Magdalen Road Church
Delighting in God, Displaying His Glory

Data Protection policy

Magdalen Road Church (MRC) is committed to following the principles of the UK Data Protection Act and to keeping the principles outlined in it. In particular, MRC seeks to ensure that the personal data it holds is:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept for longer than is necessary
6. Processed in line with an individual's rights
7. Kept securely
8. Not transferred to other countries without adequate protection

The Act applies to personal data stored in computer systems or structured filing systems, but the principles can be applied to all personal data that MRC holds in whatever form. The details of how these aims are achieved is worked out in the paragraphs below.

1) Registration

MRC considers that it is exempt from registration under the Data Protection Act.

2) Data subjects

'Personal data' means information about a living individual who can be identified from that information and other information which is in, or likely to be in, MRC's possession.

MRC primarily holds personal data on:

a) Staff, including former members of staff and potential new staff.
b) Supporters including those who have identified that they wish to be considered as members of MRC

This list is not exhaustive – for example, MRC may also hold data on referees, family of friends of the above.

MRC also holds data on different supporting organisations, churches and trusts. Some of this data is not personal data – for example, the minister of a church is a matter of public record - and some data is effectively in the public domain but this does not necessarily reduce the responsibility to keep the requirements of the Data Protection act.

3) Good practice

a) Ensuring data is fairly and lawfully processed

Processing data has a wide meaning in the context of data protection and refers to any action involving personal information, including obtaining, adding, storing, viewing, copying, amending, extracting, deleting, disclosing or destroying information. MRC will ensure that the data it holds is processed fairly. The main test for this will be the subject's permission and expectation, i.e. will MRC staff and supporters feel this is a proper use of the information that is held?

Where possible, MRC will be explicit about this by explaining what use the information supplied will be put to for example,

- *We will use this information to keep you informed of MRC activities*
- *The information on this form will only be used to consider your application* (Application form for church membership)
- *Your email address will be used to send you e-pray each week and will not be passed on to anyone outside MRC* (Website)

Sensitive Information

Information about a person's physical or mental health, ethnicity or race, political or religious views, sexual life, or criminal record is sensitive information under the Act. Such information can only be collected and processed as required by law, e.g., by the Children's Act 1989, or with the subject's express (written) consent. One example in this area would be a sick note supplied as part of the absence procedure. Sensitive information must be protected with a higher level of security. It is recommended that sensitive records are kept separately in a locked drawer or filing cabinet, or in a password-protected computer file – see also below for general recommendations concerning security.

b) Ensuring data is processed for limited purposes, in line with an individual's rights and that the data held is adequate, relevant and not excessive

In order to be able to monitor and control what data is held and to meet the requirements of this principle, MRC very much encourages the holding of personal data within defined IT systems and databases. Currently these are:

- Church Insight (church attenders management database)
- Central Desktop (no sensitive information is held here)
- Finance Co-ordinator accounts system

Before designing sources for data capture, such as paper forms, response slips or web pages, the designer should review with staff each item captured to assess if it is relevant and how this information will be stored.

Personal data kept on a laptop then this data **must** be stored in the encrypted partition of the laptop drive. (see also part 3-iv below – Security of data in transit)

Personal contact data will not be passed to other organisations without the person's explicit permission or instruction.

c) Ensuring data is accurate and up to date

Keeping data accurate and up to date is a difficult and ongoing task. MRC will make every effort to do this such as:

- Processing all returned mail to update the supporters database.
- Updating the records when advised of changes in direct debit instructions.
- Updating personnel records when advised of staff changes.

Officers and members of staff in MRC are encouraged to regularly review the personal data they hold for accuracy and develop procedures in this area to ensure compliance.

d) Ensure data is not kept for longer than is necessary

MRC will continue to develop policies of securely destroying personal data when it is no longer needed. MRC currently destroy:

- Unsuccessful job applications 3 months after the due date
- Applications for church membership 1 year after initial acceptance

- Any documentation relating to pastoral issues 6 months after they are created.

'Securely destroying' usually means the shredding of paper copies of data and the deletion of computer files, emails and database entries. When a computer is disposed of, computer hard drives **must** be cleaned with a "zero fill" secure deletion process or be physically destroyed before being removed from the building. Data which is held on CD's must be physically destroyed when it is no longer needed.

Officers and members of staff within MRC are encouraged to monitor the accumulation of personal data held and develop procedures in this area to ensure compliance.

e) Ensure data is kept securely

i) Physical security

The physical security of Magdalen Road Church is an important part of keeping data secure. Because of the level of public use of the building, all personal data **must** be stored in the office which must be locked when not in use.

Staff **must** ensure that all paperwork containing personal data is removed from their desks at the end of a working day. It is recommended that sensitive records be kept separately in a locked drawer or filing cabinet.

In addition bank account details are treated as sensitive and these are only held by the Church Treasurer in hard copy in a locked filing cabinet.

It is essential that all sensitive hard-copy material is transferred hand-to-hand. It should never be left in a folder for a person to pick up when convenient.

ii) Network security

All personal data stored on a computer must be protected by a robust username and password for access. Passwords should be sufficiently complex and regularly changed. Staff **must not** share network usernames and passwords. Passwords for any computer system should not be written down on paper.

iii) Backups

The holders of personal data should ensure that a regular backup process takes place and that a copy of the most essential data is stored off-site in a safe.

iv) Security of data in transit

When personal data needs to be transferred to other parties, care must be taken to ensure that the data cannot be accidentally disclosed to unauthorised recipients. Secure methods of data transfer need to considered in all cases - preferences should be given to methods that ensure the data is encrypted such as secure ftp or SSL connections.

If encrypted transfer is not possible, personal data must at least be password protected.

Email is not a secure way of transferring personal data, as potentially an email can be read at any intermediate server. . If personal data is sent by email it is recommended that the files be encrypted and password protected before being emailed.

USB data sticks represent a very high risk area for the security of data, because they are so easily lost. Personal data **must not** be stored on personal data sticks belonging to officers or members of staff.

Laptops also represent a high risk area. If personal data needs to be kept on a laptop then this data **must** be stored in the encrypted partition of the laptop drive.

v) Home and remote working

When working from home or other locations outside the office, staff **must** maintain appropriate levels of security, including physical security of printed material and data.

Special care should be taken in the transport of personal information to and from home. Physical data media containing personal information – paperwork and CDs – should preferably be kept in a locked briefcase and laptops should not be left unattended in public places.

vi) Guarding against disclosure

All staff should ensure that personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party. Unauthorised disclosure may be a disciplinary matter, and may be considered gross misconduct in some cases.

4) Training

a) Staff

As part of the induction process, each member of staff will receive basic awareness training in the data protection act. This session will cover the principles outlined above and will also address particular issues that they may have within their job description.

b) Volunteers

Volunteers who work with personal data will be given the opportunity to attend staff induction sessions. They will also receive a written briefing which will address the particular issues they are involved with – See Appendix A

5) Right to access information

Staff, supporters, and other data subjects have the right to access any personal data that is being kept about them by MRC either on computer or in structured and accessible manual files. Any person may exercise this right by submitting a request in writing to the church office. MRC is entitled to make a charge of £10 for each official subject access request under the data protection act – this charge will be waived in the case of supporters. MRC aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days unless there is good reason for delay. In such cases, the Elders will explain the reason for the delay in writing to the data subject making the request.

Under certain circumstances, MRC may disclose personal information to the police and other law-enforcement bodies. MRC will do this only if it considers the request reasonable and proportionate.

6) Compliance

Compliance with the Data Protection Act and with this policy is the responsibility of all members of staff and any volunteers who have been entrusted with personal data. Any deliberate or reckless breach of this policy may lead to disciplinary, and where appropriate, legal proceedings. Any questions or concerns about the interpretation or operation of this policy should be taken up with Elders in the first instance.

February 2009

Appendix A – Advice to Volunteers

Magdalen Road Church is committed to following the principles of the UK Data Protection Act and to keeping the principles outlined in it. In particular, we seek to ensure that the personal data we hold is:

1) Fairly and lawfully processed
2) Processed for limited purposes
3) Adequate, relevant and not excessive
4) Accurate and up to date
5) Not kept for longer than is necessary
6) Processed in line with an individual's rights
7) Kept securely
8) Not transferred to other countries without adequate protection

The Act applies to personal data stored in computer systems or structured filing systems, but the principles can be applied to all personal data that we hold in whatever form. We work out some of the details of how we achieve these aims in our Data Protection policy. MRC considers that it is exempt from registration under the Data Protection Act but is committed to the principles of the Act.

As a volunteer working for MRC, you are required to follow the same procedures as staff in the handling and processing of data. If you are in doubt, please ask to see the entire data protection policy and ask for further advice.

The main issues that may arise will be:

1) Ensure data is kept securely

a) Please make sure that the data you have been given is kept securely, whether in paper or electronic form. If travelling by public transport, keep them within your other luggage as you travel so that there is no risk of items being left on a train, or similar.

b) USB data sticks are notoriously easy to lose. Please do not transfer personal data to these data sticks, unless they are encrypted.

c) When working from home, you **must** maintain appropriate levels of security, including physical security of printed material and data.

2) **Ensuring data is processed for limited purposes, in line with an individual's rights and that the data held is adequate, relevant and not excessive**

Please ensure that the data you have been given is only used for the purpose intended and is not given to or shared with anyone else. The data must be destroyed/deleted once it is no longer needed for that purpose.