Melton Mowbray Baptist Church

Leicester Road, Melton Mowbray, Leicestershire, LE13 0FA

Church Office: 01664 480786 Email: office@mmbc.org.uk Web: www.mmbc.org.uk

IT POLICY

Version 1.1

Prepared by	GDPR Working Group: N Ashton, A Thomas, P Appleby, R Nicholls
Leadership Approved	Leaders Meeting:
Operational Date	Adopted at Church Meeting – 17th May 2018
Review Date	12 months from adoption

Minister: Rev. Dr. Nick Ashton DipTh, BSc(Hons), MTh

Office Telephone: 01664 567529 Email: nick@mmbc.org.uk

Melton Mowbray Baptist Church is committed to protecting all personal and sensitive data for which it holds responsibility as Data Controller about people we support and work with, and to respecting people's rights around how their information is handled.

This policy explains how we will meet our responsibilities towards data in using IT.

This policy needs to be read in conjunction with other key polices such as:

- *The MMBC Internet Usage Policy*
- *The MMBC IT Policy*
- *The MMBC Social Media Policy*
- *The MMBC Safeguarding Policy*
- *The ICO Cloud Computing Guidance*
- *The ICO Data Sharing Code of Practice*
- *The ICO Privacy Impact Assessment Code of Practice*
- *The BUGB Data Protection Leaflet (revised 2017).*

Throughout this policy, Melton Mowbray Baptist Church is referred to as MMBC and Trustees refers to currently appointed and serving Leaders.

Terms	***Definition***
SHALL / SHOULD / SHOULD NOT	*This term is used to state a **Recommended** requirement of this policy*
MAY / MAY NOT	*This term is used to state an **Optional** requirement*

Contents

Section A – What This Policy Is For

1. Policy Statement

1.1 MMBC is committed to protecting personal data as securely as possible by complying with all relevant laws and adopting good practice in managing and storing data.

MMBC uses both paid staff and volunteers to carry out its business and this policy sets out the use of IT equipment to be followed by any data processor or data controller acting on behalf of MMBC whether paid or not.

1.1 This policy has been approved by the church's Trustees who are responsible for ensuring that we comply with all our legal obligations.

2. Why This Policy is Important

2.1 MMBC are committed to protecting personal data from being misused or getting into the wrong hands as we are aware that people can be upset or harmed if any of these things happen.

2.2 This policy sets out the measures we are committed to taking as an organisation and, what we will do to ensure we comply with the relevant legislation.

3. How This Policy Applies To You And What You Need To Know

3.1 **As an MMBC appointed representative** processing personal information on behalf of the church, you **shall** comply with this policy. If you think that you have accidentally breached the policy it is important that you contact the Trustees immediately who **shall** take swift action to try and limit the impact of the breach. The Trustees are by default the currently appointed Leaders.

Anyone who breaches the IT Policy may be subject to disciplinary action, and where that individual has breached the policy intentionally, recklessly, or for personal benefit they may also be liable to prosecution or to regulatory action.

3.2 Before you collect or handle any personal data as part of your work (paid or otherwise) for MMBC, it is important that you **shall** take the time to read this policy carefully and understand what is required of you, as well as the organisation's responsibilities when we process data.

3.3 Our procedures **shall** be in line with the requirements of this policy, but if you are unsure about whether anything you plan to do, or are currently doing, might breach this policy you must first speak to any Trustee.

4. Training and Guidance

4.1 We **shall** aim to provide general IT training for all staff and volunteers who request it in order to up-skill and be competent in abiding by this policy.

4.2 We **may** also issue procedures, guidance or instructions from time to time. Trustees **shall** also set aside time to review IT procedures as issues arise.

Section B – Our IT Responsibilities

1. Confidential Data and Security

1.1 We **shall** suggest optimum methods of working to maximise the security of personal data. Some things **shall** be expected, others **may** be optional.

For example:

- Home router security
- Emails and attachments
- Removable media and mobile devices
- Password protecting files
- Broadcasting personal data
- Computer/device protection
- Strong passwords
- Cloud storage
- Data retention and methods of disposal
- Data transfer and encryption
- Backup and Recovery
- Securing home router
- Software
- Incident reporting procedures

2. Specific Security Suggestions

2.1 E-Mails

- Groups and/or individuals within MMBC may hold contact lists
- It is expected you **should** use BCC not CC to protect other people's email address

2.2 Removable Media & Mobile Devices

- You **should** reduce the risk of data loss by password protecting MMBC files stored on removable media, whether short term or long term, using different passwords for each
- Where your device allows, eg phone, tablet, you **should** use the pin-code/password feature to access the device and you **should not** disable in settings
- Where your device allows, Biometric passwords eg thumb print, facial recognition are safer than a pin-code or a password and **may** be used
- You **should not** share passwords or pin-codes with anyone else where they protect MMBC data
- You **should not** store the pin-code or password on the removable media containing MMC data
- While you **may** store MMBC files on a temporary basis on removable media, eg to take to church for a presentation, **you should** transfer them to longer terms storage as soon as practical and delete from the removable media (delete/overwrite, scrub or reformat)
- Where your device allows, **you should** set mobile devices to return to the lock screen after 5 minutes inactivity
- You **should o**nly access MMBC data on removable media using secure and trusted networks eg do not using public wi-fi
- You **should** ensure your mobile device has up to date operating system patches, anti-virus, anti-spyware and anti-malware
- You **should r**egularly update Apps on mobile devices to remove back door hacking opportunities
- You **may** use a mobile device that uses encryption to access/store MMBC data
  You **may** set your mobile device to remote -wipe capability
- You **may** enable 'Find My Phone' or similar feature
- You **should** report any lost devices holding MMBC data to the Trustees.

2.3 Password Protect files

- If using standard MS Office software, you **should** set a password on the file before sharing by email, Drop Box, One Drive or similar file sharing platforms.
- Other brands of software also allow password protection
- You **should** forward the password to people you want to give access to the file by a different communication channel eg email the password protected file, instant message the password or give it in person or by telephone
- Email is not secure so you **should not** email passwords – most instant message services are secure eg WhatsApp, iMessage on IPhones and android phones.

2.4 **Broadcasting personal data**

- For example – address, telephone number, bank details: you **may** do this using a password protected file but a safer method is to use instant messaging which is encrypted, or give it in person or over the telephone (not in a public location)

2.5 **Anti-virus, Anti-Spyware, Anti-Malware**

- You **should** check your protection package covers all of these - running all three is a must
- Some top of the range anti-virus software includes cover for all three areas, but not all do, you will need to check what you are using
- Free software is available eg MS Defender for malware, MalwareBytes for spyware, Avast, or AVG for anti-virus. We are, however, unable to recommend any.
- You **should** ensure that your anti-virus, anti-spyware and anti-malware software are all set up update automatically on a scheduled basis – you are only as safe as the last time you updated

2.6 **Use of strong passwords**

- You **should** choose a password that has at least 8 characters
- You **should** use a mix of upper and lower case letters and numbers
- It **should** be personally memorable but difficult for others to be guessed
- Not all web sites can handle random characters like $, #, % in password authentication
- You **should not** use information about yourself in a password that can be easily guessed or gleaned from your social media account – eg your name, surname before marriage, date of birth, date of marriage, names and dates relating to children or other close family members or pets
- You **should not** repeat password across different websites, devices, programs or files
- You **should not** write passwords down
- You **should** change your password regularly eg every 3 months
- You **should** immediately change your password if you think it is compromised
- You **should not** check that it does not appear in clear text in any file or program
- You **should not** give anyone else your password
- You **should not** change your password by adding an incremental number on the end

2.7 **Cloud Storage**

- You **should** use only large recognised companies for cloud storage eg Sky, Google, OneDrive, Drop Box etc
- Cloud storage companies have to comply with GDPR as well if they hold your data as you are an EU/UK citizen
- In agreeing to their terms and conditions on-line you have a contract with them
- If they have a data breech they must inform you, you inform MMBC Trustees if any of our data is affected and we will inform the ICO

2.8 Data Retention and Disposal

- Anyone who requests that their data be amended/deleted **should** complete a Data Access Request form which will go to the nominated Trustee. The Trustee will investigate and then give you authority to amend/delete if appropriate. You **should not** amend/delete until advised by the Trustee.
- Data must only be held for the period of time that it is relevant to the purpose it was gained for. All MMBC appointed representatives **should** need to check the data held periodically and delete any data that does not meet this criterion.
- Digital data **should** be removed by deleting and overwriting to fully remove it from your devices.
- Paper based data **should** be shredded.
- It is recommended that data is reviewed every six months.

2.9 Data Transfer

- You **should** use password protected files only when sending as e-mail attachments
- You **should** send the password using a different communication channel eg face to face, WhatsApp
- You **may** use an encryption package to encrypt files before sending but be aware that commercially available packages are hackable and have associated costs
- You **may** use collaboration software to share files such as Google Docs, OneDrive (5Gb free file storage with an outlook.com email address) and enable access to files rather than emailing them

2.10 Backup and Recovery

- You **should** store password protected files only on your home PC/laptop/tablet
- You **should** store copies of files on a removable back-up drive. You **should not** keep it permanently attached to your device. Keep it unplugged from your device, if it is not plugged in it cannot be hacked into. Keep it in a safe place away from your device. Keep this drive only for back-ups, do not take it outside the house, otherwise you have data in transit and this is a risk.
- Instead of a straight file copy you **may** use a specific back-up program but you do not have to.
- Back-up copies **may** also be stored in the cloud
- Removable device can fail, specially those with moving parts eg hard drive, so periodic testing of your back up copies **should** be carried out to ensure your recovery plan works.

2.11 Increase Security on Home Router

- You **should** change the default Admin password

- You **should not** use an Admin password you have already used elsewhere
- You **should** change to an enhanced security - WPA2
- You **may** change the default network name (the SSID)

2.12 **Software**

- Whilst MMBC do not supply hardware or software, nor can we recommend any, any person acting on behalf of MMBC **should** ensure that they have legal entitlement to both the operating system and any productive software such as MC Office. You **should not** use pirated copies.
- Operating system software and productive software **should** be regularly updated to ensure all realised insecurities are patched.

2.13 Incident Reporting

- Following our policy will minimise data loss or data breeches
- If any data loss or breeches occur involving MMBC data you **should** inform the Trustees as quickly as possible by following the set procedure.
- The Trustees will investigate and inform the ICO, if appropriate, within 72 hours

---

MMBC IT Policy Acceptance Form

NAME	
ORGANISATION or CHURCH GROUP	
Email	
Phone No.	
Signature	
Date	