Data Protection Policy

Version 2016.2

M J Church holds and processes information about its employees, clients, and other individuals for various purposes (for example, the effective provision of healthcare services, to operate the payroll, and to enable correspondence and communications).

To comply with the Data Protection Act 1998 (DPA), information must be collected and used fairly, stored safely securely disposed of, and not disclosed to any unauthorised person. This act outlines the law relating to the processing of the data on identifiable living people. It governs the protection and use of personal data in the UK. The definition of personnel data is any data which can be used to identify a living individual such as name, address, telephone number and email address. The DPA applies to both manual and electronically held data.

The policy applies to all personal information in the company. Non-compliance with this policy may result in disciplinary action.

Scope of this Policy
This policy covers all records held and processed by the company. The company is responsible for its own records under the terms of the DPA, and it has submitted a notification as a Data Controller to the Information Commissioner - Registration Ref: ZA207874

Policy Aims
The lawful and correct treatment of personal information is vital to the successful operation of, and maintaining confidence within the company, and the individuals with whom it deals.

Therefore, the company will, through appropriate management, and strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information;
- Meet its legal obligations to specify the purposes for which information is used;
- Collect and process appropriate information, and only to the extent that it is needed to fulfill operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;
- Ensure that the rights of people about whom information is held can be fully exercised under the Act. (These include: the right to be informed that processing is being undertaken; the right of access to one's personal information; the right to prevent processing in certain circumstances; the right to correct, rectify, block or erase information which is shown to be inaccurate information.);
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards.

The Information Commissioner
The company has an obligation to protect and secure the integrity and possession of the data it holds. It has an obligation as a Data Controller to notify the Information Commissioner of the purposes for which it processes personal data.

Notification monitoring within the company is carried out by the Information Technology Department

Individual data subjects can obtain full details of the company's data protection registration/notification with the Information Commissioner from the Information Technology Manager or from the Information Commissioner's website (ico.org.uk).

Data Protection Principles

The company, as a Data Controller, must comply with the eight Data Protection Principles set out in the Data Protection Act 1998. In summary, these state that personal data shall:

• Be processed fairly and lawfully and shall not be processed unless certain conditions are met;
• Be obtained for specified and lawful purposes and shall not be processed in any manner incompatible with those purposes;
• Be adequate, relevant and not excessive for those purposes;
• Be accurate and kept up to date;
• Not be kept for longer than is necessary for those purposes;
• Be processed in accordance with the data subject's rights under the 1998 Act;
• Be the subject of appropriate technical and organisational measures against unauthorised or unlawful processing, accidental loss or destruction;
• Not be transferred to a country outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Privacy Notices
Sometimes called a Fair Processing Notice, any collection of personal data must satisfy the requirements of the fair processing condition set out in the first Data Protection Principle.

This includes paper or electronic application forms, telephone calls, and surveys.
M J Church will ensure an appropriate Privacy Notice is included wherever personal data is collected.

This particularly applies to client consent forms: it may be that current forms need to be amended to include a statement about data protection.

The purpose of a Privacy Notice is to explain to the individual:

- The identity of the organisation collecting his or her data;
- How the personal information which is provided will be used;
- Any other information which the individual should be told in order to ensure the processing of his or her information is fair, for example: A description of any other organisations the information may be shared with or disclosed to; whether the information will be transferred outside the UK;
- The fact that the individual can object to the use of his or her information for marketing;
- The fact that an individual can obtain a copy of his or her information.

M J Church will ensure that the Privacy Notice is in a prominent position whenever used.
An example form of words for a Privacy Notice might be:

Your personal data will be used only in accordance with the M J Church notification under the Data Protection Act 1998. The company will not disclose any personal information to any other third parties, without your express consent except where there is a legal justification or required by law.

Responsibilities of Individual Data Users

All employees and Members of the company who record and/or process personal data in any form (called "Data Users" in this policy) must ensure that they comply with:

- The requirements of the Data Protection Act 1998 (including the Data Protection Principles);
- The company's Data Protection Policy, including any procedures and guidelines which may be issued from time to time.

A breach of the Data Protection Act and/or the company's Data Protection Policy may result in disciplinary action.

Consideration should be given towards contacting the IT Department for data protection advice concerning the following:

- When developing a new computer system for processing personal information;
- When using an existing computer system to process personal data for a new;
- When creating a new manual filing system containing personal data;
- When using an existing manual filing system containing personal data for a new purpose.

Localisation of Data

M J Church data will be required to ensure that the data it holds will be stored on servers in countries within the EU or UK following its exit from the EU. M J Church holds most of its data on its own servers within the UK.

Contractors and Data Processors

Outside agents working with M J Church data will be required to ensure full data compliance in accordance with contractual arrangements.

Any external data processors will have to prove to the company that they are fully aware of all aspects of data protection, that they are registered with the Information Commissioners Office and that their registration is currently valid. Copies of their registration will be kept and asked for when the next renewal date becomes due.

M J Church reserves the right to inspect contractors and Data processors to satisfy these requirements.

Accuracy of Data

Staff that have responsibility for handling any client, staff or other individual's information must ensure that it is accurate and as up to date as possible.

All staff members are responsible for checking that any personal information they provide to the company in connection with their employment is accurate and up to date e.g. change of address or name.

The company cannot be held responsible for any errors unless the member of staff has informed the company about them.

Sensitive Personal Data

a) The company will process "sensitive personal data" relating to staff, clients, contractors and other individuals. This sensitive personal data may include information which has incidentally come into the possession of the company. This type of information will not be routinely sought by the company.

b) In exceptional circumstances, the company may need to process information regarding criminal convictions or alleged offences in connection, for example, with any disciplinary proceedings or other legal obligations.

c) In circumstances where sensitive personal data is to be held or processed, the company will seek the explicit consent of the individual in question unless one of the limited exemptions provided in the Data Protection Act 1998 applies (such as to perform a legal duty regarding employees or to protect the data subject's or a third party's vital interests).

Data Security and Disclosure

All staffs within the company are responsible for ensuring that any personal data which they hold is kept securely, and that personal data is not disclosed either orally or in writing or otherwise to any unauthorised third party, and that every reasonable effort will be made to see that data is not disclosed accidentally.

Unauthorised disclosure is a disciplinary matter and may be considered gross misconduct. If in any doubt, consult the Information Technology Department or Human Resources. Personal data must be kept securely and examples of how this may be done will include:

Keeping the data locked in a filing cabinet, drawer or room; or if the data is computerised, ensuring that the data is password protected or kept on a secure network and only where necessary as a temporary measure on secure removable media

Any other appropriate security measures which are detailed in the company IT Security Policy.

Information Sharing Agreements will be required to facilitate regular and routine sharing of personal information with external organisations and partner agencies. All other information sharing will need to be justified in accordance with the data protection principles and documented.

Data Subjects' Consent

Where appropriate the company will seek consent from data subjects to process their personal information.

Right of Access to Personal Data

All individuals have the right under the DPA to access any personal data that is being held about them. They also have the right to request the correction of such data where they are incorrect.

CCTV

A number of CCTV cameras are present on the company sites, to assist with security for staff, other individuals and their property, and in accordance with the company's 'notification' to the Information Commissioner.

Disclosure of images from the CCTV system will be controlled and consistent with the purpose for which the system was established. For example, it will be appropriate to disclose images to law enforcement agencies where a crime needs to be investigated, but it would not be considered appropriate to disclose images of identifiable individuals to the media for entertainment purposes or place them on the internet.

Images can be released to the media for identification purposes; this should not generally be done by anyone other than a law enforcement agency.

If you have any queries regarding the operation of or access to the CCTV system, please contact the IT Department.

If access is required in connection with ongoing disciplinary matters, permission should be sought from the Head of Human Resources or nominated deputy.

Email
It is permissible and appropriate for the company to keep records of internal communications, provided such records comply with the Data Protection Principles.
All company staff should be aware that the DPA subject access right, subject to certain exceptions, applies to emails which contain personal data about individuals which are sent or received by company staff.

Retention of Data
The company will hold different types of information for differing lengths of time, depending on legal and operational requirements, following which it will either be archived or destroyed.
All data retention will comply with the 5th Principle of the Data Protection Act 1998.

Disposal of IT Equipment and Information
Should the company need to dispose of redundant IT equipment it will do so in a responsible manner and in agreement with its Secure Disposal of IT Equipment and Information Policy.

Training
All staff will receive mandatory training on data security, data principles, and general compliance with the DPA. This training will be repeated at regular intervals and tailored to meet different needs of the various company service areas.

For & on behalf of MJ Church

Steve Blower

Managing Director

Last reviewed: July 2017