Data Handling Policy

Version 2016.2

M J Church holds and processes information about its employees, clients, and other individuals for various purposes (for example, to operate the payroll, and to enable correspondence and communications). This policy provides guidance on how data must be stored and processed within the company.

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.

Non-compliance with this policy may result in disciplinary action.

The M J Church computer network is the property of the company. Employees should have no expectations of privacy in anything they create, store, send or receive using the company's computer equipment or any other equipment connected to the network. The company has the right to monitor any and all aspects of the network, including all internet sites visited by employees, file downloads and all communications sent and received by users.

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.

The handling of all information held by the company is important to maintain the security and integrity of the information it holds.

This policy applies to all employees, contractors and consultants who handle data whether via a computer, mobile phone, PDA (personal digital assistant) handheld machine or paper records. It applies to all connections made to the M J Church network whether at the company's premises or elsewhere.

Users must also be aware of the responsibilities and liabilities for personal communications and the consequences of their actions with regards to privacy and security issues.

All electronic data held by M J Church is held on servers within the EU.

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.

The confidentiality and integrity of records can only be maintained by applying strict controls on how information is handled within the company.

Statement of Policy
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 DPA.;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards
- Keep all data, whether electronic or paper based, stored securely,
- Apply such measures as necessary to prevent unlawful access to information by the use of firewalls, anti-virus software, penetration testing of our network (both externally and internally) and to dispose of redundant IT hardware and software appropriately to remove any data beforehand;
- Ensure all servers and network equipment are locked in secure rooms;
- Protect material produced under copyright law

Policy Details

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.

All MJC staff must ensure that:

- They have read and comply with the MJC Data Protection Policy – This policy outlines the requirements of staff to ensure that personal data is handled appropriately and is compliant with the Data Protection Act (1998).
- They have read and comply with the MJC Network Access Policy – This policy outlines the requirements of staff to ensure secure access to the M J Church network is maintained.
- They have read and comply with the MJC Secure Disposal of IT Equipment and Information Policy

In addition all MJC staff must ensure that they abide by the following:

<u>Storage devices</u>

- The use of personally owned USB memory sticks is strictly **forbidden**. This also includes any other form of personally owned removable media. This includes but is not restricted to personal cameras, phones, CDs and DVDs. Non-compliance may result in disciplinary action being taken.
- USB memory sticks that are issued by the IT department may be used but should never be used for long term storage.
- The use of any removable media issued to M J Church by a customer or client for use in the normal operational use of a contract is permitted. However on every occasion that removable media is received by an office it must be virus checked before being attached to any part of the M J Church IT network.

Personal Use

- Employees may access their personal email accounts during official breaks. However the code of conduct relating to emailing (see below) also applies to personal emails sent during working hours.
- Employees may access the internet for personal use during official breaks. However the code of conduct relating to internet use (see below) also applies to personal internet use during working hours.
- Employees may **not** illegally copy material protected under copyright law or make the material available to others for copying.
- In times of high demand for network bandwidth employees should refrain from using the internet for personal use.

Code of conduct relating to Emailing

- Employees may **not** send by email or any other electronic means any material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating defamatory or otherwise inappropriate.
- Employees may **not** send by email any credit, debit or payment card data relating to anyone.
- Employees may **not** send by email or disclose by any other means proprietary information, data, trade secrets or other information belonging to M J Church or its customers, suppliers or contractors.
- Employees may **not** send by email or any other means information which criticises M J Church or otherwise brings the company into disrepute. If an employee is dissatisfied with some aspect of their employment this should be addressed using the company's grievance procedure.
- Non-compliance with any of the above **will** result in disciplinary action
- 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.
- M J Church reserve the right to monitor email use over its network.

Code of conduct relating to Internet and social media use

- Employees may **not** access any inappropriate web site during working hours or on any computer belonging to M J Church.
- The M J Church computer network may **not** be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive code (i.e. viruses), political material, pornographic text or images or any other unauthorized material at any time.
- Employees may **not** send blogs or via social media information which criticises M J Church or otherwise brings the company into disrepute. If an employee is dissatisfied with some aspect of their employment this should be addressed using the company's grievance procedure.
- Non-compliance with any of the above **will** result in disciplinary action.
- Copyright rules apply to articles on the internet. Copying, electronically or by other means, of such material is prohibited.
- M J Church reserve the right to monitor internet use over its network.
- Assume that everything which you write on social media sites can be traced back to you personally as well as colleagues, customers and suppliers.

Rules relating to the use of the internet also apply to that of any company intranet.

M J Church company websites

- No employee shall add or amend any information on any company website without the permission of a Director.

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 IT 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

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.

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.

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.

Training

All staff will receive mandatory training on this policy.

For & on behalf of MJ Church

Steve Blower

Managing Director

Last reviewed: July 2017