# Data Governance.

**SECTION 1 - DATA PROTECTION**

The Data Protection Act 1998 gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly. The Act works in two ways. Firstly, it states that anyone who processes personal information must comply with eight principles, which make sure that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant, and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with the individual's rights
- Secure
- Not transferred to other countries without adequate safeguarding

The second area covered by the Act provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records. Should an individual or organisation feel they are being denied access to personal information they are entitled to, or feel their information has not been handled according to the eight principles, they can contact the Information Commissioner's Office for help. Complaints are usually dealt with informally, but if this is not possible, enforcement action can be taken.

There is an exemption under the Data Protection Act that can be applied if the police need some information to prevent or detect crime or catch or prosecute a suspect. However there are limits on the information that can be released. If we are satisfied that the information is going to be used for this purpose, and that if we did not release the information it would be likely to prejudice (that is, significantly harm) any attempt by the police to prevent a crime or catch a suspect, then we can disclose this information.

**Contacting individuals**
The Village MCC must not contact individuals without their prior consent unless they have indicated an interest in The Village MCC through any method where they have personally given their information.
In all generic correspondence, there will an 'opt out' clause. If this is indicated as a desire from the person, it must be dealt with immediately upon receipt.

**SECTION 2 – DATA SECURITY**
**All staff (paid or volunteer) are responsible for ensuring that:**

1. Any personal data they hold, whether in electronic or paper format, is kept securely.
2. Personal information is not disclosed deliberately or accidentally either orally or in writing to any unauthorised third party

**Requests for Access to information:**
Any member of the public has the right to access personal data that is being kept about them insofar as it falls within the scope of the Act. Any person wishing to exercise this right should make their request in writing to the church secretary, who will comply with requests for access to personal information within forty days of receipt of the request.

**Subject Consents**
In some cases, if the data held is sensitive, (for example information on health, race, or gender,) express consent to process the data must be obtained. This processing may be necessary to operate The Village MCC policies such as health and safety and equal opportunities.

**Where will electronic information be stored?**
Access to all electronic files is to be controlled by the Board of Trustees (the church secretary - under the Data Protection Act 1998). The Village MCC must ensure that data is centrally managed and up to date, that it is only accessible by authorised persons, backed up regularly and destroyed properly.

**Non-Sensitive Data**
Non-sensitive data such as Worship Powerpoint slides, Worship Bulletins etc, may be prepared and operated from a portable machine and past presentations can be archived.

**USB Sticks**
USB sticks have to be authorised for use with The Village MCC data and must be encrypted.

**Paperwork**
All paperwork containing personal data shall be stored securely.

**SECTION 3 - DATA RETENTION**

**Summary**
The Village MCC Data Retention Policy covers the 'lifespan' of records and information that we hold, from creation through to destruction or retention for historical or research purposes. Detailed below is The Village MCC approach to data retention, and for each type of information it explains what we do with it and how long we will keep it for.

**ACCIDENT AND INJURIES RECORDS**
**Official Copy: Church office**
**Retention:** 6 years after any case settlement.

**ACCOUNTS PAYABLE RECORDS**
*Including but not exclusive to: Claims and Disbursements Records, Expenses, Accounting, Bookkeeping, Paid Invoices, Finance, Purchasing*
**Official Copy: Treasurer**
**Retention:** 7 years.
**Other copies used in offices**
**Retention:** 2 years.

**ACCOUNTS RECEIVABLE RECORDS**
*Including but not exclusive to: Membership contributions, offerings,*
**Official Copy: Treasurer**
**Retention:** 7 years.
**Other copies used in offices**
**Retention:** 2 years

**ADMINISTRATIVE REPORTS AND POLICIES**
*Including but not exclusive to: Conference reports, Board of Trustees Reports,*
This series documents the annual activity of the local church and its subdivisions.
**Official Copy: Church office**
**Retention:** Permanent
**Other copies: Specific Teams**
**Retention:** Until superseded or obsolete. Destroy all other copies when superseded, obsolete, or no longer needed for reference.

**ANNUAL FINANCIAL REPORTS**
*Including but not exclusive to: Closing of the Books Records, Financial Reports, Balance Reconciliation Records*
**Official Copy:** Treasurer
**Retention**: Permanent - Send official copy to be archived by the Church Secretary annually.

**Other copies used in office**
**Retention:** 3 years.

**ASSET LIST**
**Official Copy: Church Office**
**Retention:** permanent

**AUDIT RECORDS**
**Official Copy: Treasurer and Church Office**
**Retention:** Permanent - Send official copy to be archived by the Church Secretary annually.

**BANK DEPOSIT BOOKS**
**Official Copy: Treasurer**
**Retention:** 7 years

**BANK DEPOSIT SLIPS**
**Official Copy: Treasurer**
**Retention:** 3 Years

**BANK STATEMENTS**
**Official Copy: Treasurer**
**Retention:** 7 years.

**CCLI PAPERWORK**
**Official Copy: Church Office**
**Retention:** 7 years

**EMPLOYERS LIABILITY INSURANCE**
**Official Copy: Church Office**
**Retention:** 20 years after the Policy has expired.

**INSURANCE POLICIES AND CLAIMS**
**Official Copy: Church Office**
**Retention:** 7 years after the Policy has expired.
**RISK ASSESSMENTS**
**Official Copy: Church Office**
**Retention:** 3 years.

**STAFF APPOINTMENTS/CONTRACTS**
**Official Copy: Church Office**
**Retention:** 2 years after appointment ceased or after unsuccessful application.

**STAFF HOLIDAY TIME**
**Official Copy: Church Office**
**Retention:** 2 years

**STAFF MONITORING/REVIEWS**
**Official Copy: Church Office**
**Retention:** 5 years

**STAFF TERMINATION**
**Official Copy: Church Office**
**Retention:** 6 years

**STAFF TRAINING AND DEVELOPMENT**
**Official Copy: Church Office**
**Retention:** For 7 years after staff have left their position.

**SECTION 4 - DATA DESTRUCTION**

The DPA 1998 is not prescriptive concerning the exact ways in which care needs to be taken of personal data.

This means that *The Village MCC* has to consider whether the measures we are taking comply with the intent of the Act.

The Act covers computer records, information held in manual files (e.g. index cards, filing systems etc), discs, CDs. The destruction of the data has to be carried out in such a way as to ensure that data from which individuals can be identified can't fall into the wrong hands. The Act specifically says that in deciding how far to go with this, we need to consider the level of technology available, together with the cost of using it, and the effect it would have on the data subject if the information was misused as a result of it falling into the wrong hands.

**Why is Data Destruction important?**
The responsibilities of organisations relating to confidential data have become more stringent since the implementation of the Data Protection Act 1998. Organisations must destroy under secure conditions any data containing personal information. Putting information in bins and hoping that it will be appropriately destroyed at a later date is not enough. If the church secretary.  is using a sub-contractor as their data processor, they must choose one who gives guarantees about security measures, takes reasonable steps to ensure compliance with those measures, and have a contract with the data processor. The church secretary.  is legally responsible for the data right up until the point of destruction, so it is important to get a certificate of destruction from the sub-contractor as proof that the process has been completed

An individual who suffers damage because of a contravention by the church secretary is entitled to compensation for that damage. Contravention of the Data Protection Act is a criminal offence carrying a maximum £5000 fine.

**Destruction of records: general principles**
Destruction of any record produced by *The Village MCC* in the course of its activities, including confidential records, should only be carried out where authorised. There may be legal, administrative or archival retention requirements. Provision of lists of categories of records destroyed and the authority under which they were destroyed will be a legal requirement under the Freedom of Information Act. (Please see Section 3) These requirements **do not,** however, apply to material routinely discarded in the course of an administrative activity i.e. duplicates, information material, rough drafts or ephemera.

**Destruction of records: confidential material**
Any record produced by *The Village MCC* which is not in the public domain and which contains information on identifiable individuals should be treated as confidential..Most confidential material is subject to the Data Protection Act. Under the Act the **individual** handling or processing confidential personal data is **personally responsible** for the proper disposal of such data.

**Data Protection Compliance checklist**
This is not part of the notification process but this short checklist will help us to comply with the Data Protection Act. Being able to answering every question correctly does not guarantee compliance, and we may need more advice in particular areas, but it should mean that we are heading in the right direction.

- Do we really need this information about an individual?
- Do we know what we are going to use it for?
- Do the people whose information we hold know that we’ve got it, and are they likely to understand what it will be used for?
- If we're asked to pass on personal information, would the people about whom we hold information expect us to do this?
- Are we satisfied that the information is being held securely, whether it’s on paper or on computer? And what about our website? Is it secure?
- Is access to personal information limited to those with a strict need to know?
- Are we sure the personal information is accurate and up to date?
- Do we delete or destroy personal information as soon as we have no more need for it?
- Have we trained our staff in their duties and responsibilities under the Data Protection Act, and are they putting these into practice?
- Do we need to notify the Information Commissioner, and if so is our notification up to date?

To help determine how well we comply with the data protection principles, please refer to the ‘Data protection audit manual’, www.ico.gov.uk