



Secure Disposal of IT Equipment and Information Policy

Version 2016.1

In the course of its operations M J Church will need to dispose of redundant IT equipment and information. It will undertake this task in a responsible manner to comply with its obligations with the Data Protection Act 1998 (DPA) and that of the EU Waste Electrical and Electronic Equipment (WEEE) directive and the UK Waste Electrical and Electronic Equipment Regulations 2006. Copyright software will be disposed of in line with copyright legislation and software licensing provisions.

Scope of this Policy

Disposal means the process by which IT equipment and the information held on the equipment is irretrievably destroyed. The IT equipment will include but not limited to servers, computers (desktop, laptop, tablet and notebook), printers, photocopiers, firewalls, scanners, cameras, digital recorders, mobile phones, USB storage devices, DVDs, CDs and other portable and removable media and devices. Information means all information and data held whether recorded electronically or on paper.

Information can be classified as either sensitive or nonsensitive. Sensitive information comprises of confidential personal information. For the purposes of this policy all information will be treated as sensitive unless specifically identified as otherwise.

This policy sets out the requirements for all staff for the secure disposal of M J Church equipment and information.

Responsibilities

The DPA applies to both manual and electronically held data.

The IT department will be responsible for the disposal of all IT hardware and software. All such redundant items should be identified and the IT department notified immediately. If the items are unable to be immediately collected then they should be stored securely. The items will be collected and disposed of accordingly by the IT department. When disposing of IT equipment all IT department staff must be mindful of the WEEE regulations.

Any unwanted manually held information recorded on paper should be disposed of by shredding.

It is the responsibility of all M J Church staff to ensure that information is disposed of appropriately and that all sensitive information is disposed of securely.

All line managers should report any breach of this policy to the Operations Director or other Director if not available. Failure to comply with this policy may result in disciplinary action being taken.

Statement of Policy

This policy on disposal covers all data or information held by M J Church whether held digitally, electronically, on IT equipment or as manual records held on paper or in hard copy.

It is the policy of M J Church that all information held by M J Church, whether sensitive or not, is disposed of securely.

IT equipment must be disposed of in line with the EU Waste Electrical and Electronic Equipment (WEEE) directive and the UK Waste Electrical and Electronic Regulations 2006

Policy Details

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.

IT Equipment disposal:

- All IT equipment awaiting disposal must be stored and handled securely;
- Where the physical destruction of IT equipment is to be carried out on behalf of M J Church by a third party there must be a contract with that party outlining:
 - its obligations to keep the data secure
 - its obligations under the Data Protection Act 1998 for the secure disposal of the data
- It is assumed that all printers and photocopiers owned or used by M J Church may have a data storage capacity and therefore disposal of this equipment must be done in accordance with this policy
- M J Church does not sanction the use of external cloud services for the storage of data where there is no contract in place. Contracts must be in place before instigating the use of any cloud storage service. If in doubt contact the IT department.
- Removable digital media including but not limited to CDs, DVDs, USB storage devices will be by default considered that they hold sensitive data. These devices will be physically destroyed.

Hard copy and paper based information:

- Sensitive information held in paper or hard copy will be destroyed by shredding, pulping or incineration. This process will be carried out securely.
- A contract will be in place if the destruction of sensitive paper or hard copy information is to be carried out by a third party. The contract will appropriately evidence that:
 - the third party's obligation to keep the data secure and confidential
 - the party's responsibility under the Data Protection Act (1998)
- If the information is stored by an external data storage contractor then the contract with this contractor shall ensure:
 - the third party's obligation to keep the data secure and confidential
 - the contractor's responsibility under the Data Protection Act (1998)
 - the disposal of the information at a time which conforms to the requirements set by M J Church

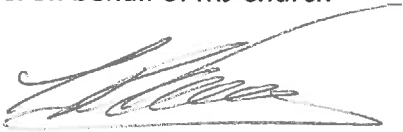
Record of Destruction

M J Church will ensure that records are kept of the method and outcome of the disposal process

Note to all staff

Forensic computer analysts and IT specialists may still be able to successfully reconstruct data from devices which users have deleted data from. Data should be irretrievably destroyed by being over written in accordance with the appropriate industry standard or the hard disk removed and physically destroyed.

For & on behalf of MJ Church

A handwritten signature in black ink, appearing to read 'Steve Blower', with a long horizontal flourish extending to the right.

Steve Blower
Managing Director

Last reviewed: July 2017