Catholic Mutual. . . "CARES"

CYBER SECURITY PRACTICES

STAYING SAFE ONLINE

The widespread availability of computers and connections to the Internet provides 24 hour access to information, credit and financial services, and shopping. The Internet is also a great communication and learning tool for educators and students. People have begun in expect instant access to information from a wide variety of sources, including the Catholic Church. The Church is being asked to provide online services creating the concern for safeguarding sensitive data. A breach in the church's information security system could result in an unintentional disbursement of confidential information including parishioner's personal information, or financial or personnel records for the church.

Unfortunately, there are people who take advantage of the Internet through criminal behavior and other harmful acts. These criminals try to gain unauthorized access to your computer and use that access to steal identities, commit fraud, or even launch cyber attacks against others.

The National Cyber Security Alliance recommends adhering to the following cyber security practices. These practical steps will help your parish/school and staff stay safe online to avoid becoming victims of fraud, identity theft, or cyber crime.

❶ Protect Personal Information

Criminals are very interested in obtaining personal information. The reality is that anyone can be a victim of identity theft. According to a recent Federal Trade Commission survey, almost 10 million people are the victims of identity theft every year. The following steps should be followed while online to minimize your risk of identity theft:

- Before giving out personal information (i.e. name, address, account numbers, social security number), learn how it will be used and how it will be protected.
- Do not open unsolicited emails or those from unknown sources.
- If making a purchase online, do not provide personal or financial information unless you have checked to ensure a site is secure. Examples include a "lock" icon on the browser's status bar or a website URL beginning with "https:".
- Read and understand a website's privacy policy. This details what personal information is collected by the site, how the information is used, and if information is passed along to third parties.

❷ Know who you're dealing with

- Phishing – "Phishers" send spam or pop-up messages claiming to be from a business or organization that you might deal with on a regular basis (i.e. your financial institution, an Internet Service Provider (ISP), a governmental agency). This is the "phishers" way of tricking you into divulging personal information so they can steal your identity. Never open unsolicited email messages; don't open attachments from people you don't know or don't expect; and don't reply to or click on links in email or pop-ups that ask for personal information via email. Legitimate companies never ask for this information in this manner. Verify the request by calling the company directly; however, use a contact number on a recent statement instead of one given on the email.

- Free Software and File Sharing – File sharing entails downloading special software that connects your computer to a network of other computers running the same software. By not checking the proper settings, you run the risk of allowing access to other information on your hard drive, instead of just the files you originally intended to share. Downloading file-sharing software is not advised and could place personal information and your computer at risk.

- Spyware – Spyware is software installed without your knowledge or consent that adversely affects your ability to use your computer, sometimes by monitoring or controlling how you use it. In some cases, it can also use your computer to access or launch attacks against others. All computers should have some type of anti-spyware software installed to scan for and delete any spyware programs that may sneak onto your computer.

- Email Attachments and Links – A virus sent over email cannot damage your computer without your help. Never open an email attachment unless it's from a known source or you know what it contains. When sending emails, help others trust your attachments by including a message in your text explaining what you are attaching.

❸ Use anti-virus software, a firewall, and anti-spyware software

- Anti-virus Software – Anti-virus software protects your computer from viruses that can destroy your data, slow your computer's performance, cause a crash, or even allow spammers to send email through your account. It works by scanning your computer and your incoming email for viruses and then deleting them. Anti-virus software must be updated routinely. Most commercial anti-virus software includes a feature to automatically download updates when you are on the Internet. When deciding on a brand of software, keep in mind that good anti-virus software should recognize current viruses, as well as older ones; effectively reverse the damage; and update automatically.

- **Firewalls** – Firewalls assist to keep hackers from using your computer to send out your personal information without your permission. Basically, it acts as a guard watching for outside attempts to access your system and blocking communications from and to sources you don't permit. Many operating systems and hardware devices come with a built-in firewall. To ensure your firewall is effective, ensure it is turned on, properly set up and updated regularly.

- **Anti-Spyware Software** – Anti-spyware software helps protect your computer from malicious spyware that monitors your online activities and collects personal information while you surf the web. Since the sophistication of spyware programs is increasing, consider using two different anti-spyware programs to offer increased protection.

4 Proper set up of operating system and Web browser software

- Hackers take advantage of unsecured Web browsers (i.e. Internet Explorer) and operating system software (i.e. Windows). Lessen your risk by changing the settings in your browser or operating system and increase your online security. Built-in security features can be found in the "Tools" or "Options" menus.

- Your operating system may offer free software patches that close holes in the system that hackers could exploit. In fact, some common operating systems can be set to automatically retrieve and install patches for you. If not, make regular visits to your system's manufacturer website and update your system with defenses against the latest attacks. Your email software may assist in avoiding viruses by providing the ability to filter certain types of spam; however, you must activate the filter.

5 Passwords

- **Protect** your passwords by keeping them in a secure place and out of plain view. Never share your passwords on the Internet, by email, or by phone.

- **Strengthen** your password by making it harder for hackers to figure them out.

    - **Use passwords that have at least eight characters and include numbers and symbols.**

    - **Avoid common words**

    - **Never use your personal information or login name as password**

    - **Change your passwords regularly (at least every 90 days)**

    - **Use a different password for each online account you access**

6 Back up files

- No system is completely secure so it's important to copy important files onto a removable disc and store securely in a building other than where your computer is located. If a different location is not practical, consider encryption software. This software scrambles a message or a file in a way that can be reversed only with a specific password.
- Always keep your original software start-up disks handy and accessible for use in the event of a system crash.

7 Learn what to do if something goes wrong

- **Hacking or Computer Virus** – If your computer gets hacked or infected by a virus:
    - Immediately unplug the phone or cable line from your machine. Then scan your entire computer with fully updated anti-virus software and update your firewall.
    - Alert the proper authorities by contacting your ISP and the hacker's ISP (if you can tell what it is). Often, the ISP's email address is abuse@yourispname.com or postmaster@yourispname.com. Include information on the incident from your firewall's log file. Also, alert the FBI at www.ifccfbi.gov.
- **Internet Fraud –** All fraud related complaints should be reported to the Federal Trade Commission (FTC) at www.ftc.gov. They enter Internet, identity theft, and other fraud related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.
- **Deceptive Spam** – If you receive deceptive spam, including email phishing for your information, forward it to spam@uce.gov. Be sure to include the full Internet header of the email. For further information, go to http://getnetwise.org/action/header.
- **Divulged Personal Information** – If you believe you have mistakenly given your information to a fraudster, file a complaint at www.ftc.gov and then visit the Federal Trade Commission's Identity Theft website at www.consumer.gov/idtheft to learn how to minimize your risk of damage from a potential theft of your identity.

*****Information provided by the National Cyber Security Alliance*****

(Revised 11/2018)

Catholic Mutual…"CARES"

CYBER SECURITY TIPS

Parishes, schools and other Catholic organizations may be daunted by the perceived resources it takes to secure their computer systems; however, not making cyber security a priority could be a costly decision. The National Cyber Security Alliance recommends implementing the following key security principles to provide a starting point for a comprehensive security plan.

1. **Ensure that all employees use effective passwords.** Encourage passwords that are comprised of different characters and change them every 60 to 70 days, but no longer than 90 days. Passwords should be required to include both numbers and letters.

2. **Protect your systems.** Install and use anti-virus, anti-spyware and anti-adware programs on all computers. Ensure that your computers are protected by a firewall. A firewall can be a separate appliance, built into wireless systems, or a software firewall that comes with many commercial security suites.

3. **Keep all software up-to-date.** Ensure that all computer software is up-to-date and contains the most recent patches (i.e. operations system, anti-virus, anti-spyware, anti-adware, firewall and office automation software). Most security and operating systems contain automatic updates; make sure that function is turned on and sign up for security notifications from the software company. Without these updates, your systems will not be well protected against new cyber threats.

4. **Create backups.** Make regular (daily or weekly) back-up copies of all of your important data/information. Store a secured copy away from your office location and use encryption to protect any sensitive information about your institution and parishioners.

5. **Be prepared for emergencies.** Create a contingency plan so you can recover if you experience an emergency. Include plans to continue business operations at an alternate location when necessary. Test your plan annually. Make sure to erase all data on the hard drive before recycling or throwing away a computer.

6. **Report Internet Crime.** Locate and join an organization for information sharing purposes. If you suspect fraud or criminal intent, report it to local law enforcement agencies, the Federal Bureau of Investigation, Secret Service or the State Attorney General's Office.

(Revised 11/2018)

Catholic Mutual. . . "CARES"

DATA PROTECTION POLICY

The Church is constantly evolving and making changes to meet the technical needs and expectations of its parishioners. Dioceses, parishes, and schools are developing their own websites and offering new services online in an effort to keep up with today's society. Some of the newer online ventures being offered by Church websites are fundraising, chat rooms, newsletters, employment applications, bulletin boards, tuition/collection/donations online, etc. Oftentimes, personal information is collected by the Church electronically from individuals, including names, addresses, phone numbers, bank and/or credit card account numbers, incomes, etc. A policy should be in place to properly safeguard diocesan/parish sensitive information as well as the personal information of parishioners, students and employees. The following lists items to consider when developing a policy for data protection.

- Any individual who will have access to sensitive information should have a background check completed.
- Access to this information should be strictly limited to individuals who have a business reason to see it.
- Users should be required to utilize passwords that are at least six characters and contain a combination of letters, numbers, and symbols. Passwords should be changed frequently.
- Password-activated screen savers should be used to lock computers after a period of inactivity.
- Procedures should be in place for the appropriate use and protection of laptops, PDA's, cell phones or other mobile devices. Any sensitive information should be in encrypted files.
- Employees and volunteers must be trained to ensure security, confidentiality, and integrity of sensitive information is maintained such as:
    - Locking file cabinets or doors to rooms where records are kept
    - Not allowing passwords to be shared or posted in work areas
    - Ensuring sensitive information is encrypted when sent electronically

    - Reporting suspicious attempts to obtain sensitive information to supervisors

- Employees should be reminded on a regular basis of policy to keep information secure and confidential.
- Impose and follow through with strict disciplinary measures for policy violations
- Terminated employees or volunteers should have their passwords deactivated immediately
- Know where sensitive information is stored and keep it secure. Remember, only authorized individuals should have access.
    - Storage areas of sensitive paper files should be protected against damage from physical hazards such as fire or floods.
    - Sensitive records should be stored in room or cabinet that is locked when unattended.
    - For sensitive information stored on a server or other computer, it should be password protected by a "strong" password.
    - An inventory should be maintained of all computers and other equipment on which sensitive information may be stored.
    - When transmitting credit card information or other sensitive data, use a Secure Sockets Layer (SSL) or other secure connection to ensure information is protected in transit.
    - When collecting sensitive information online directly from parishioners, make secure transmission automatic.
    - If confidential information must be transmitted by email, the data must be encrypted.
- Ensure disposal of sensitive information is done in a secure manner. All paper records should be shredded in a manner that it cannot be read or reconstructed. Data must be erased when disposing of computers, disks, CD's, hard drives, laptops, cell phones or any other electronic devices containing sensitive information.

(Revised 11/2018)

Catholic Mutual… "CARES"

Electronic Signatures (e-signatures)

As technology continues to evolve and develop into our everyday lives, electronic signatures are becoming more prominent. An electronic signature or e-signature is defined as a symbol, sound, or something else in electronic form used by a signatory (signer) to represent his or her signature. If legal and/or regulated in your State, e-signatures have benefits of increased efficiency and enhanced security.

For e-signatures to be valid and legally binding, they must adhere to certain standards. In the United States, e-signatures are both legalized and regulated under two separate laws, the United States Electronic Signatures in Global and National Commerce (ESIGN) Act and the Uniform Electronic Transactions Act (UETA) which makes e-signatures valid and uniform across state lines. UETA has been passed in all 47 states, plus Washington, D.C. and the U.S. Virgin Islands. New York, Illinois and Washington have their own laws regulating e-signatures.

For an e-signature to be legitimate, it must possess the following attributes:

1. The signer must be aware of their actions and intent to sign.
2. The signer must have given consent indicating they agreed to allow the transaction to take place electronically.
3. The electronic software that captured the signature must keep a record of the process used to obtain the signature.
4. The documents that were signed electronically must be retainable for recordkeeping purposes and reproducible so all parties have a copy.

When contemplating using e-signatures, you should ensure the four criteria listed above are met.

Should you have any additional questions, please feel free to contact your Risk Management Representative at Catholic Mutual Group.

(Revised 2/2019)

Catholic Mutual. . . "CARES"

Network Security Policy and Usage

OVERVIEW

Internet access to global electronic information resources on the World Wide Web is provided to clergy, religious, employees, volunteers and students to provide ease in obtaining data and technology to assist in their respective ministries, duties or studies.

Our technology systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and File Transfer Protocol (FTP), are the property of the diocese/parish/school, and are to be used in support of the mission of the Catholic Church. Maintaining a safe, reliable, and secure system is a collaborative effort involving the participation and support of every individual who uses our information systems. It is the responsibility of every computer user to know and conform to these guidelines.

PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment. These rules are in place to protect both the members of our community and the diocese/parish/school. Inappropriate use exposes the diocese/parish/school to risks including virus attacks, compromise of network systems and services, and legal issues.

SCOPE

This policy applies to anyone using the diocese/parish/school technology system, including parishioners, students, employees, contractors, consultants, temporaries, volunteers, and other workers, as well as all personnel affiliated with third parties. This policy has specific provisions for students. The provisions which apply to students, likewise apply to minors who take part in ministries for children and young adults. For clarifications on how this policy applies to minors, the school principal, pastor, or the religious education director is the primary point of contact.

GENERAL USE AND OWNERSHIP

While the network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on parish systems remains the property of the diocese/parish/school. Because of the need to protect our network, management cannot

guarantee the confidentiality of information stored on any network device and no rights of privacy exist.

All users are responsible for exercising good judgment regarding the reasonableness of personal use. Commercial use is prohibited. If there is any uncertainty, users should consult the administrator responsible for technology management, the School Principal, or the Pastor.

The equipment, services and technology provided to access the web are the property of the diocese/parish/school. For security and network maintenance purposes, administrators may monitor equipment, systems and network traffic at any time. We reserve the right to audit networks and systems, monitor internet traffic, retrieve and read any data composed, sent, or received on a periodic basis to ensure compliance with this policy.

We rely upon the active cooperation of parents and the responsibility and integrity of students to maintain safe and secure facilities for approved uses of our technology in our school. All users of our computer facilities are asked to live up to that same standard.

UNACCEPTABLE USE

The Diocese/Parish has taken the necessary actions to assure the safety and security of our network. Any individual who attempts to disable, defeat or circumvent security measures is subject to disciplinary action up to and including dismissal. The following are examples of actions and activities that are prohibited:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the diocese/parish/school, or use of classified government information.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, copyrighted video, and the installation of any copyrighted software for which the diocese/parish/school or the end user does not have a valid, active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws is illegal and prohibited.
4. Knowingly or negligently introducing viruses, Trojans, worms, or other commands, scripts or programs intended to damage, disable, or degrade computer systems or network resources or to make unauthorized access of networks or systems.
5. Using or attempting to use administrative accounts or other network accounts without authorization.

6. Defeating or attempting to defeat content filtering systems.
7. Stealing, using or disclosing another user's password or code without authorization.
8. Using any network systems to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws, Canon Law, or Diocesan rules and policies. This includes morally objectionable materials, files, images, text or other content.
9. Security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning, intrusion detection or other security scanning is expressly prohibited by anyone other than systems administrators charged with responsibility for system security.
11. Executing any form of network monitoring which will intercept data not intended for the employee's system, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, system, network or account, or disguising or attempting to disguise the identity of a host, system, account, or service on the network.
13. Interfering with or denying service to any other user (for example, denial of service attack.)
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, by any means, locally or via the network.
15. Providing information about, or lists of, staff, students, or parishioners to parties outside the diocese/parish/school.
16. Use of wireless access to network resources without prior written permission of the technology administrators, principal or pastor.
17. Use of resources which are wasteful or which monopolize system resources at the expense of other users.
18. Use of peer-to-peer file sharing software to access, share or trade any files.
19. Using internet for participation in Chat rooms or other web-based forums unrelated to ministry, duties or studies.
20. Engaging in any other illegal activities.

DISCRETION

Those who minister and work in pastoral settings must take great care to be consistent in representing the worth of their character online. Clear communication and respect for boundaries is needed at any level of contact. Emails, text messages, blog postings or

comments, and YouTube videos are all public forums from which a permanent record can be obtained. As a representative of the Church, users should be diligent in avoiding situations which might be the source of scandal for themselves or others. Furthermore, those to whom we minister must be educated on the public nature of such communication. Confidential information should never be sent via email.

EMAIL, INSTANT MESSAGING, AND VIDEO CHATTING

Email and instant messaging (IM) allows for increased flexibility and immediacy in communication. When appropriately combined with face-to-face communication, email and IM can significantly enhance how we minister to others. The same boundary issues that must be respected in oral communication must be respected in written ones. Good judgment should always be used with text based communication tools. Parental/guardian consent needs to be obtained when communicating by email or instant messaging with young people.

- Maintain a separate email account for your professional communication and only use this account when communicating with youth.
- Email, IM, and Video Chatting communication should only be used with matters that deal with an individual's professional relationship. Communicate only about matters that address the business-at-hand of your ministry.
- Care should be taken to maintain professionalism and appropriate boundaries in all communication.
- There should be absolutely no personal exchanges.
- Electronic communication can be easily misinterpreted. Communicate in person whenever possible. Before sending an email, ask yourself if someone might "read something into it" that you didn't intend. If you think your email might somehow be misunderstood, don't send it.
- If there is any potential for embarrassment or harm, reconsider sending the email or IM.
- Be cautious when sending an email, especially either in haste and/or when emotions are involved.

Always avoid any communication that might be construed as having inappropriate sexual or romantic overtones. Do not reply to any such email from a minor. Instead, make a copy of such inappropriate communication and notify your supervisor. Remember, there is no such thing as a private email. All emails and IM's can be logged, archived, and forwarded to other parties. Your communication can quickly become a public matter.

- Unlike verbal communication, any form of written communication has a form of permanence.
- There should be no expectation of privacy.
- At no time is one-on-one video chatting appropriate with young people.

MINISTRY WEB PAGES

Anyone who establishes a ministry web presence should make a commitment to this vehicle of communication. Web pages, especially the index or main page(s), should be regularly updated. As with any ministry effort, there should be an intentional plan and set of goals regarding establishing and maintaining a web presence. Great care should be used to protect people on a web page that is publicly accessible.

- Personal information should never be made available (i.e. home address, home or cell number, home email address, etc.).
- Written authorization must be obtained from parent/guardian before posting photos or videos of young people.
- Pictures or videos should not be captioned with a young person's name unless the parent/guardian has given you written authorization to do so.
- Never use a picture or video that might be considered embarrassing or unflattering.
- Care should be taken to protect the reputation of our church membership. If individuals are uncomfortable with a particular photo or video, it should be immediately removed from the website.

SOCIAL NETWORKING

A social network service utilizes software to build online social networks for communities of people who share interests and activities. Most services are primarily web-based and provide various ways for users to interact, such as chat, messaging, email, video or voice chat, file sharing, blogging, discussion groups, etc.

Social networking has become a part of everyday life, as a variety of social networking tools are being used by millions of people on a regular basis. The most popular sites include www.facebook.com, www.myspace.com, and www.twitter.com. Social networking has revolutionized the way we communicate and share information with one another. Therefore, it can be a way to connect people with the church and the church's activities with people.

On any social network site, personal opinions and discussions are often conducted. It is essential for users to remember that even on the World Wide Web, others may recognize them as representing the values of the Catholic Church.

- If a professional staff minister wants to use social networking sites for ministry purposes, a professional social networking account should be created that is separate from their personal account. This account should be seen as an official extension of the ministry organization's web presence, administrated by an adult, and approved by the pastor or supervisor in which the social networking site will be

used. Volunteers should not set up a special ministry site without the permission of the professional staff minister and/or the pastor.
- There is a difference between initiating a 'friend request' and accepting one. Pastoral ministers must not initiate and 'seek' friends on the professional social networking account. Outside individuals must request you as a friend first.
- Using the Internet for accessing information about the people to whom we minister is a violation of their privacy, even if that information is publicly accessible.

SOCIAL NETWORKING WITH MINORS

Anyone who ministers and works in pastoral settings with young people with a "personal" social networking site should never advertise that site nor 'friend' a young person to their "personal" site. If you become aware of information that is in the public domain of such a site, you are responsible for information that must be reported if a minor has been abused or is under threat of harm.

"Best Practices"

Ideally, the professional minister, with permission from the pastor/supervisor, should create an online group on social networking sites that both young people and adults can join and interact without full access to one another's profile.

BLOGGING

One method to develop and disseminate content is through a blog. The word "blog" is short for 'Web log' or 'Web-based log.' Those who minister and work in pastoral settings may only establish and publish through ministry-based blogs with the prior approval of their pastor or supervisor. As a representative of the Church, blogging should be conducted in a professional manner for ministry purposes only. As with any professional communication, ministry blogs should not be used:

- For any personal communication or agenda.
- To conduct or promote outside business activities.
- To defame or cause defamation of the character of any individual, organization or institution.
- To divulge any personal information about an individual or jeopardize their safety in any other way.

"Best Practices"

Ministry based blogs can publish information including, but not limited to:

- Fliers for upcoming activities, permission forms, calendar, and ministerial updates
- Additional links and references for faith formation

- Sacramental preparation information including: class times, checklists, sponsor resources, parent resources, etc.
- Descriptions of projects, including procedures, expectations, and suggested parent involvement
- Bible Studies and other spiritual links and prayer resources
- Achievements of parishioners

BLOG DISCIPLINE (needs to support the student handbook)

The question that will come up frequently is "Can students with an "anti-school" message be disciplined?" The following is a recommendation that can be modified based on your student handbook.

- If the student handbook is worded so students are on notice that behavior will subject them to discipline, they can be disciplined.
- The handbook should be worded to apply to out-of-school conduct that violates school rules.
- The handbook should be worded to address behavior regardless of whether it is verbal, physical, written, graphic or electronic.
- Distinguish violation of school rules from anti-school messages.

ONLINE GAMING

Those who minister and work in pastoral settings with young people should take care in their involvement with online gaming. While this may be a recreational alternative, for many it is also an opportunity for social networking. Pastoral ministers should take care of protecting their online game identities so that appropriate boundaries are maintained.

DEFINITIONS

1. Computer Use — Shall mean and include the use of school computers and networks and other technology resources including, without limitation, computers and related technology equipment or networks, all forms of email or electronic communication, websites and the Internet including onsite or by dial-up or remote access thereto through school accounts, as well as any use which involves visual depictions, audio, video or text, in any form.

2. Computer User — Shall mean and include any parishioners, students, employees, contractors, consultants, temporaries, volunteers, and other individuals who engage in Computer Use as defined herein.
3. Access to the Internet — A computer shall be considered to have access to the Internet

if such computer is equipped with a modem or is connected to a computer network which has access to the Internet, or which accesses the Internet by dial-up or remote access using an Internet account.

4. **Minor** — Shall mean an individual who has not attained the age of 18.

5. **Obscene** — Shall have the meaning given such term in Section 1460 of Title 18, United States Code.

6. **Child Pornography** — Shall have the meaning given such term in Section 2256 of Title 18, United States Code.

7. **Hacking** — Shall mean Computer Use or using the Internet to attempt to gain unauthorized access to proprietary computer systems.

8. **Technology Protection Measure** — Shall mean and refer to a proxy server that blocks and/or filters Internet access.

9. **Adult** — Shall mean and refer to individual age 18 or older.

(Revised 11/2018)

PHOTOGRAPH AND VIDEO CONSENT FORM:

From time to time, pictures and video may be taken of youth ministry events and gatherings. We would like to be able to use these photographs and videos for flyers, parish and diocesan publications, and the ministry website. Written consent of both the student and parent/guardian is required. Names will not be posted unless written authorization is given by the student and parent/guardian, and then only first names will be used. If there are concerns about pictures or videos posted on the website, please contact the ministry coordinator or webmaster, and they will promptly be removed.

I/We, the parent(s)/guardian(s) of this youth (name) _____, authorize and give full consent, without limitation or reservation, to (parish/school) _____, to publish any photograph or video in which the above named student appears while participating in any program associated with (parish/school)_____ ministry. There will be no compensation for use of any photograph or video at the time of publication or in the future.

Student Signature: _____ Date: _____

Parent/Guardian Signature: _____ Date: _____

Parent/Guardian Signature: _____ Date: _____

Catholic Mutual. . . "CARES"

PROTECTING YOUR NETWORK FROM INTERNET/EMAIL RISKS

Loss of valuable, confidential data, downtime and damaged systems are not pleasant issues to deal with. They can cost your organization a significant amount of money, not to mention the time involved to resolve the problems. Properly securing your computer from the numerous threats posed by viruses, spyware and hackers is just as important as being aware of the Internet's dangers. A brief investment of time and effort is all that it takes to make sure that your computer remains free of malicious software and is off limits to hackers. Implementation of the following measures will go a long way to protect your local area network (LAN). All organizations should have an IT individual or staff that would be responsible for overseeing these safety measures:

- Limit floppy drive access, USB ports and serial ports on networked computers. These are the most common entry points for problems and most users do not need access to these drives. They can email or store data elsewhere in a safe "scanned" environment.
- Do not allow any users to modify any system files. All network users should be locked down so they can only perform tasks which administration has agreed upon.
- Block Instant Messenger. These send messages and attachments out to a server and then back to its clients. By disabling its functionality, viruses and other computer risks can be controlled from spreading.
- A current subscription of antivirus software should be run on all your computers. Some examples include Norton Antivirus and McAfee Virus Scan.
- Install a firewall which helps prevent unauthorized sources from entering or leaving your computer, making you invisible on the Internet. A firewall should always be used if you have a broadband connection (DSL or cable). Some examples include Zone Alarm Pro 2007 & private firewall.
- Install anti-spyware software on each computer. Spyware software monitors or controls your computer use and is used to send you pop-up ads, redirect your computer websites, monitor your Internet surfing, or record your keystrokes. Some examples include Spybot Search & Destroy or Spyware Doctor.
- Never open attachments to an email unless you trust the sender as this is often what triggers a virus to enter your computer.

- Install filters to prevent users from accessing forbidden sites. Consider using a mechanism which allows you to monitor or track an individual users' behavior on the web.
- Install a port monitor to prevent your ports from being scanned. Hackers regularly try to find and exploit weaknesses in operating systems and web browsers.
- Require passwords to be changed frequently and the password must not be the same as any of the previous six passwords. Passwords should contain both letters and numbers or symbols.
- Require the combination of key strokes CTRL+ALT+DEL to logon. This provides an additional security layer requiring the user to physically be at the computer to log on.
- Use password-activated screen savers to lock computers after a period of inactivity.
- Continuously update your operating system and web browsers. Most can be set to check for updates automatically.
- Maintain backups of your software applications and files at a secured, off-site facility. Use encryption to protect any sensitive information.
- Enact an Email and Internet Policy. All users should be given a hard copy to read and required to sign and date they have read and understand the policy.
- Develop and implement a Security Plan and train users properly to ensure confidential information is kept secure.
- Avoid putting photos of individuals on your website, especially minors, unless photos are located under an area that is password protected.
- Ensure your IT individuals are up-to-date on the latest technology.

(Revised 02/2021)

CYBER INCIDENT REPORTING

IMPORTANT: The first few minutes and hours after learning of a cyber incident are critical to a successful recovery. The following is intended to help you and your organization know how to identify and report a suspected or actual cyber security breach.

Immediately notify your IT Resource Personnel.

During business hours, contact Jeff Schneider, Director of Claims for CMG:

402-514-2404 (Office) 402-490-0021 (Cell)

After hours contact our cyber insurance experts at Tokio Marine HCC:

1-888-627-8995 or cpl.claims@tmhcc.com – Identify yourself as a Catholic Mutual Member

Additionally, the following steps can help to mitigate possible issues:

Cyber Event	Immediate Mitigation Steps
Ransomware infection	• Isolate infected computer from all networks (by unplugging network cable and/or turning off Wi-Fi) • Take picture of the ransomware message on screen (if possible) • Contact your IT department • Do not immediately rebuild your system (you might destroy important forensic evidence) • Contact CMG Claims
Phishing email attack	• Do not click on link or open any attachment from suspicious email • Call IT representative and forward email to IT for evaluation • Take picture/screen shot of email request/solicitation • Change your email password (strong and unique passphrase) • Contact CMG Claims
Malware infection	• Notify IT to have them evaluate and remove malware • Scan network for any other unauthorized files and user accounts • Install anti-virus software and keep updated • Contact CMG Claims
Discovery of unauthorized files or	• Close Remote Desktop Protocol (RDP) ports • Change passwords (strong and unique passphrase)

user accounts on server or client	• Contact CMG Claims
Lost or stolen device	• Report lost/stolen device to IT immediately • Secure all devices and removable media (passwords and encryption)
Mistaken wire transfer	• Call bank and report details • Attempt to halt transfer • Take picture/screen shot of email request of fund transfer • Contact CMG Claims

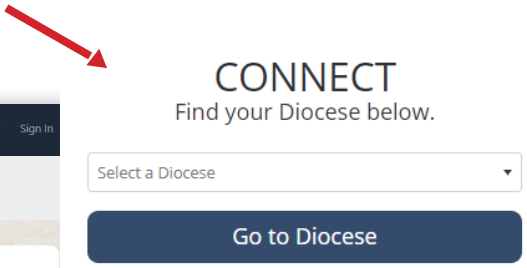
Revised 07/2020

CMGConnect

End-User Instructions

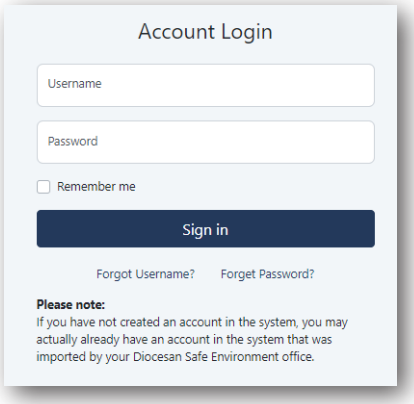
Step 1: Accessing CMG Connect

Go to **www.CMGconnect.org/** to select your organization from the dropdown box then click **GO**. This will bring you to your organization's landing page (*sample below*).



Please select the category(s) that best describe how you participate at your location. This allows the platform to automatically assign the correct training(s).

If you are unsure, contact your Safe Environment Coordinator.



If you have done training in the past, you may already have an account. Please login with your previous username and password by clicking the "Sign In" button at the top right of the page.

If you cannot remember your username and password and have an email address in the system, please click 'Forgot Password'. Please contact cmgconnect@catholicmutual.org or click Support if you need assistance accessing your account.

For more information, please use your FAQ or Support tab at the top of the screen.

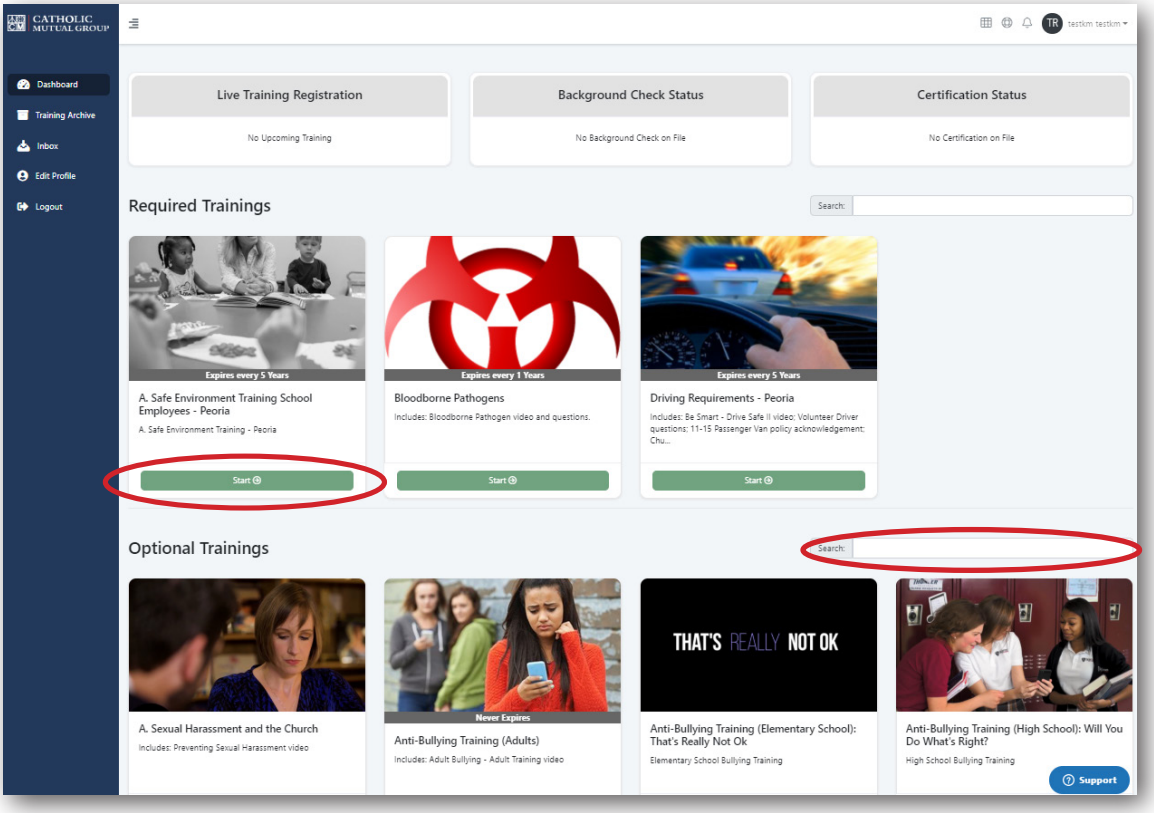
Updated: 01/16/2020

CATHOLIC MUTUAL GROUP

Step 2: Locate and Open Trainings

Once you have completed the registration process, you will see the training curriculums. Click **"Start"** to begin. ***Note: Available curriculums will vary based on your organization customization as well as the participation category you selected when registering for your account.***

To view other Optional Trainings, scroll to the bottom of the page and search for desired trianing.



Step 3 (Optional): Print Certificate

When you have reached the end of the training, click on your dashboard and find your completed training. Click **"Print Certificate"** to view and download your completion certificate.