



DATA GOVERNANCE POLICY

River of Life Metropolitan Community Church Dorchester



**ADOPTED BY THE
BOARD OF TRUSTEES, ROLMCC 22nd July 09**

LIST OF CONTENTS

<u>Subject</u>	Page
Introduction including scope of document	3
Terms	3
Responsibilities of Staff	4
Breaches of Policy	4
Confidential and non confidential records	4
Registration with ICO	5
Data Protection	7
Data Security	8
Data Retention	10
Data Destruction	13
Compliance Checklist	15

INTRODUCTION

The volunteers and paid staff who process, or use personal data must ensure that they abide by the principles outlined in this document at all times. This policy has been developed to ensure that the Data Protection/Retention/Disposal/Storage Laws are adhered to.

TERMS

ROLMCC – For the purpose of this document River of Life Metropolitan Community Church will be referred to as ROLMCC.

Personal information means information which relates to a living individual who can be identified from that information. It is also any other information which is in the data controller's possession, or that is likely to come into their possession.

Processing means obtaining, recording or holding the data or carrying out any operation or set of operations on that data. Processing includes the following activities: organising, adapting, amending, retrieving, consulting, using, disclosing, erasing, destroying, storing.

Data Subject is the individual to whom the information pertains.

Data Controller is the individual or body of individuals who are responsible implanting this policy; in the case of River of Life it is the **Board of Trustees**.

Data Class is the type of information held about a Subject

SCOPE OF DOCUMENT

This document outlines and specifies the responsibilities of the Trustees to ensure that ROLMCC follows legislative guides and law in respect of personal data and the data owned by ROLMCC needed to continue its activities as a church.

This document will cover areas of Data Protection, Data Security, Data Retention, Data Destruction.

RESPONSIBILITIES OF STAFF

It is the responsibility of the Data Controller to:

- Assess the understanding of the obligations of ROLMCC under the Data Protection Act
- Be aware of ROLMCC's current compliance status
- Identify and monitor problem areas and risks and recommend solutions
- Promote clear and effective procedures and offer guidance to staff on Data protection issues. It is anticipated that this will include familiarisation with the Act starting at the induction process followed by training programmes/seminars, annual appraisals and intranet/internet resources.

It is NOT the responsibility of the Data Controller to:

- apply the provisions of the Data Protection Act. This is the responsibility of the individual collectors, keepers and users of personal data. Therefore staff are required to be aware of the provisions of the Data Protection Act, such as keeping records up to date and accurate, and its impact on the work they undertake on behalf of ROLMCC.

BREACH OF THIS POLICY

Any breach of the Data Protection Policy, whether deliberate, or through negligence may lead to disciplinary action being taken or even a criminal prosecution.

CONFIDENTIAL AND NON-CONFIDENTIAL RECORDS

What *is not* confidential

Any record or copy thereof which is already in the public domain e.g.

Mission statements

Charters

Constitutions

Ordinances

Statutes

Regulations

Published directories

Internet websites

Published minutes

Published reports

Press releases

Timetables

Presentation materials

Publicity material

Data which has been made anonymous

Published surveys

Magazines

Published circulars

What *is* confidential

Any record which contains personal information about a living individual e.g.

Questionnaire or other data collected under a guarantee of confidentiality.

Correspondence or other documents which reveal the contact details or any financial details of a named living person, unless permission has been given to circulate the details.

Correspondence or other documents which reveal personal details or pass comments on a named living person.

Staff personnel records

Discipline records

Grant applications

Job applications

Interview notes

Admissions records

Sick pay records

Wages and salary records

Accident books and records

Health records

Medical records

Any record which, if made public before a certain period, may breach commercial confidentiality e.g.

Contracts

Tenders

Purchasing records

Maintenance records

Insurance records

Unpublished accounting records

Any record which may breach intellectual property rights e.g.

Unpublished research material, drafts and manuscripts.

REGISTRATION WITH INFORMATION COMMISSIONERS OFFICE

ROLMCC does not need to register with the Information Commissioners Office (I.C.O.) due to the nature of its activities as a church and as a registered charity provided that:

- Our processing is only for the purposes of establishing or maintaining membership or support for a body or association not established or conducted for profit, or providing or administering activities for individuals who are either members of the body or association or have regular contact with it.
- Our data subjects are restricted to the processing of those for whom personal information is necessary for this exempt purpose.
- Our data classes are restricted to personal information that is necessary for this exempt purpose.
- Any disclosures other than those made with the consent of the data

subject are restricted to those third parties that are necessary for this exempt purpose.

- The personal information is not kept after the relationship between ROLMCC and the data subject ends, unless (and for so long as) it is necessary to do so for the exempt purpose e.g.; to comply with Retention time for Financial Records for HMRC, Companies House or the Charities Commission.

Therefore all information gathered will be kept under these guidelines.

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

ROLMCC must not contact individuals without their prior consent unless they have indicated an interest in ROLMCC 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 are responsible for ensuring that:

- Any personal data they hold, whether in electronic or paper format, is kept securely.
- 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 Data Controller.
- The Data Controller aims to comply with requests for access to personal information as quickly as possible, but must comply with all access to records requests within forty days of receipt of the request, or if later, within forty days of the receipt of the identity information required

Subject Consents

- The need to process data for normal purposes will be communicated to all staff. In some cases, if the data 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 ROLMCC 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 Data Controller under the Data Protection Act 1998).

ROLMCC 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.

To facilitate this it is recommended that all electronic data is stored on a file server and backed up without user intervention to a secure cloud storage system. The security model on the server such as with Windows Server 2003 or higher would provide familiar processing and familiar applications to all users.

Accessing the server – with passwords

Users may access the system via remote access terminals (on their own PC's or Laptops) which enables them to run a session on the server to access all the programs and data they require or need, without holding ANY data on their own computers whatsoever.

A strict access security model will be applied using proper login and password access to different areas of ROLMCC ministries. These will be set in consultation with the Web Manager and the Data Controller. This will ensure access is only gained to the relevant information for each person.

Upon a person leaving a position in ministry, the password will immediately be

changed to ensure further security.

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 to the server, or kept on a laptop.

USB Sticks

USB sticks have to be authorised for use with ROLMCC data and must be encrypted.

Email addresses

No identifying emails for Data Subjects to kept on any personal computers, merely on server.

Paperwork

All paperwork containing personal data shall be stored securely.

SECTION 3 - DATA RETENTION

Summary

ROLMCC 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 ROLMCC 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 Archives on regular basis.

Other copies used in office
Retention: 3 years.

ASSET LIST

Official Copy: Church Office
Retention: permanent

ATTENDANCE SHEETS

As soon as they are entered on to the SAGE System, they are to be shredded.

AUDIT RECORDS

Official Copy: Treasurer and Church Office
Retention: Permanent
Send official copy to Archives on regular basis

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

CONTACT SHEETS

As soon as they are entered on to the SAGE System, they are to be shredded.

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 LEAVE

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: 7 years

EXCEPT IN THE CASE OF RELATION TO CHILD PROTECTION

Official Copy: Church Office

Retention: 35 years

EXCEPT IN THE CASE OF HEALTH AND SAFETY

Official Copy: Church Office

Retention: 50 years – This does not relate to course work – merely results.

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 ROLMCC have 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 data controller 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 data controller 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 data controller is entitled to compensation for that damage

Contravention of the Data Protection Act is a criminal offence carrying a maximum £5000 fine. The trend is for prosecutions to be on the increase

Destruction of records: general principles

- Destruction of any record produced by ROLMCC 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 ROLMCC 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.

YES NO Do we really need this information about an individual?

YES NO Do we know what we are going to use it for?

YES NO 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?

YES NO If we're asked to pass on personal information, would the people about whom we hold information expect us to do this?

YES NO 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?

YES NO Is access to personal information limited to those with a strict need to know?

YES NO Are we sure the personal information is accurate and up to date?

YES NO Do we delete or destroy personal information as soon as we have no more need for it?

YES NO Have we trained our staff in their duties and responsibilities under the Data Protection Act, and are they putting these into practice?

YES NO 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