BPIC
A Member-Owned Insurance Company

Bishops' Plan Insurance Company
Safety and Loss Control News

Prepared by Gallagher Bassett | Risk Control Services *Spring 2023*

Inside this issue:

About BPIC

Bishops' Plan Insurance Company (BPIC) is a nonprofit group reinsurance captive and company established in 2003 to serve the risk management needs of Dioceses across the United States. We are 30 members. BPIC offers a customizable program that allows each diocese to work with its broker and BPIC's underwriting team in designing its own program structure as a portfolio of coverages. BPIC is led by its Board of Directors along with the spiritual guidance of its Episcopal Moderator. BPIC offers a member's only website comprised of risk management information. Contact information is provided below if you would like more information about BPIC or the website.

Phone:
Toll-Free: 877.325.BPIC (2742)

Email:
info@bpicmembers.org

Website:
www.bpicmembers.org

BPIC Risk Control Committee Members:

Tom Schadle (Chair), Tulsa
Mike Witka, Indianapolis
Bill Rafferty, Paterson
Patrick Ketchum, Springfield, IL
John Eric Munson, Las Cruces

School Safety—Visitor Management

Effective visitor management procedures are an important component for creating a safe and secure school environment. The procedure typically used by schools for visitor management programs is to have the visitor sign themselves in on a sign-in sheet. After signing in, a sticker is issued to the visitor that identifies who they are. The security risk in this system is that oftentimes, the signature on the sign-in sheet is illegible and the issued visitor sticker does not adhere securely to clothing.

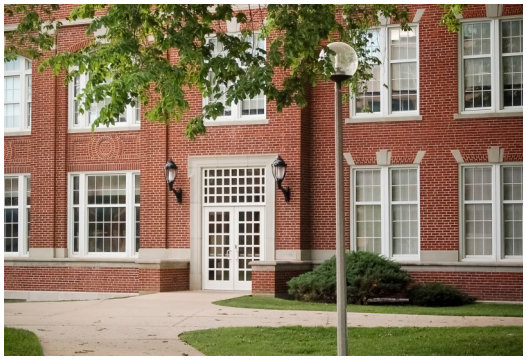
The following procedure was developed by RETA Security, Inc. and is designed to ensure that all visitors are accounted for from the time they enter the school to the time that they leave the building.

When a visitor arrives, the school receptionist or other designated personnel should greet the visitor and ask them for their photo ID. The school personnel should read the visitor's name on the supplied ID and print it legibly along with the time of the visitor's arrival, onto a corresponding school visitor sign-in sheet.

After entering the visitor's name on the sign-in sheet, verify that the picture on the visitor's ID matches the person that is standing there.

Keep the visitor's ID and put it in a designated, secure place in the office. Next, give the visitor a school-issued "Visitor" badge that hangs on a colored lanyard. Use a break-away lanyard so as not to endanger the visitor. The lanyards used for visitors should be the same designated color so that visitors are easily distinguishable from other personnel in the school building.

It is important to consider using lanyards in another color for all school staff to wear so that they are also easily distinguishable from visitors and other personnel who may be in the building.



Have the visitor put on the lanyard. The ID portion of the lanyard will hang in the middle of the person's body and will be visible at all times. This ensures that the lanyard does not fall off, is misplaced or not visible, which often happens with stickers. The important component of this system is not the ID, but the colored lanyard, which designates the person as a visitor and is visible on the person at all times.

At the conclusion of the visit, the visitor must come back to the main office to sign out. A school receptionist or other designated personnel must sign the visitor out and write down their time of departure on the sign-in sheet.

Ask the visitor to return the school's lanyard and then give back the photo ID to the visitor.

The importance of signing out a visitor at the end of their visit is critical to emergency situations. Should the school encounter an emergency scenario, they now have a record of who came into and left the building. This makes it easier for emergency responders to account for all persons who were in the building on that particular day.

-Information excerpted from RETA Security, Inc. *School Safety Strategies, Visitor Management.* http://www.retasecurity.com/.

Return to "Inside This Issue" index.

School Field Trip Safety

School-sponsored field trips are an excellent opportunity to provide students with educational opportunities that they normally would not experience in the classroom. Regardless of student grade level, whether the planned event is a day trip or overnight, the following are safety best practices to follow to ensure that everyone on the trip has a safe and rewarding experience.

Planning and Permission Slips

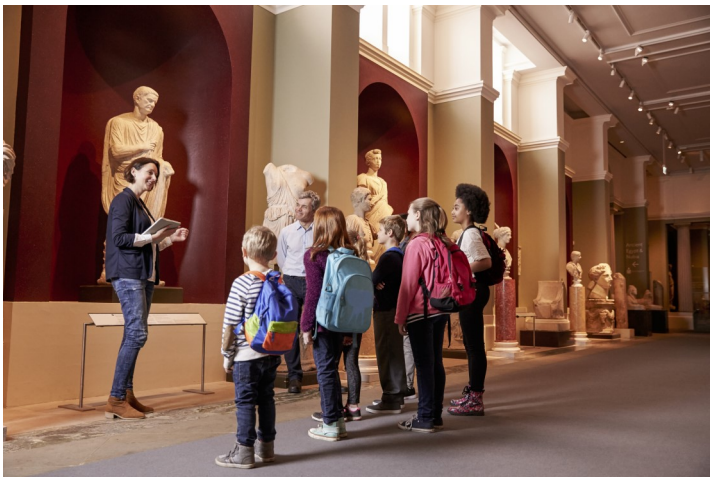
When planning the field trip, make sure the destination and content is age-appropriate to the children who will be participating and commensurate with classroom curriculum. Seek approval from the school board and once approved, notify parents of trip details by requiring each student to return a signed permission slip.

Permission slip information should include the date, name of minor, relationship to parent/guardian, address, description of the activity along with dates, times and location(s). The permission slip should also include a signature for the relinquish of claims against the school district and a medical release form, giving the representative of the school district authorization to seek medical treatment for the participant in case of injury or sudden illness. The medical release may also include a request for the child's health benefit medical card, emergency contact and family physician contact information and a space to list any relevant allergies, reactions or other issues the student may have. If the participant requires medication while on the trip, a Medication Authorization Form must be completed by the parent/guardian and the student's physician. For students who are not able to attend the field trip, provide an alternate experience held on campus related to the subject matter.

Teacher/Student Responsibilities

Discuss the subject matter of the field trip with students and answer any questions they may have. To keep students engaged during the field trip, require them to complete a graded worksheet of questions.

Prior to the trip, discuss with students expectations for behavior and emphasize that students who do not follow the instruction and directions of the teachers and chaperones or do not conduct themselves in an appropriate manner will not be able to participate on the field trip and will be subject to the school district's discipline policies. Students sent home for disciplinary issues will be transported at the parent's expense where allowed by state or local regulations. Remind students that they are



representing their school and that school staff will monitor their behavior.

Prior to leaving school, take roll and count students. Make a note of absences and report this information to the office. While on the field trip, teachers and chaperones should take a facecount of participants to ensure that all students are accounted for throughout the day. Encourage students to use the buddy system while on the field trip and educate them to stay alert with strangers and not to take any gifts or items that strangers may offer.

Remind students to dress appropriately for weather conditions and of the importance of wearing footwear conducive to trip activities.

Overnight Stays

When the need arises to extend a field trip for overnight stays, make provisions to ensure the safety and well-being of students and participants. Consider the following best practices.

Rules and Provisions

- Overnight stays must be approved by the Superintendent or School Board.
- Give careful attention to the location, safety and security of the facility selected.
- District administration should be responsible for ensuring that a criminal background check, which includes a sex offender registry check, has been completed for all chaperones.

(Continued on page 3)

School Field Trip Safety

(Continued from page 2)

- All students must have signed parental/guardian permission forms, which should be maintained by the chaperone assigned to them or the trip coordinator.
- All students must have an emergency medical release form, which should be maintained by the chaperone assigned to them or the trip coordinator.
- Emergency contact information must be collected from each student and maintained by the chaperone assigned to them or the trip coordinator.
- Emergency provision planning should be made for, but not limited to: theft, illness, vehicle emergency, weather delays and student misconduct.
- No students are allowed to stay in a room alone with a chaperone.
- A student will be permitted to stay in the same motel/ hotel room with a chaperone only if the chaperone is the student's parent or legal guardian.
- Shared rooms are only permitted with same gender students.
- A system should be put in place for communication and performing student counts.

Communication

Communicate information to students/parents in advance regarding schedules, departure locations, travel route, meal stops, lodging, emergency procedures, protocol for problems, and rules of conduct.

Transportation

Arrangements for motor pool vehicles or charter bus transportation should be made well in advance. Decide upon the route, stops and timetables.

Travel Outside of the Continental U.S.

No trip should be made to any country for which the U.S. Department of State has issued a travel warning. The warnings, as well as helpful information on international travel, are listed on the State Department's website at: www.travel.state.gov. In addition:

- Request parents to consult their medical care provider on whether any immunizations are advisable for their student (s).
- Careful selection and screening is essential to ensure that each chaperone has the necessary skills and experience for an international trip.
- Additional orientation should be provided if necessary, such as cultural issues, crisis management planning for travel abroad and first aid procedures.
- Funds should be available (traveler's checks, credit card, etc.) for medical or other emergencies.
- Special travel insurance may be necessary.
- If English is not the native language of the country, it is necessary to have an adequate number of chaperones who speak the country's native language.

Chaperones and Volunteers

Chaperones and volunteers are an integral part of helping the school system provide students with opportunities for educational and inter-personal growth outside of the classroom. Having chaperone/volunteer guidelines and policies in place are a good way to help ensure consistency in supervision for travel and activities sponsored by the school district. Effective screening, evaluation and placement of chaperones and volunteers is an excellent way to minimize the risk of liability when their services are warranted for school-related trips—whether a day trip or overnight stay.

Screening Process

An approved chaperone/volunteer meets the following requirements:

- An adult over the age of 18 (which is the minimum requirement; adults aged at least 21 are recommended).
- A criminal background check has been completed on the chaperone/volunteer.
- The chaperone/volunteer has been approved by the School District to supervise children.
- The school district has selected the chaperone/volunteer for a specific activity and the chaperone/volunteer is included on the school district's list for the given event. (Note: fulfillment of the first three requirements listed above is not a guarantee of the fourth.)

Supervision

School chaperones/volunteers are expected to support teachers during activities and provide supervision at all times. Students must be under adult supervision at all times. It is recommended that chaperones/volunteers refresh rules and expectations in compliance with school policy to help ensure safety and cooperation.

Criteria to be considered in determining the number of

(Continued on page 4)

School Field Trip Safety

(Continued from page 3)

chaperones needed include age and needs of the students, distance to be traveled, nature of the field trip activities and safety requirements.

Chaperone/volunteer guidelines:

- Sign-in must be completed at the office before participating in an activity or entering the school.
- All chaperones/volunteers must be included on a pre-approved list prior to the event.
- Chaperones/volunteers must follow directions given by the teacher(s).
- Smoking or the use of drugs or alcohol is not permitted while supervising students.
- Only the school district's students are allowed to participate; siblings are not approved.
- No student is to be left without a chaperone.
- Chaperones/volunteers will help maintain school standards of behavior.
- Chaperones/volunteers will adhere to School Code, Board Policy and School Rules.
- Chaperones/volunteers will work cooperatively with other school personnel to meet individual students with special needs.
- Chaperones/volunteers will assist the teacher(s) in implementing all policies and rules governing student conduct.
- Chaperones/volunteers will meet accepted standards of professional behavior.
- Chaperones/volunteers will refer all disciplinary issues to the school administrator present.
- Chaperones/volunteers must report all incidents to the school administrator present.
- Chaperones/volunteers are expected to take all necessary and reasonable precautions to protect students.

Transportation

Field trip transportation will be ordered to accommodate the students and teachers. Chaperones/volunteers are welcome to ride if space allows, but additional transportation cannot be ordered to accommodate chaperones/volunteers. Chaperones/volunteers must be prepared for the possibility of driving their personal vehicle at their own expense and liability. Students are required to use the transportation provided by the school district to be part of the class activities.

Return to "Inside This Issue" index.

Responding to Slip, Trip and Fall Accidents

In addition to having policies, procedures and training on the prevention of slip, trip and fall accidents, it is also important to be prepared to respond to these incidents. Development of a formal policy and conducting training on how to respond to a slip, trip and fall accident will go a long way in providing immediate assistance to the injured person and reducing claims costs and the possibility of potential legal recourse.

The following information, excerpted from *A Four-Step Response to Slip and Fall Accidents,* published by EMC Insurance, provides actions to take in response to slip, trip, and fall accidents.

Offer Assistance to the Injured Person

The primary focus following a slip, trip, fall injury is to address the injured person's immediate needs. When responding to an injured person, instruct employees to provide only the level of care they are qualified to offer. Immediate actions include:

- Determine if an injury has occurred and the necessity of medical assistance.
- Call 911 if necessary.
- Refrain from making statements to the injured person related to cause, responsibility, or blame and do not refer to the payment of medical bills.

Document the Incident

Regardless of whether or not the person is injured, document the incident. Record the person's full name, address and contact information. Survey the physical area where the accident occurred to determine the location of the accident and any potential causes. Write down this information along with the type and condition of footwear worn by the affected person. Take photos if necessary and review video surveillance footage if available. Complete a formal incident report according to your organization's policies and procedures.

Report the Incident

Report the incident to the appropriate channels within your organization as soon as possible. If the affected person is an employee, follow policies and procedures for workers' compensation cases, including filling out a first report of injury form.

Investigate the Accident

Whether the incident was an accident or a near miss, conduct an accident investigation in accordance with your

(Continued on page 6)

Cyberattack Preparedness

As a result of the Russian invasion of Ukraine and the recent sanctions that have been placed on Russia by the U.S. and other countries, businesses and organizations have been advised to be on alert for an increase in cyberattacks. As a result, it is important that businesses/organizations and employees know how to prepare for and respond to these types of threats.

The Cybersecurity & Infrastructure Security Agency (CISA) "... recommends that all organizations—regardless of size—adopt a heightened posture when it comes to cybersecurity and protecting their most critical assets." In addition to heightening and protecting internal systems, it is critical that communication be provided to employees asking them to be aware of and vigilant of anything deemed suspicious or unusual from a technology or data perspective, which could arrive in the form of an email, text or phone call.

Who is at Risk?

According to *CNN Business,* cyberattacks conducted by Russian organizations could target the following entities, disrupting U.S. business operations and the general public:

- **Ukrainian Businesses:** Companies in the U.S. working with organizations in the Ukraine need to be cautious due to connections with Ukrainian systems. These systems may be pivot points to other targets.
- **U.S. Military Technology:** Russian cyberattacks could target foreign military technology, including spy imagery captured by commercial satellites potentially located in the U.S.
- **Domestic Targets:** Large-scale U.S. infrastructure is at risk, including banks, local governments and businesses. Recent notable attacks perpetrated by Russian organizations included online disinformation campaigns such as interference with U.S. elections, the SolarWinds hack (which infiltrated several government agencies in 2020), a ransomware attack that forced shutdown of one of America's largest fuel pipelines and an attack on the world's largest meat producer, JBS.

In an interview with *CNN Business*, Herb Lin, senior research scholar for cyber policy and security at Stanford University's Center for International Security and Cooperation recommends that the public and private sectors, "Ensure any potential vulnerabilities in your devices are patched, whether that's through software updates or additional security measures such as two-factor authentication, where a code from an external device or app is used in addition to your password."

Cybersecurity Recommendations

The following recommendations, excerpted from CISA.gov provide information on how businesses and organizations can help to prevent a cyberattack.

<u>Reduce the likelihood of a damaging cyber intrusion</u>

- Validate that all remote access to the organization's network and privileged or administrative access requires multi-factor authentication.
- Ensure that software is up-to-date, prioritizing updates that address know exploited vulnerabilities identified by CISA.
- Confirm that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes.
- If the organization is using cloud services, ensure that IT personnel have reviewed and implemented strong controls outlined by CISA's guidance.
- Sign up for CISA's free cyber hygiene services, including vulnerability scanning, to help reduce exposure to threats.

<u>Take steps to quickly detect a potential intrusion</u>

- Ensure that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behaviour. Enable logging in order to better investigate issues or events.
- Confirm that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated.
- If working with Ukrainian organizations, take extra care to monitor, inspect, and isolate traffic from those organizations; closely review access controls for that traffic.

<u>Ensure that the organization is prepared to respond if an intrusion occurs</u>

- Designate a crisis-response team with main points of contact for a suspected cybersecurity incident and roles/ responsibilities within the organization, including technology, communications, legal and business continuity.
- Assure availability of key personnel; identify means to provide surge support for responding to an incident.

(Continued on page 6)

Cyberattack Preparedness

(Continued from page 5)

- Conduct a tabletop exercise to ensure that all participants understand their roles during an incident.

Maximize the organization's resilience to a destructive cyber incident

- Test backup procedures to ensure that critical data can be rapidly restored if the organization is impacted by ransomware or a destructive cyberattack; ensure that backups are isolated from network connections.

- If using industrial control systems or operational technology, conduct a test of manual controls to ensure that critical functions remain operable if the organization's network is unavailable or untrusted.

Security Guidance for Email Phishing, Text Messages and Phone Calls

Employee vigilance for email phishing scams is another critical component to maintaining online security. Your IT Security department should provide clear guidance and communication to employees on how to identify a phishing email scam, provide information related to any current scams and the steps to take should employees receive suspicious emails.

For example, if a suspicious email is received, the first question to ask is: *Were you expecting the email?*

If the email was unexpected, ask the following questions:

- Is the email domain an email domain you have worked with or seen before?
- Has any part of the business mentioned that you will be receiving an email from an external email address recently?
- Does an email like this usually get sent to you?
- Does the email ask you to undertake an action an attacker would typically ask you to do? (E.g. "click on this link, download this attachment, enter your details on this web page.")
- If the email message looks odd, **report it immediately** via your normal channels. If you have a "Report Phishing" button on your Outlook ribbon, use it to report the phishing.

In addition to phishing email scams, text message and phone scams are another channel cybercriminals will use to gain unsolicited personal and business information. If you receive odd text messages or phone calls, think first before taking action and report suspicious receipt to your IT Security department.

Additional Resources

- Ready.gov/cybersecurity
- DHS Stop. Think. Connect.™ Campaign
- Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure
- StopRansomware.gov

Sources:

Gutman, Rachel. (2022, February 24). What Americans Should Do to Prepare for Russian Cyberattacks. Retrieved February 25, 2022 from https://www.theatlantic.com/technology/archive/2022/02/ukraine-war-russian-hack-cybersecurity/622922/

Cybersecurity & Infrastructure Security Agency. Shields Up. Retrieved February 25, 2022, from: https://www.cisa.gov/shields-up

Ready.gov. Cybersecurity. Retrieved February 25, 2022, from: https://www.ready.gov/cybersecurity

Rishi Iyengar, Sean Lyngaas, Julia Horowitz, CNN Business. (2022, February 24). US braces for Russian cyberattacks as Ukraine conflict escalates. Here's how that might play out. Retrieved February 28, 2002, from: https://www.cnn.com/2022/02/24/tech/russia-ukraine-us-sanctions-cyberattacks/index.html

Return to "Inside This Issue" index.

Responding to Slip, Trip and Fall Accidents

(Continued from page 4)

organization's policies and procedures. Focus on determining the root cause of the incident and do not place blame on the employee/affected person. Ask the "Who," "What," "When," "Where," "How" questions. Determine if physical hazards/ unsafe conditions or human behaviors/unsafe acts contributed to the accident.

Examples of physical hazards/unsafe conditions could include the presence of black ice in the parking lot, water on the floor from a spill or leak within the facility, or worn stair treads.

Human behavior/unsafe acts could include carrying a load that obstructed the person's sight, tripping over a box left in an aisle, or texting while walking.

Implement Corrective Actions

Once the accident investigation is complete, implement corrective actions to ensure that a similar accident does not happen again and address the unsafe exposure(s). Corrective actions could include making repairs/enhancements to the facility/work area or providing employee training and communication on the identification and prevention of slip, trip and fall hazards. If training is conducted, document the time and date of the training sessions and the names of the employees in attendance.

-Information excerpted from EMC Insurance. *Loss Control Insights, A Four-Step Response to Slip and Fall Accidents.* Retrieved on April 5, 2023 from https://www.emcins.com/losscontrol/insights-d/2015/11/slipfall/.

Return to "Inside This Issue" index.

BPIC
A Member-Owned Insurance Company

The information in this report, provided by Gallagher Bassett Services, Inc., was obtained from sources which to the best of the writer's knowledge are authentic and reliable. Gallagher Bassett Services, Inc. makes no guarantee of results, and assumes no liability in connection with either the information herein contained, or the safety suggestions herein made. Moreover, it cannot be assumed that every acceptable safety procedure is contained herein, or that abnormal or unusual circumstances may not warrant or require further or additional procedures.

GALLAGHER BASSETT
GUIDE. GUARD. GO BEYOND.

17771