** prior to recycling or the refurbishing, resale or physical disposal
  - *Why? The trash is a prime target for people looking to obtain sensitive information. Paper and electronic copies should be shredded. Deleting electronic files on a computer does not mean the information no longer exists on the computer. Hard drives should be electronically shredded before donating or disposing of them.*

- **A proactive procedure for determining the severity of potential data security** breaches and providing prompt notification to all individuals who may be adversely affected by the breach must be in place.
  - *Why? If there is a breach of a system, the school district must notify everyone whose information is on the system that there has been a security breach. An Incidence Response Plan (IRP) is critical in these situations.*

- **A written Incidence Response Plan (IRP)** that provides step-by-step actions that should be taken in the event of a breach must be in place.
  - *Why? An Incidence Response Plan provides an action plan should a breach occur. The IRP should be written with an individual responsible for implementing the plan in the event of a breach.*

- **A written Information Systems Security Policy**, including laptop security must be in place.
  - *Why? This policy should address common security protocol, i.e. do not leave computer logged on while you are away, don't put log on and password on computer, etc. This policy should be provided to each new hire, and annually to all employees. Employees should be accountable if procedures are not followed.*

- **Procedures for honoring the specific marketing "opt-out" requests** of parents/students that are consistent with terms of your currently published privacy policy must be in place.
  - *Why? If the school shares information with a third party, the school district will want to make sure that the third party honors the "opt-out" request of the parents/students. In addition, if the school district posts pictures, addresses, etc., the school district must make certain the "opt-out" requests are honored. Failure to do so could allow estranged parents, grandparents, etc. to locate a child.*

- **Conduct regular reviews of third party service providers/vendors** to ensure they adhere to your contractual requirements for protection of sensitive data you entrust to them. Contracts should include indemnity provision for any liability arising out of their loss of sensitive information for which you are responsible.
    - *Why? Schools may use third party vendors for a wide range of services. For example, the school district may put students/families in touch with vendors/third parties such as school lunch programs, yearbooks, school rings, clothing, insurance providers, etc. In these cases, the school should make certain the third party/vendor is not sharing or selling the confidential information. If they are, the parents should be aware this is being done and have the option to "opt-out." Schools should also make sure that any third party/vendor that they deal with has indemnity agreements in the contract, which require at least $1 million in limits and the school should request a Certificate of Insurance.*

Claims

Many people only associate security/privacy breaches with large corporations or financial institutions, not schools. Schools, however, are just as vulnerable. Cyber security breaches rose in rural and suburban districts in 2008, with 14 percent of the districts reporting at least one IT breach compared to nine percent in 2007. Approximately 18 percent of school districts with enrollments of 1,000 to 4,999 reported security breaches in 2008 year, compared to only eight percent in 2007.[1]

- **April 2008, Public School – NC:** A school computer containing the names, test scores and Social Security numbers of students from three county high schools was stolen from a locked closet according to authorities. The school system sent home a letter to parents notifying them of the theft, which affected between 400 and 800 students.

- **May 2008, Public School - PA:** A 15 year old student broke into the school's computer system and accessed the names, social security numbers and addresses of 41,000 adult residents and 15,000 students.

- **May 2008, Public School - TX:** A laptop computer and flash drive containing the personal information of approximately 8,000 students was stolen from an employee's car. The flash drive contains students' Social Security numbers, personal information, schools those students attend, as well as their grade levels and birthdates. The drive also contained the Texas Assessment of Knowledge and Skills test results. The district was attempting to withhold information about the theft from the general public "because we hope to retrieve the flash drive before the information is accessed."

- **November 2008, Public School – TN:** Disk containing Social Security numbers and test scores was stolen from the principal's car. The school must now pay a firm to monitor the information of more than 200 students affected. A fraud alert was placed at the three credit reporting agencies. It will cost the school district more than $3,000 for one year of the monitoring service.

- **January 2009, Community College – OR:** The privacy of hundreds of community college students is put at risk, after someone steals a laptop computer from the campus at a community college. The school issued a press release stating that a new computer that contained student records for approximately 200 current and former students at the community college was stolen.

- **University of California at Los Angeles (UCLA):** A major security breach at UCLA occurred after a hacker broke into the campus computer system. University officials alerted approximately 800,000 current and

former students, faculty and staff. The database included social security numbers, home addresses and birth dates.

About ACE Westchester

ACE Westchester, part of the ACE Group, was one of the first to develop unique insurance products designed to help schools reduce the risks of embracing Internet-related business activities.

Today, ACE Westchester and its insurance providers is a leading global provider of comprehensive professional liability and network risks insurance products.

- ACE Westchester underwriters understand the complexities of network risk and use their expertise to accurately assess potential exposures
- The claims and legal experts within ACE Westchester draw upon a thorough and up-to-date understanding of the technology business arena, providing active and expert claims handling.
- ACE Westchester policies are backed by the financial resources and globally networked underwriting and claims expertise of the ACE Group of Companies.

[1] Information Week, Public Schools Improve Physical Security, But Cybersecurity Declines, May 19, 2008

PLEASE READ CAREFULLY

The above is only a summary and the underwriter reserves the right to request additional information and determine if a policy quote can be offered. If a policy is issued, please see the policy for actual terms and conditions. All products may not be available in all states and surplus lines products are only available through licensed surplus lines brokers.

Insurance provided by insurers within the ACE Group of Companies. ACE Westchester is the U.S.-based wholesale focused excess and surplus property and casualty operations of the ACE Group of Companies, headed by ACE Limited (NYSE: ACE). The ACE Group of Companies provides insurance and reinsurance for a diverse group of clients around the world. Additional information can be found at www.acewestchester.com.

Any recommendations or information provided herein is not intended as a substitute for advice from an expert or legal counsel you may retain for your own purposes. It is not intended to supplant any legal duty you may have regarding your operations.

Program Administered by:
Swett & Crawford
Lucille Sulock
215 572.4908
Lucille_sulock@swett.com

www.acewestchester.com