May 2022

A quarterly newsletter of the Diocese of Trenton Risk Management Program

Diocese of Trenton
Risk Management Quarterly

Parishes, Schools, Cemeteries & Catholic Institutions

Summer Edition

Back to Ministry
and Back to a Strong Post-Pandemic Footing

By William Staub, Associate Director of OCYP, Diocese of Trenton
and Margaret Dziminski, Associate Director of OCYP, Diocese of Trenton

As the world turns to post-pandemic activity, it is important that we continue to maintain best practices of the safe environment program in all ministries. Covid-19 is not an excuse to let our guard down or brush off the essential norms of a safe environment.

It is likely that Covid-19, like influenza, will remain part of the daily health vernacular, so we must move ahead and re-establish our footing to monitor and maintain a safe environment for children and vulnerable adults as in-person activities have returned.

In all sectors of our society, we have experienced significant Covid-19-initiated adaptations and changes over the last two years. We are finding that some of the pandemic forced changes have driven beneficial adaptation in our programs. Online VIRTUS Training has become an effective tool within the existing safe environment program. Training, in-person or online, prepares employees and volunteers to bring the knowledge and awareness to all of our ministries for effective compliance and to provide a safe environment for minors and vulnerable adults.

As we move into Spring of 2022, it is important that we focus on the return to increasing in-person activities with all parish programs, in addition to religious education. Each parish, school and ministry within the Diocese of Trenton should review their safe environment compliance standards to be sure they are on the right footing. The backbone of compliance depends upon the rigorous monitoring and enforcement of background checks, safe environment training, and the understanding of the standards of the Diocesan Code of Conduct. Compliance Auditing for the Articles and Essential Norms of the USCCB Charter with onsite visits has returned.

Background Checks

Article 13 of the Charter instructs each Diocese to evaluate the background of all diocesan and parish personnel who have regular contact with minors, youth, and vulnerable adults.

This would include all priests, deacons, and seminarians regardless of contact with children, youth, and vulnerable adults.

This policy also pertains to all religious, employees, certain 1099 contractors, volunteers, and third-party vendors who have direct or indirect contact with minors or vulnerable adults during their work or volunteer activity at any Diocesan entity. Every employee, including 1099 contractors such as bookkeepers and music directors, in regular positions of employment who are not W2 employees are required to undergo criminal record background checks at regular intervals as determined by the Executive Director of Child Protection for the Diocese of Trenton. The exception is school personnel who are cleared and monitored by the New Jersey Department of Education.

Safe Environment Training

Article 12 of the Charter instructs each Diocese to maintain "Safe Environment" programs which the Bishop deems to be in accord with Catholic moral principles. The Diocese is to provide education and training for minors, parents, ministers, employees, volunteers, and others in ways to sustain and foster a safe environment for children, young people, and vulnerable adults.

The Diocese of Trenton mandates that all priests, deacons, seminarians, religious, employees, volunteers, faith formation students, Catholic School students, and third-party vendors must receive Safe Environment training as prescribed by the Charter. The Diocese of Trenton utilizes the following programs:

- VIRTUS, Protecting God's Children for Adults and all re-certification programs

continued on page 5

Cybersecurity Threats to Diocesan Schools

COVID forced the technology departments in schools to rapidly ramp up local network capabilities and services. Students needed to be educated in their homes and educators required remote access to resources for teaching, assessing, grading and keeping attendance.

Technology leaders in schools and parishes quickly rose to the occasion at warp speed. Cybersecurity concerns lagged behind the imperative to create remote learning environments that could be used by the novice and the experienced alike.

Cybersecurity attacks on schools are increasing nationwide. While large school districts represent many of the reported targets, small schools in wealthy communities are becoming equally attractive to cyber criminals.

The number of cyberattacks perpetrated on schools is reported to have increased six-fold in the past five years. This is a low estimate as there are little or no requirements for schools to report incidents.[1]

Attacks include:

- Student data breaches where thieves threaten to publish personal information unless a ransom is paid
- Human resource data breaches where thieves gain access to sensitive personnel data including Social Security numbers
- Ransomware attacks where school personnel find their systems inaccessible and high financial ransoms are required to get the system re-activated
- Business email scams where thieves cleverly send emails by mimicking authentic school personnel requesting the issue of a check or money transfers into designated accounts
- Website defacement where destructive and hateful content is added to school sites
- Invasions of online classes or school meetings where unwanted individuals interrupt school operations

These attacks are perpetrated by:

- Highly-skilled and organized online criminals
- Unwitting teachers, administrators, and parents who unknowingly allow network access to criminals
- Tech-savvy students who want to create mischief
- Vendors of school software programs who do not have adequate security practices

National and local examples of the difficulties schools have experienced:

- A Missouri school district was forced to cancel classes for two days when cyber thieves locked their network. Not only was classroom access to learning and assessment tools impossible, but phone systems, attendance tools, classroom management records, and security cameras were shut down.[1]
- In 2020, Baltimore, Maryland County Public Schools spent over $9 million to recover from a ransomware attack.[1]
- About five years ago, right here in Mercer County, an administrator received a request from the school's accounts payable clerk to pay a little over $3000 to a vendor commonly used by the school. The administrator emailed questions about the invoice to the clerk who shared information from the electronic invoice. The administrator authorized the payment and it was mailed. A hacker in upstate New York had entered the network, identified frequent vendors, and communicated as the accounts payable clerk with the appropriate system email.

In order to avoid the loss of money to hackers, interrupted instruction, the legal complications from personal data theft, and the embarrassment from damaged websites, all schools must invest in cybersecurity strategies. Understandably, resources may be limited, especially in small parish schools. Some of the strategies below are available to any institution.

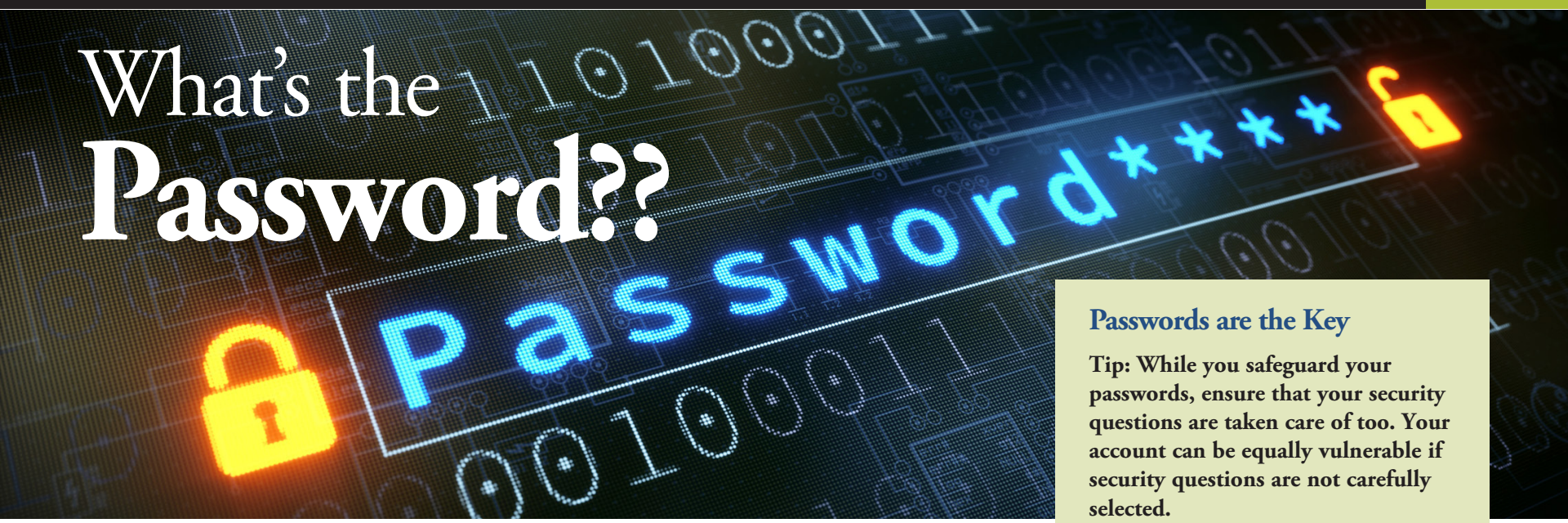
1. **Create discussion groups among school and parish technology coordinators.** High schools in the Diocese found that meeting periodically during the school year allowed them to lean on a wide variety of expertise located within school technology departments. Open and honest conversations about threats and resources allowed this group to bargain collectively for resources, create redundancy of data, and develop well-formed policies.
2. **Build a solid infrastructure.** Invest in quality firewalls. Investigate best practices for allowing off-site access to networks. Institute regular password change procedures. Inquire about encryption systems especially when demographic or financial information is housed in local databases.
3. **When purchasing data management, assessment, attendance and discipline systems, make sure these vendors have responsible and effective cybersecurity programs in place.**
4. **Educate <u>all users</u> on methods for supporting the security of computer services.** One of the weakest links in any community that relies on technology is the end user. Cyber criminals are well studied and very clever.

continued on page 6

Diocese of Trenton Risk Management Quarterly

If you have any questions, comments or topic requests for future newsletters, please send an email to newsletter@dotinsurance.org

What's the Password??



Passwords are the Key

Tip: While you safeguard your passwords, ensure that your security questions are taken care of too. Your account can be equally vulnerable if security questions are not carefully selected.

Abridged and Edited from the blog, "Passwords are the Key" by WillisTowersWatson (WTW)

Set a Strong Password

As we live and work online more than ever, there are so many applications/websites that require a login with a username and password, and remembering all of them is challenging.

The average person has at least 30 passwords for daily life, across personal accounts and for their work devices and systems. Obviously, some are more important than others. Below are a few different methods you can try to set strong passwords that you will have a chance of remembering without compromising them by writing them down!

Methods for Creating Strong, Secure Passwords

Create a Passphrase

A passphrase is longer than a password and contains spaces or symbols in between words. For example: **The road to success is always under construction!**

A passphrase can also contain symbols or special characters, upper and lower case, and does not have to be a proper sentence.

The passphrase could be the whole sentence typed out in full as shown above (making for a very long password), or you could take characters from the phrase to make your password. For example: **TR2SUCCESS1@uc!**

As before, at least 15 characters is the recommended minimum. For this reason, we typed one of the words out in full.

- Passphrases are easier to remember
- They satisfy systems that require more complex passwords
- All major operating systems including Windows, Linux and Mac, allow passphrases of up to 127 characters long, so you can opt for longer passphrases for maximum security
- Passphrases are very difficult to crack, brute-force, or pre-compute

Tip: Ensure that the phrase you choose is not a well-known quote, or a line from a play or song that could be easily guessed by someone who knows you. It is best if you make up a rhyme of your own.

Longer is stronger!

To save yourself from a brute force attack, it is always advisable to go longer when it comes to character length. There are hackers who claim to be able to crack any 8-character Windows password in minutes with programs that try hundreds of billions of guesses per second.

Mix it Up

Use a combination of upper case, lower case, symbols or special characters and numbers in your passwords. The more complicated you make it, the harder it is to crack using brute force. However, avoid well-known patterns like swapping certain letters for numbers or symbols such as: **a=@, s=5, 0=o, 1=i**

If your system allows, try adding a space-bar character somewhere in the password.

Sets of Passwords

Try to create a set of resembling passwords for each purpose. For example:

Group 1 = Strongest password with second factor authentication

- Your login to your parish, school, or diocesan computer (securing corporate systems and confidential data)

Always ensure this is totally unique and never re-use this anywhere else.

Group 2 = Very strong password, plus other authentication method (multi-factor authentication)

- Personal banking (access directly to funds)
- Online shopping accounts (transactions are made with these)
- Payment services, e.g. PayPal

Because these allow access to your personal finances, they should be unique, although they could follow a pattern which helps you to remember them.

Group 3 = Simpler password

- Sites used only for browsing; you never make transactions or give personal credentials including your personal email
- That is, if group 3 accounts were compromised, you wouldn't lose anything

Use a Password Manager Program

Most password managers can generate complex, random, and unique passwords for you to use when signing up for accounts and services, or you can add your own passwords into the PM program.

The password manager is a bit like a vault inside which you keep your precious jewels. You will usually have one long and strong password to open the vault and then you can cut and paste or copy the complex passwords out of the safe into the system you are logging into. Yes, it might take a little longer every time you need to login, but it would safeguard your information more effectively.

Tip: You must not forget the master password that opens the "vault." ■

Important Update: Internet Explorer 11

Internet Explorer (IE) 11 is the last major version of Internet Explorer. As of June 15, 2022, the IE 11 desktop application will no longer be supported on certain versions of Windows 10. Internet Explorer mode in Microsoft Edge will be supported through 2029.

Keeping Our Churches Safe for All

By Mary Liz Ivins

Our churches are meant to be places of welcome and comfort for all. However, incidents of violence in synagogues, mosques and churches across the country challenge this open and peaceful environment. Parish teams need to assess the potential threats to their communities and create reasonable and responsible plans to minimize any risk to those who come for worship and community.

Recent years have taught that dangers do not only come from an active shooter, but from health emergencies, weather disasters, fire, robberies, domestic violence "spillover," vandalism, and child abuse. The Catholic Church has worked tirelessly to create systems to protect God's children. In addition to strict adherence to these safety precautions, it would be wise for parishes to create security plans to protect and respond to all potential threats.[1]

Within every parish, there are members who have expertise in various areas of security. There may be law enforcement professionals, health workers, contractors who deal with facility safety issues, technology experts, and fire prevention personnel sitting in the pews. Call on knowledgeable volunteers to form a security council or committee. Their challenge will be to assess the parish facility and operations and build a security plan that lives within the mission of the parish. Security risks can raise dramatic emotions. It is essential that members of this committee approach their task in an intelligent, emotionally balanced manner. The plan they develop must support and never obstruct a parish's mission. For example, an access control system may enhance security but if it makes it difficult for those who need the church to enter, the plan would be defeating the church's purpose.

A word about consultants: Hundreds of experts and security companies can be found by searching the web for "Church Security." A parish may have the financial ability to contract with a service, but many may not. If a provider is considered, it is essential that his or her training and experience be carefully reviewed. Multiple references from similar institutions should be attained. In every community, there are "consultants" who can offer free insights. Consider speaking to local law enforcement. Contact an administrator from a nearby school. Schools have been challenged by law to develop and implement a wide variety of security protocols. Reach out to leaders of neighboring houses of worship. Host a discussion with them on what they may be doing to keep their congregations safe.

Parish security teams might consider the following in their planning:

- Complete a walkthrough of all parish facilities. Create a document that shows all buildings, windows and exits. Assess how often and in what way facilities are used. How are meeting rooms, classrooms, sanctuary and offices accessed and secured? Are all exits clear and well-signed?
- Do a walkthrough with local police. Ensure they have a copy of the facility diagram and are aware of exits and entrance locations. Consider giving them a copy of master keys and access to the parish's schedule of events. Invite on-duty officers to stop in for coffee. Positive relationships with local law enforcement enhances their ability to protect and serve.
- Create an effective communication plan. Make sure contact information is readily available for police, fire stations, the Pastor, parish staff, and security committee members. Designate who will create messages to send to parishioners, local community members, and the press.
- Consider security technology. Cameras, access control systems, and alarm systems are excellent supports when building a safe church property. Two-way radios enhance communication, especially when the parish has multiple buildings. Require event leaders to sign in with the office or rectory and have them take a radio to their meeting or class. This allows for immediate staff notification when problems arise. Radios are often easier to grab than cell phones and no phone number is needed.
- Ensure all WiFi networks are secure. Online donation programs diminish the amount of cash on premises. Grants for physical security enhancements are available from FEMA under the Nonprofit Security Grant Program.[2]
- Some parishes have greeters who welcome people to Mass. "Simply saying 'Hello' can prompt a casual conversation with a new person, providing an opportunity to observe and establish a connection."[3]
- Train volunteer security personnel for evenings when there are meetings and educational programs. No event leader should ever be alone in a building/parish during a calendared event.
- Have the security committee meet with the Safe Environment Coordinator to learn what is required from all staff and volunteer workers. This committee could then periodically review all documents and procedures to assure that practices are in place to keep children safe.

According to Mike McCarty, CEO of SafeMinistry Solutions, "The definition of security is the absence of risk. ...That doesn't exist." The goal of a good security plan is to diminish the extent of harm a threat can cause. Develop a prevention plan that diminishes risks and offers the parish a greater sense of security. Gently educate parishioners through church bulletins to prepare them to respond safely to dangers. Reiterate that if they see or hear a potential threat, they must say something to parish personnel. This can be as simple as noting a blocked entrance or as complex as reporting an overheard threat. Above all, remember that after all precautions are taken and all effective planning is done, prayer to the Father who is always with us is truly essential in any security plan.

Additional Sources:

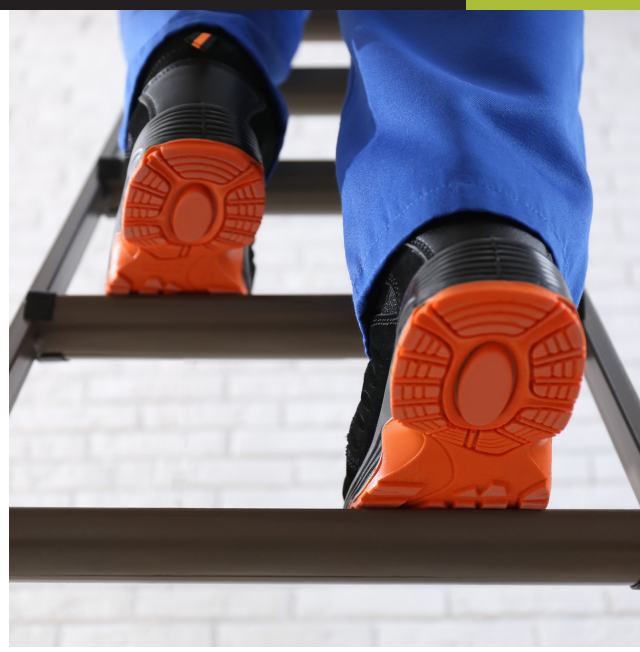
- Recommended Best Practices for Securing Houses of Worship for People of All Faiths: asisonline.org/globalassets/get-involved/councils/documents/best-practices-securing-houses-of-worship.pdf
- Everything You Must Know About Church Security: A Comprehensive Guide: donorbox.org/nonprofit-blog/church-security/
- Faith-Base Security Strategy: hnjhomelandsecurity.gov ■

(1) https://www.ncregister.com/features/keeping-churchgoers-safe-strategies-for-houses-of-worship, Susan Klemond, Keeping Churchgoers Safe:Strategies for Houses of Worship,2/22/22

(2) https://www.fema.gov/grants/preparedness/nonprofit-security

(3) https://www.cisa.gov/sites/default/files/publications/The%20Power%20of%20Hello%20Guide%20for%20Houses%20of%20Worship_508.pdf

Ladder Safety



Ladders are simple tools, but they can be the source of serious injuries if not used properly. It is important to take as much care when using ladders as you would when using other tools and equipment.

Risks Involved When Using Ladders

The most common accident involving ladders is falling from one, potentially injuring the user as well as others in the area. There are several factors that can contribute to falls from ladders, including:

- Climbing or descending too quickly
- Making sudden movements
- Not paying attention
- Using ladders that are damaged
- Wearing improper footwear
- Using a ladder when you are not in good health

Tips for Using a Ladder

- For starters, never climb a ladder if you are tired, feel dizzy or have trouble keeping your balance.
- Inspect a ladder for damage beforehand. Never use a ladder that is damaged or has loose or missing parts.
- Be sure to wear slip-resistant shoes. Clean and dry the soles before climbing; it is especially important that there is no oil or food residue on the soles.
- Select a ladder that is the proper size for the task and don't use a ladder that requires you to stretch to get the job done.
- Sometimes instructions regarding height and weight limits can be found on ladders; look to see if there are any instructions and be sure to follow them.
- Set the ladder on firm, level ground that is not slippery. Inspect the area for safety; do not set up a ladder in front of a closed door that can be opened towards the ladder and cause it to be knocked over.
- Climb a ladder slowly and take deliberate steps. Never climb more than one step at a time and never jump down from the ladder.
- Do not carry anything that prevents you from having a good grip on the ladder. Being overloaded with items when climbing can lead to slips and falls and can injure people in the area if the objects are accidentally dropped.
- Do not lean to the side to put objects away; this increases your chances of falling sideways off the ladder. Instead, descend the ladder and move the ladder to where you need it.
- Use ladders only for the purpose for which they are intended.

Best Practice for Climbing a Ladder

It is good to use the Three-Points-of-Contact method when climbing a ladder. Face the ladder and have either two hands and one foot or two feet and one hand on the ladder at all times. This helps to keep the climber steady when ascending or descending the ladder.

If ever in doubt about the safety of a ladder, 1.) do not use the ladder and 2.) speak to a supervisor.

For more information on ladder safety in English and Spanish, please see OSHA's publication, **Falling Off Ladders Can Kill: Use them Safely**: https://www.osha.gov/sites/default/files/publications/OSHA3625.pdf ■

Back to Ministry and Back to a Strong Post-pandemic Footing, continued from page 1

- Loyola Press, Growing with God – Grades K-8
- RCL Benziger, Family Life – Grades K-8
- Teen Lures – High School and Youth Groups

Code of Conduct/Christian Witness Statement

Article 6 of the Charter instructs the Diocese to have well-publicized standards of ministerial behavior and appropriate boundaries for all priests, deacons, seminarians, employees, volunteers, and third-party vendors.

A signed Code of Conduct or a Christian Witness Statement must be completed upon onset of ministry or acceptance of contract and renewed as necessary with any content changes. These program requirements are only effective when we remember that they do not replace but are in collaboration with a high degree of vigilance and attention to the protection of young people and vulnerable adults in our programs and ministries.

To say we offer a safe environment for all means that we continue to communicate with our employees, volunteers, parents, and all those whom we serve.

We must remember that those we minister to and with are to be treated with respect and dignity every time they are with us. The key to a successful program is full compliance - 100%, no exceptions.

The Diocese of Trenton monitors and audits every parish and school to ensure compliance. On-site audits have resumed and every effort is made to verify that every person who should be background-checked and trained has been in accordance with our Safe Environment Program, no exceptions. ■

When is the Last Time You Looked at Your AED?

Every 90 seconds in America, someone suffers Sudden Cardiac Arrest (SCA). The national survival rate for SCA is only 5%. For every minute that goes by without CPR and the use of an AED, the patient has a 10% less chance of survival. Average response time for an ambulance is 8-12 minutes.

As a first step, your church and school know these statistics and bought an AED. The question now is: when was the last time you looked at your AED? An Automated External Defibrillator (AED) is truly a lifesaving medical device, but it does need some care to keep it in full rescue ready mode. There are several models of AEDs on the market, and all of them need to have the pads (electrodes) and batteries replaced as per the manufacturer guidelines. In addition, every AED should be registered with the manufacturer.

This brings us to a problem in the AED world: Recalls. Every AED manufacturer has had a recall of their AEDs at one time or another. An AED is a Class 3 medical device that is regulated by the FDA. If your AED is not registered with the manufacturer, it is unlikely that you would find out about a recall.

AEDs also have a lifespan, and many manufacturers give notice to the end user when they are going to stop supporting the AED model. If your AED is not registered, or if the e-mail of the contact person is not up-to-date, you may never realize the AED is no longer supported until you try to purchase pads or batteries.

Having an AED is good. Having a Rescue Ready AED is better, and having a person confident enough to use the AED is best. Training, either an overview of the AED, or better yet, a full CPR/AED certification course, should take place every 2 years.

This leads to an important point. Where you buy your AED is more important than which AED you buy. Your vendor should keep you advised of any recalls, software upgrades, or when an AED will no longer be supported.

Ask before you buy if your vendor provides continuous updates regarding the equipment you purchase through the end of useful life. Ask if your vendor registers every AED they sell before delivery of the unit. Does your vendor provide training?

When was the last time you looked at your AED?

Visit the Diocese of Trenton Insurance Website **www.dotinsurance.org** and watch the AED/CPR Demonstration Video.

Jim Schatzle, Paramedic & President of TEAM LIFE

TEAM LIFE is a vendor to many Diocese of Trenton parishes and schools, providing equipment, supplies and training.. They provide equipment, supplies and training to many of our schools and churches ■

Cybersecurity Threats to Diocesan Schools, continued from page 2

It is very easy for a user to fall prey to a well-crafted criminal attempt to gain access. The Diocese offers KnowB4, an excellent online training resource, to all Diocesan entities. Contact the Director of Computer Services, Anthony Delorenzo, **adelorenzo@dioceseoftrenton.org**, for access to this resource.

No matter how simplistic or complex a school's computer services may be, building an effective cybersecurity plan is absolutely essential.

One computer with an email to or from a parent, an assessment meant to measure learning, a list of student addresses, or a link to a wonderful learning site becomes a liability if proper caution is not practiced.

Avoid the interruption of instruction, the embarrassment of hacked demographic information, and the financial losses from cyber ransoms by learning more about cyber threats and instituting good security practices.

Additional Resources

- **Nine Tips for a Robust Discussion on Student Data Privacy:** iste.org/explore/Lead-the-way/9-tips-for-robust-discussion-on-student-data-privacy
- **Data Encryption 101: A Guide to Data Security Best Practices:** preyproject.com/blog/en/data-encryption-101/

(1) The State of K-12 Cybersecurity: 2022 Annual Report https://static1.squarespace.com/static/5e441b46adfb340b05008fe7/t/6228bfe3f412c818293e16e1/1646837732368/StateofK12Cybersecurity2022.pdf ■

Items of Importance

PosterGuard Compliance Notice: NJ Family Leave Act Updated 12/21/2021

The NJ Family Medical Leave Act was amended to expand protection to employees forced to take time off to care for a family member during the COVID-19 outbreak, with up to 12 weeks of unpaid family leave in a 24-month period. Be prepared for FMLA requests made under NJ or Federal Labor Law. The process begins with determination of employee eligibility. If leave is requested, provide the employee with a notice of eligibility and rights and responsibilities, which are program-specific. Determine if a medical certification is required. Is the leave requested qualified? State and federal qualification may differ. Grant or deny the leave as quickly as possible with written notice. Health benefits must be maintained for the duration of the leave. Upon return, the employee must be returned to their previous or an equivalent position. Keep a file and seek assistance from the Diocesan Benefits Department when clarification in required.

NJ Poster Update 4/22/2022 – A new update of the NJ Employment Law Poster will be shipped to participating locations. If the update is not received by May 15, please send an e-mail to Joe Cahill at **jcahill@dioceseoftrenton.com** with your parish name and address to initiate shipment tracking.

The NJ Earned Sick Leave Poster has been updated; however, the changes are not mandatory. The existing poster is fully compliant. To view or download the new poster, go to: **https://www.nj.gov/labor/forms_pdfs/mw565sickleaveposter.pdf**

NJ Employment Law - Hiring Preference for Workers Injured at Work, NJ A2617/S-2998

Signed and effective September 24, 2021, the NJ Workers Compensation Law requires employers with 50 or more employees to provide a "hiring preference" to any employee who has a job-related injury and has reached Maximum Medical Improvement (MMI) where the worker cannot return to their former job with the employer. The amendment requires the employer to afford the employee a preference in hiring for any of the employer's existing and open positions for which the employee can perform the essential job functions. Employers are not required to create a new position or remove a current employee from an existing position in order to accommodate the injured worker.

Roof Inspection Program

As the weather improves and the wind becomes less of a factor, the Diocesan Roof Inspection program will gear up to complete inspections at all parish properties before winter begins. JD Cummins & Company has been hired, at no expense to the parishes, to conduct roof inspections that include gutters, flashing, roof penetrations, roof coverings, and chimneys. They will produce a report with recommended corrective action to address immediate and near-term (less than a year) issues. A representative from JD Cummins will contact the business manager to arrange a date and time. They will bring their own ladders and a drone. No assistance is required by parish personnel unless roof hatch or building interior access is unavailable. The parish business manager or facilities manager is always welcome to participate in the inspection. In order for the program to be cost effective for the Diocese, inspections are coordinated geographically so that several inspections can be conducted in a single day, reducing overall cost. If there are any questions, please contact Joe Cahill, **jcahill@dioceseoftrenton.org**, or 732-284-1600 (cell).

Electrical Inspection Program

Infrared Thermographic Inspections of electrical systems will resume at parishes starting this month and will continue through October. The program was interrupted for two years due to COVID. As with the roof inspection program, inspections are coordinated geographically for cost efficiencies. The parish facility manager must accompany the inspector and it is strongly recommended that the parish electrician be onsite during the inspection. This will keep the inspection time to a minimum and also allow for immediate corrective action when possible. Three or more parishes will be scheduled for inspection each day, over a 3 or 4 day period, twice per month. Inspectors are not local so schedule coordination is critical. The Diocesan Insurance Fund will cover the cost of inspections; the cost of cancellation or rescheduling will be charged to the parish.

New Jersey – New Legislation

As of April 18, 2022, employers in New Jersey must provide written notification to employees before use if tracking devices are utilized on vehicles operated by employees, regardless of whether the employee uses a company-owned vehicle or the employee's personal vehicle. A tracking device is defined as an electronic or mechanical device which is designed or intended to be used for the sole purpose of tracking the movement of a vehicle, person or device. It is not uncommon for these types of devices to be installed on school buses and transport vans, company provided cell phones, electronic notebooks and laptops.

HSB Sensor Report Jan. 1st – Mar. 31st 2022

Total Alerts	**1591**
76 building locations	
Urgent Alerts	**538**
34 building locations	
Warning Alerts	**570**
51 building locations	
Low Temperature	670 alerts
Refrigeration	402 alerts
Water	42 alerts
Power Loss	254 alerts
Other	223 alerts

Urgent – pipe freeze – water present – very low building temperature – high refrigerator/freezer temperature

Warning – low pipe temperature – refrigerator/freezer temperature rising – building temperature below 55° F with outdoor temperature below 20° F.

Knights of Columbus

Over the last several years, the Knights of Columbus implemented a Safe Environment initiative to protect children and other vulnerable persons served through their various programs. Supreme Knight Patrick Kelly has stated, "Protecting our children is the sacred duty of every Knight." The Knights of Columbus utilize the PREASEDIUM'S ARMATUS® Safe Environment Training Program. The Knights of Columbus Program is not a substitute for compliance with the Diocese of Trenton Safe Environment Training Programs or Criminal Background Check Requirements. The Knights of Columbus Office of Youth Protection has taken a cooperative approach towards diocesan safe environment programs and in guidance to council leaders has stated that the first requirement of the Knights of Columbus program is for Council Members to be compliant with diocesan safe environment requirements applicable to members' volunteer activities on parish properties.

Parish Safe Environment Coordinators should direct any questions to the Diocese of Trenton Associate Directors Office of Youth and Child Protection Bill Staub and Margaret Dziminski. ■

Roman Catholic Diocese of Trenton
Department of Administrative Services
701 Lawrenceville Road
Trenton, NJ 08638

FIRST CLASS MAIL
US POSTAGE
PAID
MAILED FROM ZIP CODE 07006
PERMIT NO. 881

2022 Summer Edition

Diocese of Trenton Risk Management Quarterly

Parishes, Schools, Cemeteries & Catholic Institutions

Inside this Issue:

Risk Management Key Contacts

Willis Towers Watson Team
Willis Towers Watson Southeast
Concourse Corp. Center 5, 18th Fl.
Atlanta, GA 30328

Jen Adams, Assistant VP
Tel: 404-302-3841
Jen.Adams@willistowerswatson.com

Mike Farrand, Sr. Principal
Tel: 610-715-1951
Mike.Farrand@willistowerswatson.com

Alex Lok, Sr. Client Specialist
Tel: 404-302-3824
Alex.Lok@willistowerswatson.com

Certificates of Insurance
For our online form, go to:
dotinsurance.org/forms/certs

Claim Reporting
PMA Management Corp.
PMA Corporate Processing Center
Tel: 800-482-9826; Fax: 856-727-3186

Auto Insurance Cards
Porter & Curtis, LLC
Tel: 484-445-7174
Email: trenton@aeti-inc.com

For our online form, go to: dotinsurance.org/forms/auto-forms

Diocese of Trenton
Chancery
701 Lawrenceville Rd.
Trenton, NJ 08638
Main Tel: 609-406-7400

Joseph Bianchi, Chief Administrative Officer
Tel: 609-403-7208
Fax: 609-406-7413
jbianc@dioceseoftrenton.org

Joseph Cahill, Director of Risk Management
Tel: 609-403-7189
Fax: 609-403-7215
jcahill@dioceseoftrenton.org

Scot Pirozzi, Director, Department of Construction and Property
Tel: 609-403-7195
Fax: 609-406-7412
spiroz@dioceseoftrenton.org

www.dotinsurance.org