safeministry
PROTECTION AND CARE FOR EVERYONE

Storage & Retention of Safe Ministry Records

This paper is designed to assist parishes in planning and implementing a comprehensive process to properly store Safe Ministry Records securely for the long term.

Background:

For many years now, our churches have been required to keep comprehensive records of people who work with children in our church.
Those records consist of a person's name and contact information, their WWCC number, DOB, verification information relating to the WWCC, their Safe Ministry Training and leadership role information.
This can be thought of as *Core Safe Ministry data* and is detailed in the Safe Ministry Blueprint for Safe Ministry Representatives document.
In addition to that core data, churches also collect varying quantities of physical documents – things like (but not limited to):

- Copies of Safe Ministry Training Certificates
- Documents relating to disclosure of abuse
- Risk of harm reports
- SMR reports to Parish Council
- Permission slips and enduring permission documents
- Attendance data (sign in/sign out records) for children's and youth ministry groups
- Safe Ministry Plans

What has been uncertain up to now is *how long* all this information should be kept for.
It is now clear that we need to be keeping this data **indefinitely**.

This is largely due to the NSW government changing the laws in 2018 surrounding child sexual abuse claims, to remove any time limit for these complaints to be made. In addition, institutions in NSW now bear an onus in civil litigation to prove they took reasonable steps to prevent child sexual abuse.

The implication for our record keeping is significant.
It means that **ALL** of our safe ministry related records need to be kept indefinitely, meaning increasing quantities of historic data that needs to be stored in logical manner to allow possible retrieval many years later.

Storage & Retention of Safe Ministry Records

To be clear, this means that for each person who works with children in our churches, we need to keep details of *every* WWCC verification, *every* Safe Ministry Training course they do, *every* leadership role they hold, and so on. Nothing is to be overwritten, deleted or thrown out.
When people leave your church or die, their record must not be deleted – ever. They can be 'archived' but never deleted.

Key Points:

- It is vital to have a well thought out plan for your church for storage and retention of Safe Ministry information.
- Ensuring that all leaders in children's ministries are aware of the need to keep required data.
- Managing an ever-increasing quantity of data and documents will mean digital storage in preference to paper documents.
- Digital storage (and backups of that data) will likely mean *cloud-based* storage/backup.
- It is very important to choose secure, private cloud storage services.
- If required, seek skilled IT advice and assistance in implementing your storage and retention plan.

Recommended approaches for storing this data

Core Safe Ministry data

Your church is probably already storing this data electronically, eg: as part of your church Elvanto, CCB, Fuse or SaMRO account, or a similar online database system.
If your church is still using a spreadsheet for this data, now is the time to stop doing that and move to better system. Spreadsheets are an insecure and inefficient way to store this information and will become increasingly impractical as the amount of historical data mounts.
If your church has no other system, please prepare your core SM data to move to SaMRO (see: https://safeministry.org.au/samro). This is a no-cost system offered to all Sydney Anglican Parishes by the PSU.

As this data is 'live' information (ie: it is being modified and added to constantly), a secure and private online tool such as those mentioned above are the best options. As mentioned, no part of core Safe Ministry data can ever be deleted.

Other Safe Ministry-related documents.

For your additional, *paper* Safe Ministry-related documents, the requirement for indefinite storage means that keeping physical documents is simply not practical – nor is it the wisest approach from a security and privacy perspective.
Likewise, existing *digital* Safe Ministry-related documents will require careful planning to store them for the long term.

The key considerations when planning to store this information are ***security and privacy***.

Many Safe Ministry documents are highly sensitive in nature and therefore the *security* of their storage is vital along with the *privacy* of that information.
That means being as sure as you can of the integrity of the storage medium (ie: *where* it is stored), plus having a carefully thought out policy to restrict access to that information to only people with a genuine need to know.

Examples of inappropriate *long-term* digital storage locations:

- The average church office PC with poor security provisions.
- The minister's laptop (with poor security provisions)
- External hard disk drives
- USB flash drives

How to approach long term storage of documents

A suggested approach looks like this:

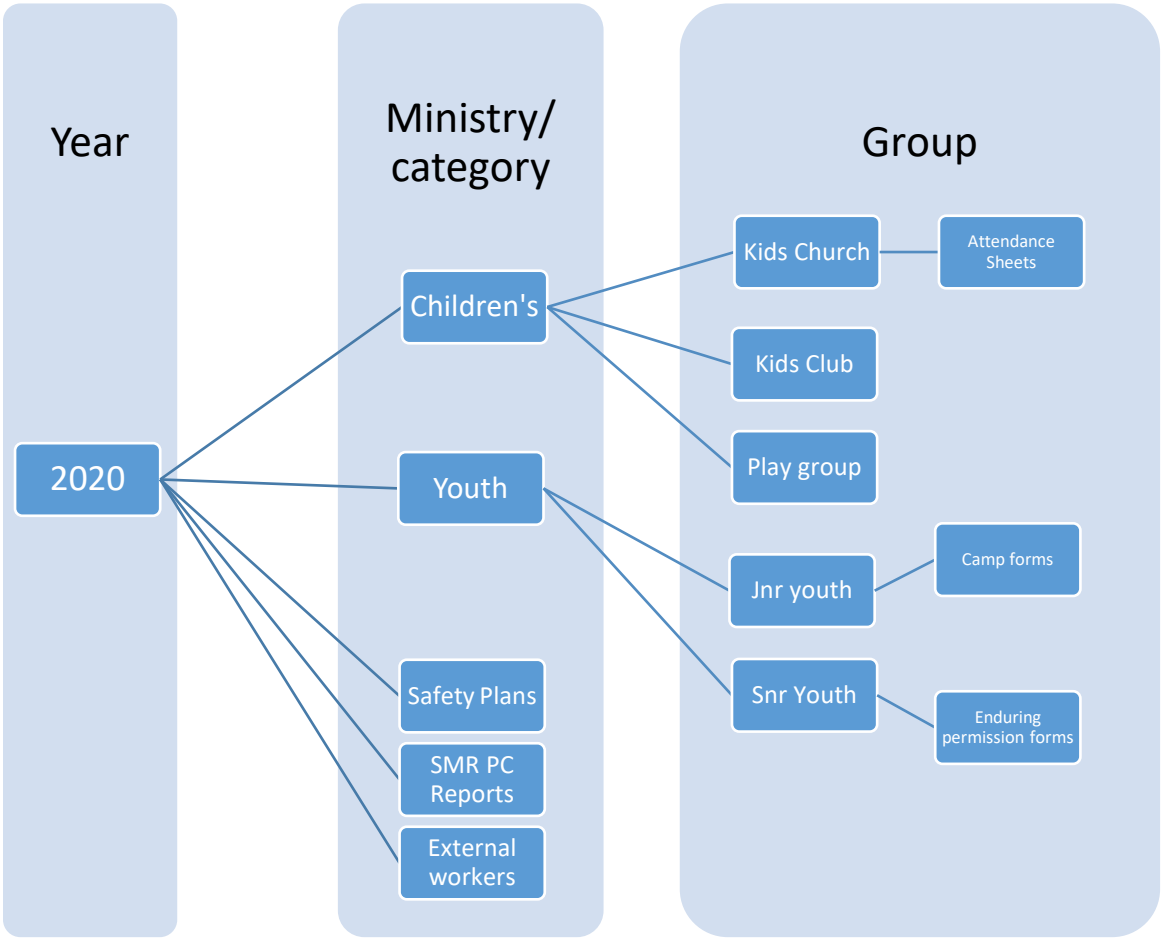
Plan how you will categorise your church Safe Ministry data and then create a file structure on the primary computer that holds this data that reflects that breakdown. eg: by year, and then by ministry group and/or category of documents.
This plan should include consistent and logical file naming practices – filenames that will make sense 10, 20 or 30 years into the future.

For this to be effective, all your existing paper documents should be scanned into an appropriate digital format. More on that a bit later.

Upload a copy of that file structure with all documents to your chosen cloud storage platform (more on that later). In other words, create a mirror backup of all the Safe Ministry-related data in the cloud. More on this below.

Storage & Retention of Safe Ministry Records

A typical church file structure might look like (each dark blue block would be a folder in your file system):



The above is meant to be an example only – a real life church would have many more branches/folders, and larger churches would require a more sophisticated system to manage the larger amounts of data they would produce.
The key is to be consistent in naming the folders and the files in them.

Who should have access?

With the sensitivity of most Safe Ministry-related documents, access to this data needs to be strictly controlled. The current Safe Ministry Rep, Wardens and the Senior Minister of the church are the main people who should have access to all Safe Ministry Related documents.
Key admin people might also require access to some or all such documents, but in general, ministry leaders do not require such access or if they do, it should access only to documents and files relating to their specific area of ministry and their level of responsibility within that ministry.
That will mean developing an approach of password-protecting certain folders in the

data structure.

Note:

- There are two types of Safe Ministry document which should have restricted access:
    - Safe Ministry Check forms. These should on be viewable by the Senior Minster or possible other pastoral staff. They should not be routinely viewable by the Safe Ministry Rep or admin people.
    - Safety Plans. These should only be accessible by the Senior Minister and the current wardens. Note that these documents are often only kept as paper documents.
- When the people in those roles change, their access should be immediately revoked, and new office holders given fresh credentials.
- Access for all relevant people should be password protected with ***strong*** passwords. See this article for guidelines on how to make strong passwords work for you.
- A careful and detailed record of who has access to what should be kept, but NOT records of passwords. If a password is forgotten, it should be reset by the person with oversight of such processes – usually a church administrator or possibly the Safe Ministry Rep in a smaller church.

Where to store the data?

It is assumed that the church will already have a reliable and secure computer system for the local storage of digital Safe Ministry-related data.
But that data requires a sound method to back it up away from the everyday computer used.
The most common approach to back up local computer data is an external hard drive or a USB flash drive. While easy and convenient, both are compromised approaches to backups in that they are easily stolen, lost or damaged.

A cost effective and efficient way to backup and store large amounts of data is to use a recommended *cloud storage platform*.
What does that mean? It means a service that specialises in storing your data on secure servers located 'in the cloud' (ie: accessible via the internet).

Storage & Retention of Safe Ministry Records

The best expression for the type of cloud storage that our churches should be looking for is a *cloud backup solution* where one or more folders or drives on a local system (ie: your church desktop or laptop) is mirrored to a cloud service.
This way, files are easily retrieved if local copies are deleted or for remote access (ie when you are away from your desk).
In other words, a copy of all your Safe Ministry-related data is securely stored in the cloud. That way, all the digitised documents are available locally on your desktop or laptop, but are securely backed up for easy retrieval if and when required.

Key to effective cloud backup solutions is a reasonably fast internet connection at the location where your local device is located/used – usually the church office. If you already have a large amount of data to store, be aware that uploading that will take considerable time (probably some weeks or even months on slower NBN connections) and so should be planned to happen in stages.
If your church does not have a decent NBN connection (eg: 50mbps or higher) or is still on ADSL, you will need to consider implementing this approach at another location, upgrading your church internet connection, or implementing a temporary solution until a faster internet connection can be put in place.

Which cloud platform?

Note that the terms '*secure and private*' and '*free'* do not go well together, and that means that your church should **NOT** be using any of the 'free' cloud storage services like Google Drive, iCloud, the free version of Dropbox, OneDrive, etc.
While the price tag on these services is attractive, if they are free, then you will find on reading the fine print in their Terms & Conditions that in return, they will take ownership of your data.
That means you have no control over what happens to your data and how it is used.
This is clearly not a good idea when we are dealing with highly sensitive data.

So your church should be looking for a company with an excellent reputation for security and privacy, and at a price that will fit your church budget.

The good news is that there are some good options that meet that criteria.
Here are three such companies:

Backblaze Business Backup – This service is a sound and cost effective solution (from $US60 per year for one PC/Mac).

Pcloud – A Swiss-based company which is a standout in this field, having never been hacked. It has a service which allows for up to 2Tb of data storage per year around $US100 per annum. This service offers either the 'mirroring' approach to backing up as discussed earlier and a virtual hard disk approach where your uploaded files are accessible for your local device, but they are not stored on your device (ie: you need an internet connection to access the files). Security is excellent with the level of encryption very high.

Tresorit - Another Swiss-based, highly secure service. At time of writing 2Tb of storage will cost $US72 per year. This uses the mirroring approach to backing up. It also has very strong levels of encryption.

All three use end-to-end encryption, meaning that your data is encrypted as it leaves your local device and is stored in an encrypted state on their servers and is only de-encrypted when you download it back to your local device if and when required.
These services also use real-time backing up – so when you have completed your initial upload of historical data, any edits made to existing files or new files added as you work locally are immediately backed up in real time.

Document format

Before you start uploading documents, it is important to consider what format they should be in. In 20-30 years time, if your church needs to check some of the information in a stored document, it should be in a format which is most likely to be easily readable into the future.
The following formats should age well:

- pdf
- csv (NOT Excel format .xls files)
- Word files – bit of a question over these and keeping a .txt or .rtf version of files is recommended.

So that means that existing physical documents can be scanned to pdf's and uploaded, and documents like attendance data in spreadsheets can easily be saved as .csv files for long term storage.

Obviously, for many churches this will mean planning a process to progressively scan and store document over a period of time.
Note that virtually every modern copier found in many church offices can scan to pdf.

Seek advice

If this document has been hard for you to follow, we also strongly recommend that you seek some skilled IT assistance in setting any of these systems up.
It is really worth the effort and any related cost to get this right so your church is well placed to meet current and any future requirements to produce documentation if/when a complaint is lodged against someone in your church.
While it may not feel like it, good management of documentation is a key part of caring for the young and vulnerable people in our churches, and helps us be a good witness to our community by meeting key Royal Commission recommendations.

P.S. – Safe Ministry Training Certificates

One important note re: Safe Ministry Training certificates:
Since December 2019, Safe Ministry Reps (or their delegates) have access to a Certificate Verification page on the SMT website. There they can enter a certificate code from one of their church members and get instant verification of the person, the course and the date of completion.

This means that most churches do not have to store actual copies of certificates – so long as you have the certificate number, that will be sufficient proof (once verified) of Safe Ministry Training.
Note: verifying certificates is entirely optional – it is for the convenience of churches, nothing more.

safeministry
PROTECTION AND CARE FOR EVERYONE

Storage & Retention of Safe Ministry Records

Summary:

- ☑ **SEEK** – professional advice is necessary on implementing a sound data storage, backup and retrieval system for you church.
- ☑ **PLAN** – The file and folder structure for your church's current and historic Safe Ministry related data, and for the password protection protocols to govern access to sensitive information.
- ☑ **CHECK** – your church's internet connection. Is it fast enough to cope with the requirements for effective, long term storage and retrieval of large amounts of data?
- ☑ **DECIDE** – on a long-term storage/backup location. Carefully check the services offered by one of the three recommended cloud storage providers, or another of your choosing (being 100% certain of the security and privacy credentials of the service).
- ☑ **DOCUMENT** – the way the system is setup, the naming protocols for files and folders and the password protection of sensitive information
- ☑ **TRAIN** – ministry and appropriate admin staff on how to use and access the data storage system and on the file naming and folder structure of the church system