PSParish Support Pack

DATA PROTECTION

CONTENTS

1. Keeping Secrets - Confidential information

Discover why your church must be careful with the confidential information it controls.

Some documents and records that churches maintain are private.
Examples of confidential information include:

- Members' contributions records.
- Counseling notes taken by a clergy person or church counsellor.
- References you obtain when screening youth workers.
- Minutes of vestry meetings at which sensitive issues are discussed.

A church faces possible legal liability if it permits disclosure of any of these kinds of confidential records. As a result, it is important for select vestry members to take steps to insure that confidential information is not leaked or inadvertently disclosed. There are a number of ways this can be done, and to a great degree it is simply a matter of recognising the problem and using common sense.

Precautions for keeping confidential information:

1. Keep confidential information in a locked, fireproof file, and give the keys to a designated person such as the Hon Treasurer or Rector, depending on the nature of the records involved.

2. Confidential information is often stored as files on church computers, and steps must be taken to restrict access to this data by unauthorised persons.

3. Confidential information should not be disclosed to persons without a legitimate need to know. For example, if the select vestry dismisses a staff member due to a confession of misconduct, the Rector and vestry must recognize that public disclosure of this information can result in legal liability.

4. The select vestry should consider adopting a covenant of confidentiality each year. This means that vestry members sign a covenant agreeing not to disclose any confidential information shared during vestry meetings without the unanimous consent of the vestry. This kind of covenant serves a few important purposes. First, it helps to impress upon the vestry the highly confidential nature of some information, and second, it reduces the legal risk to the parish in the event that a vestry member violates the covenant and leaks confidential information. Of course, it will not work unless everyone consents, so if one or more vestry members refuse to sign, they must be excused from any discussion of confidential information.

5. Clergy often maintain counseling notes or other highly confidential records, and steps must be taken to insure the proper disposition of this information in the event of the sudden death or incapacity of the cleric.

2. Simple Tips for Protecting Church Data

Keep your church records and data safe with the right precautions and software.

Computers are absolutely vital to help keep a church running, but they are also vulnerable. Keep your church records and data safe with the right precautions and software.

Strategic Plans

- **One database is enough.** If you're using multiple databases to store information, the more you'll need to protect. Try to consolidate your data so you can better secure it.

- **Guessable passwords**. Are your passwords guessable? Avoid using words, names, or numbers that could be easily guessed by an outsider. Also, never share passwords with your coworkers.

- **Perform regular backups.** Backing up your computers daily, even hourly will save you time in the future if there's a power surge. Taking your vital records and data to an off-site location also gives you a safety if a natural disaster occurs.

Software Prevention

- **Suspicious activity.** Has your Internet service been acting strangely? If new homepages, toolbars, or unwanted ads are continually appearing on your browser, update your security software immediately.

- **Don't be fooled.** Adware and spyware are softwares whch want to trick you into installing their software onto your computer. Never agree to install software before you know what it is.

- **Update security patches.** Continually update security patches on your Windows, Internet server, and email. Sometimes these programs provide safety features to keep malicious software off of your computer.

- **The antivirus.** If your parish does not already own antivirus software, purchase it. If you own an older version of this software, you may need to update it since older versions do not protect against adware and spyware.

3. Protecting your church’s IT from disaster

Sound policies and purchases can keep churches going, even in dire situations.

We are dependent on our computers today in ways we might never have imagined. We rely on them to store contact information, process financial transactions, communicate—many of the nuts and bolts that enable and hold ministry together. Therefore we should do all that is reasonable and cost-effective to protect our organizations from being shut down by a disastrous event - natural or otherwise.

Planning now gives the flexibility needed for ministry survival.

And in the ever-changing legal and financial regulatory landscapes, IT disaster recovery plans are even more necessary.

These areas are wise to address:

* Management oversight.

Who is responsible for your church's IT decisions? Chances are good you're relying on a talented staff member, volunteer, or vendor—and that's okay!

The overall IT strategy of a parish should reflect the direction ministry in that parish is taking and the ordaied leadership may not have the expertise to make technical recommendations. But they have perspective of the ministry's direction, and hopefully, a sense of whether a recommendation is a good fit for the organization by way of integrity and stewardship.

* System security.

This is an area of great importance and it must be addressed. Tackle such issues as:

o Firewalls for systems that have full-time Internet connections;

o Server room security;

o And, additional policies to keep out those who should not be on the system.

The most common mistake made in this area is the password policy. The corporate standard in the U.S. is to have cryptic passwords of a significant length that cannot be easily cracked. But that strategy doesn't work well in church and ministry offices.

Those kinds of passwords are so hard to remember that most church and ministry system users write them down on a note kept under their keyboard, in their desk calendar, and so on. The better policy: Require passwords to be at least 6 digits, include at least one (but not all) number, at least one (but not all) punctuation, and at least one (but not all) capital letter, and use an acronym of a favorite verse, hymn or worship song. These are easily remembered, cryptic enough to not be easily hacked by an Internet program, and offer the added benefit of reminding folks of the reason they're logging in to your system. This strategy, coupled with using the network's Invalid Login Attempts function (set it to lock a user account for thirty minutes after three unsuccessful login attempts), is good and effective protection.

It is good practice not to permit users to change their passwords because most will not choose strong enough passwords, making the system vulnerable. So don't set passwords to expire; instead, change them for users if they've shared theirs with someone. The policy should state that staff members are not to share their password, but that if they do, they should inform their supervisor and have the network administrator set a new one.

* Record retention.

Another important area with legal ramifications involves record and data retention. Lawyers who specialize in the IT field say there isn't a simple remedy to this policy requirement. Based on their comments, though, retention policies should address two areas:

1. E-mail. E-mail should be archived for two years . This would satisfy most legal challenges and the most important factor is that you have a policy in place that you adhere to.

2. Files that may be necessary in pending litigation. Any files that might be subpoenaed in litigation must be archived in their original format and held indefinitely. That includes personnel-related files, church governance files (including minutes), negotiations, and so on.

Disasters Come in All Sizes

Churches could experience most any kind of disaster, and should one occur, it is good management and foresight— and the grace of God—that save the day. Each of the following disasters may affect a church's IT strategy:

* Fire
* Burglary or theft
* Storm damage
* Water damage from pipes
* Data theft
* Equipment failure

Reasonable protection against these disasters does not require a massivebudget! Some disasters can only be minimized by investments in hardware (like a backup system), but others can be minimized by simply having good policies in place.

Keeping Things Running

Having a solid backup strategy is essential, but it is not enough. Though backups address disaster recovery, they don't address business continuity. Business continuity policies speak to how the church will survive a larger disaster, such as a fire, or flood —and keep running. How will the ministry survive if one of its most important and valuable assets—its data—is no longer available?

• Backup Strategy

Whenever possible, it's best to back up the entire system often, using one of the following strategies:

Nightly tape backup.

Tape backups have improved their speed and capacity, keeping pace with the requirements of most churches and ministries. It's best to back up the entire system every weeknight, and take one backup tape off-site each week. Depending on your organisation's operations, choose the backup tape from your heaviest processing day each week to take off-site. For instance, most churches do most of their data processing on Monday because they're modifying the database with new members, address changes, and contributions. In those settings, it's best to take Monday night's tape off-site. That means asking a trusted member of management to put the backup tape in their backpack or handbag every Tuesday and bring back the previous week's tape. This inexpensive step can be very helpful for recovering data in case of a burglary or other disaster; and, doing this weekly means the church never has to rebuild a system with data that is more than a week old.

Hard drives and Online storage.

There's a lot of discussion among IT professionals about getting beyond tape technology. Some alternative choices are external hard drives and online storage. Recent research into corporate best practices in this area, found the majority still prefer tape because of its lower overall cost and its reliability. Very few have changed to alternative media options.

• Other Important Considerations

Whether yours is a small or large organisation, there are a couple of strategic issues that will make your disaster recovery or survival through a disaster more likely:

* Data location.

There are two possibilities regarding the location of your organization's data: local drives or server drives. Server drives don't fail as often because they are engineered for higher performance and reliability. We recommend configuring your system workstations to focus their data storage on the server drives, which will help achieve a more predictable outcome when trying to survive a disaster. It will also help your team because it will mean that a system user can log in at any workstation and get to their data if their workstation is unavailable due to theft, hardware failure, or something else.

* Avoid quick and cheap fixes.

Quick and cheap fixes have many more shortcomings, and they make achieving a full and timely recovery from disaster less likely. In addition to not being able to include necessary system files and being less reliable (something usually not discovered until they are really needed), trying to recover through them often costs significantly more.

A great rule of thumb when thinking of network technology is that if the hardware you want (desktop computer, notebook computer, switch, backup solution, and so on) is readily available in stores, it's most likely the wrong option and you don't want it. Instead, establish a relationship with an IT firm you trust and consult with the people there. Doing so will save you both time and money. You will even find that the right solutions often don't cost more than poor solutions, and sometimes even cost less.

Business Continuity

Recovering from a disaster is essential, but some disasters in recent history have emphasized the need to be able to survive and minister during the disaster and during the disaster recovery. Though the difference between disaster recovery and business continuity is subtle, it is important.

There are certain types of data your team will need to access during a disaster and during the recovery, and the bigger the disaster, the longer it may take to recover.

Step 1. Categorize the types of data in your organisation. Some categories might be congregational databases, financial systems, e-mail, letters, various ministry and department files, pictures, videos, audio files, older files, and so on.

Step 2. Meet with your leadership and ask them to prioritise what categories of data need to be recovered, and within what timeframe they need those categories available to the team. Let them know that the decisions they make will drive the strategy and expense of your disaster recovery and business continuity plan.

Step 3. Research IT best practices to meet the requirements of your leadership's decision, and present a budget and plan. If they require you to make modifications, do so explaining the consequences to their original requirements. When the budget and plan are finally approved, and they state the recoverable timelines they should deliver, have leadership formally approve it.

Step 4. Implement the new plan.

Step 5. Test the new plan. This is the piece that is often not done, but it is essential to ensure compliance with the requirements of leadership. Be sure to report the results of the test to leadership and get their approval.

By doing all five steps detailed above, you will have assurance that you have balanced the needs of the organization with the available funds to do what is best. Further, in the case of a disaster, leadership will have clear expectations of how the systems will come back online, which will help relieve stress. And best of all, it will help you and your leadership to hear the words we all hope for at the end of the journey: "Well done, good and faithful manager."

4. Advice from the UK information Commissioner's Office

http://www.ico.gov.uk/

Data protection – looking after the information you hold

If you hold and process information about your clients, employees or suppliers, you are legally obliged to protect that information. Under the Data Protection Act, you must:

- only collect information that you need for a specific purpose;
- keep it secure;
- ensure it is relevant and up to date;
- only hold as much as you need, and only for as long as you need it; and
- allow the subject of the information to see it on request.

Good information handling makes good business sense, and provides a range of benefits. You'll enhance your organisation's reputation, increase customer and employee confidence, and by ensuring that the information is accurate, save both time and money.

List of the data protection principles

Schedule 1 to the Data Protection Act lists the data protection principles in the following terms:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of

protection for the rights and freedoms of data subjects in relation to the processing of personal data.

http://www.ico.gov.uk/for_organisations/data_protection/the_guide/the_principles.aspx

How to respond to a subject access request

You need to reply to a request for personal information unless an exemption applies.

One of the main rights which the Data Protection Act gives to individuals is the right of access to their personal information. An individual can send you a subject access request requiring you to tell them about the personal information you hold about them, and to provide them with a copy of that information. In most cases you must respond to a valid subject access request within 40 calendar days of receiving it. For more details about how to respond to a subject access request please read our guide on the right of subject access.
http://www.ico.gov.uk/for_organisations/data_protection/subject_access_requests.aspx

The principles of the Data Protection Act in detail

This Guide explains the purpose and effect of each principle, and gives practical examples to illustrate how the principles apply in practice. We hope that, by answering many frequently asked questions about data protection, the Guide will prove a useful source of practical advice to those who have day-to-day responsibility for data protection.

http://www.ico.gov.uk/for_organisations/data_protection/the_guide.aspx

Are We Keeping Confidentiality?

Use the following assessment to gauge how your church is doing at securing confidential information.

1
Do we currently have procedures in place to keep financial and personal records private?
Yes/No

2
Are offerings and other financial documents always stored in a secure or well-supervised area?
Yes/No

3
Do we have all personal information behind safe doors or secured with password protection?
Yes/No

4
Do we strictly limit who has access to the safe, or the passwords?
Yes/No

5
Are old financial records with personal information (credit card numbers, Social Security Numbers, and so on) being shredded regularly?
Yes/No

6
Do we change the safe combination or password when someone is no longer authorized to use it?
Yes/No

7
Do we currently have a confidentiality policy on shared verbal information?
Yes/No

8
Are old voice messages erased from the answering machines to prevent eavesdropping?
Yes/No

9
Is there limited access to the church office?
Yes/No

10
Are there limits to what the church staff can access in the church office? (This includes administrator, Hon Treasurer, Hon Secretary, youth leader,curate, and so on.)
Yes/No