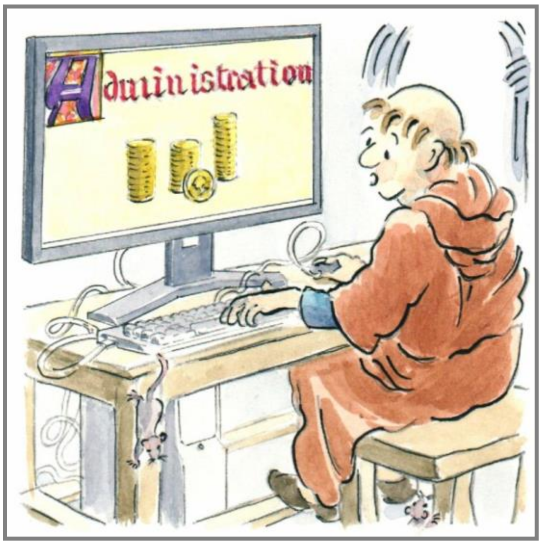
john truscott
church consultant and trainer



The management of church records

A broad overview

A55 Articles series: Administration

This Article seeks to summarise legal and best practice requirements for both the management and retention of church records.

It takes more of an overview of the topic than just listing what must be kept and for how long and so includes just a summary of retention requirements, with links provided to fuller lists on other websites. The aim is to help any church devise and implement a Document Management/Retention Policy.

Large churches which manage a significant amount of personal data should be advised to take professional legal advice to ensure they follow the requirements of GDPR (the General Data Protection Regulation) and the Data Protection Act 2018*. This Article should not be read as a legal document.

There are three main parts as follows:

1 **General issues**
Six key areas as a basis for any thinking and then policy on this topic.

2 **Records by category**
An overview of legislation and advice for different categories of record.

3 **A Document Management/Retention Policy**
This section takes the material already covered and shows how to create your own policy. There is then a listing of other websites for specific data categories and denominations.

*The Data Protection Act 2018 is the UK implementation of the GDPR and is sometimes known as UK GDPR.

Note that this Article contains a significant amount of detail some of which may change over time. If you spot any errors please advise me so they can be corrected.

Issues to consider

Here are six areas which give a good cover of this broad topic. Later this Article suggests how they might form the basic structure for a church policy.

1	Record management	4	Security
2	Holding records	5	Your church's story
3	Legal requirements	6	Implementation

Note that the words 'record' and 'document' are often used as interchangeable though, technically, they are not quite the same in that a 'record' may contain several 'documents'. You may prefer to use the word 'data' instead.

In addition to legal requirements, the main point of managing records well, as stated by the Records Management Society is to ensure that 'the right information is with the right people at the right time'.

1: Record management

A record holds information about people, events or situations which has been created or received by the church. Examples include:

- a form listing someone's contact details;
- a report and accounts;
- an official register of a baptism;
- a set of minutes;
- an insurance policy;
- a church profile;
- a set of membership statistics;
- an employee's job description;
- a risk assessment;
- a church publication.

Such records are essential for the effective operation of a church. But it will be immediately obvious that there will be a considerable number of such records in even a small church. Some will be held in paper format and many will now be electronic (and most will probably exist in both forms).

We need such records to understand the past, analyse the present and thereby plan for the future.

But things can easily get out of hand. Church records may be stored in a range of locations in different formats. Some may be lost while others will appear with many duplicates. Finding the record you need may be quite a problem and, because of national scares, people may well worry that information they provided is now being used in ways they had not anticipated.

On a national scale, record management is so important there is a considerable body of legislation that applies and that churches therefore need to comply with. For example you are not allowed to hold information about people once the purpose for that information no longer applies. On the other hand you are required to hold official records, such as accounts or employment records, for certain stated minimum lengths of time. People have been given powers to see what personal data a church holds for them.

Some legislation is a matter of specific instruction (you have to hold particular records for at least a fixed number of years) and some of which you are required to interpret wisely (such as how transparent you are in dealing with your records or, for smaller churches, whether you are required to follow every aspect of legal requirements which assume larger operations). A few aspects are more a matter of best practice.

So this Article explores how to manage records effectively in a church including, but not only, when to discard or delete them to keep the amount under control. It is all about helping the church to be operationally efficient while at the same time ensuring it meets denominational, statutory and fiscal requirements. It is also vital that we treat personal records with dignity in a sensitive and pastoral way. Effective management will enable rapid and accurate 'search and find' ability for data that is held.

But such management has to operate in a changing world where data about each one of us is held for each time we walk past a security camera, shop in a supermarket, turn our computer on or use our phone. Consider safeguarding: unknown as a topic when this writer was a church Operations Manager but now, rightly, an area of detailed legislation and practice regarding record-keeping which no church can ignore.

And this points to the link between record management, pastoral care and even evangelism. Much of this subject is concerned with looking after people, of not letting George Orwell's Big Brother take charge of our lives, although many would say that life already borders on that. Oh that the Church would set an example to the world of people care and effective management in this field!

2: Holding records

It is vital to hold records, for as long as they are required but no longer, in a tidy system where each document can be easily identified and accessed. This may be in paper form or, increasingly, as electronic files. Trustees, including PCCs, have a duty of care for their church's records which they therefore need to manage well. It is very easy for the huge volume of data to become chaotic.

It is quite possible that your church's Trustees have never realised that they hold a responsibility for record keeping that is both legal and effective. It would be good practice for the Trustees to appoint one of their number with specific responsibility for this area, and to ensure that any policy and current practice are signed off by the Trustees once a year as in good hands with robust safeguards.

It is a good idea to hold one master document with hyperlinks to all key folders.

Hard copy records should be kept:

- in suitable containers or in folders on shelves and off the ground;
- easily accessible for rapid 'search and find';
- in an indexed order that makes sense to anyone coming to them for the first time;
- with box files and folders clearly labelled;
- in a secure, cool and dry environment, avoiding basements or attics;
- as safe from fire or theft as is possible;
- using plastic or special metal clips as normal ones will rust;
- avoiding rubber bands which perish with time, using string instead
- in locked cabinets for personal and employment data;
- with a regularly updated master index;
- each file with a creation date and version number in the title;
- with training for all staff and volunteers who access such records.

GDPR's seven principles for personal data

Churches should base all their personal data record keeping on these seven, taken from Article 5 of GDPR. They are set out right at the start of the legislation and inform everything that follows. They do not give hard and fast rules, but rather embody the spirit of the general data protection regime – and as such there are very limited exceptions.

1: Lawfulness, fairness and transparency

All individuals should have their personal data processed in a way that is lawful, fair and transparent.

2: Purpose limitation

Data should only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3: Data minimisation

Data collected should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4: Accuracy

Data should be accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5: Storage limitation

Data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; (with some stated exemptions for archives for purposes in the public interest).

6: Integrity and confidentiality (security)

Data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7: Accountability

The Data Controller (see box on p5) shall be responsible for, and be able to demonstrate compliance with, the above six principles.

Electronic records need to be held:

- in a password-protected system with 'strong' passwords;
- with adequate and secure back-ups (utilising more than one system if possible);
- ideally in the cloud with at least one regularly updated back-up physically elsewhere;
- with updated virus protection on the church's IT system;
- with software that is updated as each new version is released;
- with file names descriptive enough for anyone to find easily;
- with added tags to files to speed up searching (you may need to learn how to do this for your specific software and device);
- with restricted access for all staffing and personal records;
- each document with a clear date and version number;
- with training for all staff and volunteers who access such records.

Some documents are retained in an immediately accessible way because they may be in use day-to-day. Others, usually because they need to be retained permanently, can be archived by specialist record offices even if they are not quite as important as the Magna Carta. In all cases ensure that documents are dated (this writer finds this is a weakness in many churches).

But the planned destruction of documents is as important as their retention. Holding on to documentation for too long may, of first importance, violate legal requirements but also takes up space and can result in confusion and inefficiency.

Church paperwork that is no longer needed should be cross-cut shredded. Electronic files need to be permanently deleted along with any back-ups whether on laptops, server, external hard drives or in the cloud. You may well need a policy for all those who have records on stand-alone devices to consider how this is controlled and how data deletion is secured.

3: Legal requirements

There is a range of legislation that requires certain legal and financial documentation to be held for fixed periods of time before they can be destroyed or deleted. This Article gives examples of these in what follows but cannot give full detail and so refers to other open-access resources for fuller advice.

Legislation that applies includes:

- Charities Act 2016
- Data Protection Act 2018 (DPA) and GDPR (see box on this page)
- Limitations Act 1980
- Taxes Management Act 1970
- Various items of HR and safeguarding legislation
- *For CofE churches:* The Church of England (Miscellaneous Provisions) Measure 1992

There are also HMRC requirements for some financial records as well as denominational requirements for holding official registers. The DPA includes details of security and principles for how data should be processed.

Perhaps the most important of these for churches to note is the Data Protection Act and GDPR. It is not possible to explore these in detail in this more general look at data management, but the box on page 5 provides a summary and here are a few specific points for how these work out in practice in churches.

First, any Data Management/Retention Policy should either address the issue of why records are kept in the first place, or at least refer clearly to another policy that covers this. This is because of GDPR requirements. A church should only be holding personal information where there is a legitimate interest or specific permission has been granted and is regularly reviewed.

For example, any church has a legitimate purpose in holding membership information but if someone ceases to be a member (in any obvious meaning of that term), the church can only continue to hold information about them with their recorded permission. So if a church member leaves but asks to continue on a prayer chain, they must be shown to have given permission for the church to retain their email address. Without such permission all records should be deleted.

Secondly, a church should be ready to deal with a Subject Access Request or even a Freedom of Information request, both of which have short deadlines in law. This means that records should be kept in such a way that such requests can be dealt with speedily. Under the 'Right to be Forgotten' terms it is important that any church can decide quickly whether to decline the request if there is no legitimate reason to act. If there is good reason, can the church ensure that all records, both those held centrally and those on stand-alone devices, can be deleted promptly?

A brief introduction to GDPR

GDPR began life as a European law but was later incorporated into UK legislation post-Brexit as the Data Protection Act 2018. Its regulator in the UK is the Information Commissioner's Office (ICO). It applies to churches as much as any other charities and to organisations of all kinds.

It relates to personal data about members, donors, volunteers, staff, suppliers and clients.

Terms in use

A 'data controller' is any organisation (or church) that processes personal data (which may simply be holding a mailing list).

A 'data processor' is anyone who handles that data (such as a Church Administrator who holds and updates the mailing list).

A 'Data Protection Officer' is an independent officer who supervises the church's data handling. Large and complex churches should take advice about appointing such a person but it is unnecessary for most churches.

'Data subjects', a term for all people who have personal information about them held by a church, have various rights under the legislation. For example, they can

- seek information about what is held about them and how it is being applied, processed and stored;
- access their personal data;
- update any inaccurate personal data;
- withdraw their permission for the church to process their data.

Following GDPR in practice

Most churches will comply with the legislation provided they follow the seven GDPR principles (see box on page 3) in the following way.

Ask people for their permission

Ensure you can be shown to be asking permission in writing for the church to hold personal data, and offer a clear way in which that permission can be withdrawn. Do not hide any aspect of your use of that data.

Keep all their personal data secure

It should only be available to those who have a valid reason to use it and be held in a secure way, whether hard copy or electronic.

Provide a clear purpose for the data

Ensure people know why you are holding and using personal data. You must have a valid reason that is current. This is known as a 'legitimate interest'.

Document evidence to show compliance with GDPR

Each step taken, or amended, should be recorded in a permanent folder and regularly updated. You may need this if ever accused of a breach.

Thirdly the forms in which people have given permissions regarding personal information (such as contact details) should be clear. Note that commercial management systems (such as ChurchSuite) are almost always designed to ensure forms comply with GDPR.

Finally, the church must know what it does with data held about children when they reach the age of 18, and what happens if the young adult remains in the church but their parents are no longer involved. For example you will need each young person's permission to move their record to your main database when they reach 18. Without this their record should be deleted unless there is a safeguarding issue when records must be kept (see later section). Obtain professional advice for queries.

4: Security

The first action here is to discover what requirements your denomination or stream has for document security. Church of England churches, for example, have requirements for the keeping of registers in the safe and then to be held in secure archive by the Diocesan Records Office. Hard copy records of minutes can be kept in the parish office. But how safe is this from theft, fire or damp?

The problem in many churches is that different records are held in different locations: Trustees may hold file minutes and other governance details at home. Treasurers may hold all financial records again at home and handover of office may omit some documents. Ministers may have various kind of record in their tied dwelling.

This is an important issue, not often discussed, which impacts document security. It is much to be preferred if formal documents can be held in a central system to which access is restricted and in current times the recommended location is in the secure cloud.

Only one set of records needs to be retained. Be careful if the Church/PCC Secretary and the Minister are both holding what they regard as the official church sets (as opposed to personal sets). This can easily happen with minutes, for example. One set belongs to the church and cannot be removed by an individual for their personal use.

General opinion has it that electronic files offer a more secure means of filing than hard copy. But if the necessary records are kept in this way, how helpful is the indexing system to be able to identify what there is and where?

Electronic files, especially emails, are much more easily copied and so tend to proliferate widely. This can cause problems for confidential data, such as personal data, when close control is required under GDPR.

Is cloud storage really as safe as the big companies that run it make out? What if there was a huge cyber attack of a kind we can hardly imagine today that rendered such records unreadable?

If back-ups are on external hard drives, who keeps these, in what form and where? Try to ensure that all e-documents are kept in a professional cloud-based system (such as Microsoft 365, Dropbox, Google Docs, ChurchSuite, ExpensePlus, etc.).

On security, there is also the issue of protection software for the church to ensure that any cyber attack can be resisted and those who staff the church phone lines and emails are trained to spot scams. See Training Notes TN46, *A beginner's guide to IT security,* and TN143, *Protect your church from scams,* both on this website.

The Data Protection Act states that you must ensure that:

- any paper filing system is lockable (the same if the system contains external hard drives)
- any electronic records are password and virus protected;
- only those who use the data can have access it.

There are also principles listed in how data should be processed fairly.

Security is a major issue to consider in any type of record management. Churches can be targeted to release financial information or details of members. Scams can appear in the form of telephone calls, email attachments, corrupted websites and phony callers in person. Records may also be held by church members and office holders in private homes, or regularly transported in, for example, a laptop and so vulnerable to attack or misplacement.

Warning signs for scams

(from Training Notes TN143 on this website)

1. An attachment from an unfamiliar source
2. A sense of forced urgency with penalties
3. A generic greeting
4. A strange URL
5. Poor quality text/layout
6. A recorded message
7. Any unexpected gain
8. Any request to transfer funds
9. Any offer of tech support

5: Your church's story

Another issue to keep in mind when you manage or delete and destroy records is the need to tell the story of your church. It would be sad if there was no outline history for future generations to hear or to answer questions as to when key events took place. People's memories will only cover a limited number of years and are likely to include inaccuracies.

Although we have noted already that many records have to be deleted after a certain time, there are others that need to be kept and archived for future generations. Records that tell the story of your church will include:

- minutes of Trustee and church meetings ;
- statistical information about attendance, membership, age profiles (especially for children and young people's work);
- lists of Ministers and other leaders;
- historical records about the area including church profiles;
- historical records of the church building and associated properties including Title Deeds and relevant correspondence
- an accurate record of all valuable objects owned including gold/silver, memorials, special furniture, memorabilia;
- records of baptisms, weddings, funerals and civic/special services;
- graveyard records;
- church guides and other documentation about the buildings;
- special church events with photographs;
- visitor books.

One key need for many historic buildings will be the register of burials and documentation relating to both open and closed graveyards. Some Church Administrators have to spend a significant amount of their time assisting people searching for family graves. So permanent retention will be critically important here.

But what of the story of the living? Trustee (including PCC) minutes will offer a helpful time-line of major decisions; annual reports and accounts will do the same. But it might be helpful to write and archive a short list of key actions and achievements year by year, both as a form of review, but also as a historical record.

For what to include in a church profile see Training Notes TN114, *How to prepare a church profile,* on this website.

Lists of Ministers with dates need to be kept up-to-date. Statistical data of church attendance, often through denominational returns, will offer helpful information for mission. Church guides for historic buildings tell a story.

It is therefore helpful to have in a Document Management/Retention Policy some means of recording the history of the building, the area, key changes and developments.

6: Implementation

A policy is all very well but what matters is its strict implementation. This is a task which needs a fixed point in the annual calendar for those responsible. The policy should include practical details of how implementation will be assured. For more on this, see below.

Having a document schedule in place is all well and good but where many churches fall down is on implementation in practice. Churches tend to be busy places and as a result it is all too easy to postpone apparently non-urgent tasks such as filing new records or deleting old ones until a quieter day which of course never arrives.

To avoid this trap it is important to be realistic about how much time is required and to ensure that it is prioritised appropriately at particular seasons. Perhaps certain times of each week, month or year should be set for the activity to take place. Perhaps someone outside the normal staff team (but a trusted church 'insider' for confidentiality reasons) should be asked to come in at a fixed time of year to perform the task of weeding out old records.

Consider also making use of a commercial shredding service at this time of year. These are relatively inexpensive and offer a much more practical solution than office shredder devices which tend not to cope well with large volumes.

An annual weeding of the files

It is as important to destroy or delete files no longer needed, and sometimes this is a legal necessity as has been shown. This requires an annual 'weeding' (an official term) of all documents. Some need to be kept permanently. Some need to be 'archived' (perhaps after being thinned out) and sent to a diocesan or local authority record office to clear space in your own archive.

Some need to be shredded or deleted as being no longer necessary and again freeing up space. Where this is a legal necessity it is vital to ensure that all copies are also shredded or deleted. Paper copies may be held by a number of different people, and electronic copies are likely to have back-ups and may be on a number of computers as email attachments as well as single files.

Some need to be thinned down. For example, it may be better to keep a sample church magazine from each year than to hold all 12 copies which over many years take up a considerable space.

As already advised, this process is best carried out at a fixed annual point so that it is not overlooked.

Someone responsible

But none of this will happen unless someone is responsible for the policy and an annual sort out. This ideally needs to be someone who already has access to the files to avoid unnecessary spreading of confidential and personal information.

GDPR requires Trustees as the Data Controller to appoint someone responsible and accountable to them. Confidentiality issues may lead some Ministers to feel this should be their responsibility but that would be a pity as they have more important roles to play. In some denominations the Church Secretary might be the responsible person or a Church Administrator or Operations Manager, or possibly a specialist Church Archivist.

But whatever it needs someone who feels the responsibility or it will simply not happen. And the Trustees need to own the process for they will be held liable for document leak or illegal destruction.

This person is responsible to the Trustees for ensuring compliance with some of the main aspects of that legislation. So Trustees need to demonstrate leadership in this area and should consider ways in which they might do this. An example would be to ask occasional pertinent questions at Trustees' meetings or by conducting a mini-audit from time to time.

Records by category

There is legislation that applies to different types of documentation. Here are six categories to consider and a summary of the records to keep and for how long for specific records. Note that this is an overall summary. For greater detail see the weblinks given in the final part of this Article.

1: **HR records**

Records of employees need to be kept in a well organised system, under the requirements of the DPA 2018 and the GDPR.

There is nothing in the DPA or GDPR to indicate how long to hold records for although GDPR does require you to define and implement a Data Retention Policy. Data must not be kept for any longer than necessary and the emphasis is on the employer to have proper systems in place. However other legislation may dictate statutory periods for various types of HR record (see below).

This is not a comprehensive list but gives the obvious documentation to file.

- employee personal details & NI numbers;
- recruitment details and application forms;
- signed written statement of contract terms;
- DBS records if required (for both employees and volunteers);
- hours, pay details and tax records with expense records;
- P45, P6, P11D, P60 documentation;
- SMP and SSP details;
- furlough records for Covid;
- annual returns and pension details and deductions;
- signed statements for change of contract details;
- absence details, training records, appraisal meetings and disciplinary actions.

There are a number of regulations which have to be met in HR retention periods. Here is a small selection. The norm for most HR documentation not covered by other legislation is six years plus the current year.

- medical records held under COSHH – 40 years from the date of the last entry;
- employer's liability insurance certificate – 40 years;
- National Minimum Wage Records – three years after the end of the pay reference period following the one covered;
- maternity pay and other medical HR records – three years after the end of the tax year in which the maternity period ends;
- whistle-blowing documents - six months following the outcome if substantiated;
- redundancy records – six years from the date of the redundancy.

The position for HR records where no legislation dictates a period is very much up to the employer. As a general rule of advice, seven years would cover the six-year time limit for starting legal proceedings (UK Limitation Act 1980). The following are recommendations.

- parental leave – 18 years from the birth of the child;
- pension records – 12 years after the benefit ceases;
- personnel files including disciplinary records – six years after employment ceases;
- references – at least one year;
- application forms for unsuccessful candidates – six months to one year.

2: **Financial records**

Here is a general listing of what to keep. Much of this will be in electronic format or available when required from websites (such as bank statements).

- payments cash book;
- purchase ledger, petty cash records, payroll;
- revenue and capital invoices;
- receipts cash book;
- bank statements and reconciliations;
- remittance advice, sales ledger;

- correspondence about donations and legacies;
- Gift Aid declarations;
- Trust Deeds;
- annual report and accounts;
- insurance policies and claims correspondence.

The main piece of legislation here is the Charities Act which states that financial records must be kept for six years from the end of the financial year in which transactions were made. HMRC have a similar period for Gift Aid declarations.

However, there are exceptions where HMRC requirements may over-ride the Act. Invoices for capital items must be kept for ten years. Legacy records must be kept for six years after the estate has been wound up (Data Protection Act). Many tax records also have to be kept for six years plus the current year (Taxes Management Act). It is recommended that annual accounts are kept for ten years and then archived.

3: **Governance/legal records**

Different denominations have specific requirements in this area and this list only gives a general overview. You need to hold:

- Trust Deeds, title deeds and other foundation documents;*
- LEP agreements and pastoral schemes;*
- official registers of baptisms and marriages;*
- official registers of funerals and burials with graveyard plans;*
- official registers of CofE banns, confirmations and services;*
- church membership lists;*
- church contacts lists;
- signed copies of Trustee and Church Meetings minutes;*
- copies of meeting papers and committee records;
- major agreements of historical importance;*
- investment ledgers and fixed asset registers;*
- policies.

Legislation here includes the Charities Act, Data Protection Act, Limitations Act 1980 and denominational requirements. All starred items need to be kept permanently and moved to your relevant record office but check denominational requirements. Signed copies of Trustee and Church Meeting minutes are only legally required to be kept for ten years from the date of the meeting but the recommendation would be permanent retention in archive and most denominations insist on this. Other meeting papers should be kept for five years.

Policies need to be held for three years after lapse. Church of England churches should access the paper *Keep or bin…?* (see below) for greater detail on what to keep and to delete.

Note that new arrangements for marriage registration came into force from May 2021.

There may also be records relating to the Data Protection Act 2018 such as:

- data subject access requests;
- rights to be forgotten;
- rights to restrict processing;
- data protection consent records;
- data consent forms;
- data processor records.

4: **Property/health and safety**

This is an area where different denominations have different requirements so check with yours for fuller details. The following is only an outline.

- title deeds;*
- building design drawings, records of major work and redevelopments;*
- quinquennial inspection reports;*
- leases* and licences;
- lettings agreements;
- asbestos / hazardous substance register/disposal;*
- burial registers and records of graveyards with plans;*
- churchyard maintenance including graves and memorials;*~
- full details of all major works to churchyard;*~
- property logs or equivalents;*
- Terrier, Inventory and Logbook (see box on page 10);*~
- faculties and papers, plans, drawings, etc.;*~
- plans etc. for major alterations;*~
- tenders, etc. for minor works;
- organ works;*
- PRS licences etc.;

- insurance policies and certificates for public liability;*
- public liability policies;*
- employers' liability;
- other policies and claims correspondence;
- Health and Safety inspections;
- accident books;
- visitor books;
- similar details for parsonage house or manse.

*Items marked ~ relate to Church of England churches. Those marked * should be kept in a permanent archive.*

Where property is sold, it is advisable to keep copies of title documents and design drawings etc. for a further six years but then dispose of them. But for leases, hold for 12 years after the lease expires.

Church of England property

Note: Other denominations should refer to their denominational guidelines or requirements, or seek external advice.

Section 4 of the Care of Churches and Ecclesiastical Jurisdiction Measure 1991 requires Church of England Church Wardens to compile and maintain a full 'terrier' and 'inventory' of all land and articles appertaining to their church.

There is the requirement to maintain:

- Terrier - a list of lands belonging to the Church;
- Inventory - a list of all the items belonging to the church;
- Log book - a detailed record of all the alterations, additions and repairs to the church, its land and contents.

The Register has to be completed in permanent ink, preferably the Stationery Office Record Ink used for registers of baptisms, weddings and burials.

The documents may be generated on a computer but hard copies must be produced for storage following the given format and using archival-quality paper or good-quality photocopier paper.

One full copy of each document is to be kept in the church safe and a second (paper) copy is to be deposited at the Diocesan Office.

For new developments, you need to hold documentation for at least 13 years for actions against contractors.

Papers relating to minor works on buildings should be kept for six years from last action, but organ specifications need to be archived. Recording and other licences should be kept for five years from last action.

Insurance policies should be kept for 40 years (standard commercial practice) but claims correspondence for three years from the last action. Note that some denominations may have more stringent requirements. For example, the Baptist Union ask for public and employee liability records to be kept permanently with electronic back-up. Other policies and claims correspondence are normally held for six years after lapse (or last action if longer).

Leases are normally kept for six years from the end of the agreement but then archived and lettings agreements for one year. Quinquennial inspection reports should be kept permanently.

Accident books should be retained for three years from the final incident or the end of any investigation if later, but if a child is involved details need to be kept until they attain the age of 21 plus three more years. However the CofE has 20 years from the date of incident, or the date when a child reaches 21. HSE inspection records should be held for three years.

5: **Safeguarding records**

This is a sensitive area of record keeping where retention is now in response to the Independent Inquiry into Child Sexual Abuse (IICSA). Under the Inquiries Act churches in England and Wales have to retain all documents relating to child protection and this overrides retention requirements under the Data Protection Act.

The relevant legislation here lies in Section 25 of the Inquiries Act which requires churches in England and Wales to retain child protection documentation and all allegations of abuse made against individuals or the church. Any requirement not to destroy takes precedence over the DPA 2018.

Safeguarding records include:

- allegations and concerns;
- risk assessments;
- employment;
- discipline;
- Safeguarding leadership
- DBS certificates for current volunteers and staff;

- child or vulnerable adult concerns recorded.

It is not possible in a short overview article to go into any detail for retention periods and this is not a legal document. But, briefly:

- All safeguarding records of incidents or concerns for children or adults, including risk assessments, with details of how allegations are handled and actions taken with eventual outcomes – 75# years after the last contact with the individual concerned.
- For safeguarding records of incidents relating to a church officer paid or unpaid – 75# years after employment ceases.
- For records of any children's activities and related risk assessments – 75# years after the activity ceases.
- For CofE clergy personnel records where there are no safeguarding allegations – under consideration to increase from 20 years.
- For CofE clergy personnel records where there are allegations and investigations – under consideration to increase from 50 years.
- Personnel records for lay workers whose role involves contact with children or vulnerable adults – 75 years after employment.
- DBS disclosures for vetting for employment – six months after recruitment decision.

There are further requirements affecting clergy.

For fuller details see the Church of England Record Centre's papers, 'Safeguarding Records – Retention' and the Joint Practice Guidance on Safeguarding Records May 2015 which have links below.

# CofE has 70 or 50 years here.

6: **Administrative records**

The issue here is usefulness rather than legal requirement. Here are a few examples.

- Church guides – hold one copy in archive whenever a new version is produced.
- Church magazine, news-sheets – hold one copy in archive as each new one is produced. Some would say hold for five years then destroy. These can however be helpful as a permanent history of the church.
- Lists of home groups – for as long as useful.
- Annual website snapshots – a valuable source of church history.
- Church profiles – five years from last action, although these are a valuable source of historical detail for both church and its area so might better be permanent.
- General correspondence and emails – each denomination or network may offer their own advice on correspondence that does not fall into other categories already listed. This seems to vary from one year to seven, or left as simply 'as long as is relevant'.
- Copyright licences.
- Photographic displays of church buildings and property, especially at a time when the building has been reordered

A Management/Retention Policy

The first part of this Article suggested six areas to include in a Document Management/Retention Policy. Here are points to bear in mind under each of these six headings suggested there as you prepare your policy.

1: Record management

You might like to include some of the material listed under this heading to underline the importance of record management and the place it plays in operations and administration.

It is better to write your own introduction than simply copying what your own denomination has from the sample weblinks given below. But the material under this heading will provide a good starting point.

2: Holding records

Under this heading you might list the principles for holding both hard copy and electronic files. You will find more ideas on this in several of the items web linked in the section that follows. If you do not list the seven GDPR principles under the next heading they would fit here.

3: Legal requirements

It is important to understand that your Trustees needs to be compliant with national legislation or denominational requirements. Your policy should be designed to avoid the danger of someone simply deciding to weed the files and discarding documents that you are required to hold for a longer period or permanently.

4: Security

Both paper records and electronic files need to be kept secure. There are ideas for principles in this section that you may want to set out here. Note also the dangers of, for example, a church member with records on their laptop leaving their computer on public transport. Consider two the difficulties caused if different church members hold records at home on their own computers.

5: Your church's story

To understand why key decisions were taken some years ago, it is necessary to have accurate records. To see how God has been at work, you need to understand the past and how it impacts the present. Record management is not just a legal necessity but an ongoing telling of the story. A modern-day Acts of the Apostles if you like. Where would we be without such biblical records?

6: Implementation

This should be an important section of your policy, underlining the need for the Trustees (as the Data Controller) to take action so that the policy is actioned and not just prepared for show. There should be an annual weeding out of files and clear lines of responsibility for at least one Trustee and one member of staff or a volunteer.

7: Types of record and retention periods

The Policy should include (and this will probably be the major section) a listing of different types of document and the length of time for which they need to be held and where. Som examples are given from legal and best practice but a number of more detailed lists are web-linked for fuller information. This article is not to be read as legal advice.

Helpful sources for greater detail

General advice on the Data Protection Act
https://ico.org.uk/for-organisations/guidance-index/data-protection-act-1998/ and especially https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

General advice on HR records
https://www.cipd.co.uk/knowledge/fundamentals/people/hr/keeping-records-factsheet#gref

General advice on safeguarding records
https://www.churchofengland.org/sites/default/files/2017-10/Safeguarding%20Records-%20Retention%20Tool%20kit%20-Dec%2015.pdf

General advice for charities
https://knowhow.ncvo.org.uk/organisation/operations/legal/records

General advice on legal requirements
https://www.buzzacott.co.uk/insights/retention-of-accounting-records-and-other-corporate-records
(then the 'Retention of accounting records' pdf)

For Church of England churches (and more widely applicable)
https://www.churchofengland.org/about/libraries-and-archives/records-management-guides
and then select 'Keep or bin…?', 'Safeguarding records management' and more. Note that 'Keep or bin…?' was written in 2009 before the current Data Protection Act and GDPR came in.

For Methodist churches (and more widely applicable)
https://www.methodist.org.uk/for-churches/office-holders/archivists/
and then select 'Retention schedules for Methodist records'.

For Baptist churches (and more widely applicable)
https://www.baptist.org.uk/Groups/304642/Church_data_protection.aspx
See especially their 'Data Retention Schedule'.

Please inform the author of other sites you have found to be of value so a decision can be taken on whether to include additional resources.

Legislation on the topic of data management changes from time to time. If you spot any inaccuracies in this Article, please inform the author so that this can be checked and if necessary corrected.

If you work as a Church Administrator or Operations Manager in any form, be sure to join UCAN. It has so much to offer. See their website.

This article is available at https://www.john-truscott.co.uk/Resources/Articles-index then A55. See also Articles A1, *Pass or file,* and A37, *Sorting out your study – Part 2,* plus Training Notes TN114, *How to prepare a church profile,* and TN143, *Protect your church from scams.*

Contact John if you would like to enquire about the possibility of advice or training on administrative issues.

Cartoons are by Micki Hounslow for filing categories of Leadership, Management, Structures, Planning, Communication, Administration. File A55 under Administration.

John Truscott, 69 Sandridge Road, St Albans, AL1 4AG
Tel: 01727 832176 Email: john@john-truscott.co.uk Web: https://www.john-truscott.co.uk