# Melton Mowbray Baptist Church

**Registered No: 1203133**

## Information Technology, Communication and Social Media Policy 2025

**1 Statement of Information Technology, Communication and Social Media Policy**

This policy sets out the correct use of the Melton Mowbray Baptist Church (MMBC) computers, internet and email systems. It demonstrates how the organisation will comply with the Computers Misuse Act 1990 and how it will protect its systems and the data on them.

Our computer systems are important to our operation and we therefore wish to clarify how they should be used. We also wish to protect our employees, volunteers and contractors from the possible consequences of misuse.

Non-compliance with this policy will result in disciplinary proceedings and or termination of contract(s).

Where appropriate, MMBC will involve the police or other law enforcement agencies in relation to breaches of this policy.

**2 Definitions**

**2.1** "Information Technology (IT)" is the use of computers, networks, software, and other digital systems to process, store, transmit, and secure data. It includes hardware like computers and networks, software from enterprise applications to antivirus, and related services, all of which are used to create, manage, and share information.

**2.2** "Artificial Intelligence (AI)" AI is an umbrella term for a range of technologies and approaches that often attempt to mimic human thought to solve complex tasks. Things that humans have traditionally done by thinking and reasoning are increasingly being done by, or with the help of, AI.

**3 The Church's Policy Statement**

**3.1 Use of Computers**

**3.1.1** The systems used at MMBC are varied and stand-alone

**3.1.2** Each member of staff will have access to a desktop Personal Computer (PC) or laptop and or a mobile phone belonging to the MMBC. A username and email account will be assigned to you when working at MMBC.

**3.1.3** The organisation's computers are for work use. Some reasonable personal use of computers is permitted outside of working hours.

**3.1.4** In order to protect work computers from risks of data exchange:

**3.1.4.1** You should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).

**3.1.4.2** You must not download or install software from external sources without authorisation from your line manager. Downloading unauthorised software may interfere with our systems and may introduce viruses or other malware.

**3.1.4.3** You must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems without authorisation from your line manager.

**3.1.4.4** Inform your line manager immediately if you suspect your computer may have a virus.

**3.2 Internet Usage**

**3.2.1** Internet access is provided primarily for business purposes. Occasional personal use may be permitted as set out in paragraph 3.4.

**3.2.2** You should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

We may block or restrict access to some websites at our discretion

**3.3 Email Usage**

**3.3.1 Introduction**

MMBC makes email available to its employees where relevant and useful for their jobs. This email use policy describes the rules governing email use at MMBC. It also sets out how staff members are expected to behave when using email. This policy should be read alongside other key policies. In particular, users should also read MMBC's data protection and internet use policies.

**3.3.2 Why this policy exists**

Email is a standard way to communicate in business. It's used widely and is arguably just as important as the telephone. Like any technology, email can cause difficulties if used incorrectly or inappropriately. This email policy:

- Reduces the security and business risks faced by MMBC
- Let's staff know how they are permitted to use MMBC email
- Ensures employees follow good email etiquette
- Helps MMBC satisfy its legal obligations regarding email use policy scope. This policy applies to all staff, contractors and volunteers at MMBC who use the MMBC email system. It applies no matter where that email use takes place: on MMBC premises, while travelling for business or while working from home. It applies to use of MMBC email on any device, no matter whether owned by the MMBC or employee.

.•All rules described in this policy apply equally to personal email use. For instance, inappropriate content is always inappropriate, no matter whether it is being sent or received for business or personal reasons.

**3.2.2.1** Adopt a professional tone and observe appropriate etiquette when communicating with third parties by e-mail.

**3.3.2.2** Remember that e-mails can be used in legal proceedings and that even deleted emails may remain on the system and be capable of being retrieved.

**3.2.2.3** You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate e-mails.

**3.3.3 You should not:**

**3.3.3.1** send or forward private e-mails at work which you would not want a third party to read;

**3.3.3.2** send or forward chain mail, junk mail, cartoons, jokes or gossip;

**3.3.3.3** contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to others who do not have a real need to receive them; or

**3.3.3.4** send messages from another person's e-mail address (unless authorised) or under an assumed name.

**3.3.4 Policy enforcement Monitoring email use**

Do not use your own personal e-mail account to send or receive e-mail for the purposes of our operations. Only use the e-mail account we have provided for you.

The MMBC email system and software are provided for legitimate business use. MMBC therefore reserves the right to monitor employee use of email. Any such examinations or monitoring will only be carried out by authorised staff. Additionally, all emails sent or received through MMBC email system are part of official MMBC records. MMBC can be legally compelled to show that information to law enforcement agencies or other parties. Users should always ensure that the business information sent via email is accurate, appropriate, ethical, and legal.

**3.4 Incorrect use of internet and email**

**3.4.1** We permit the incidental use of our systems to send personal e-mail, browse the internet and make personal telephone calls subject to certain conditions. Personal email use should be of a reasonable level and restricted to non-work times, such as breaks and during lunch. Personal use is a privilege and not a right. It must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

**3.4.2** Potential sanctions. Knowingly breaching this email use policy is a serious matter. Users who do so will be subject to disciplinary action, up to and including termination of employment.

**3.5 Social media policy**

**3.5.1 Purpose**

This policy is in place to minimise the risks to our organisation through use of social media.

**3.5.1.1** This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Google+, Wikipedia, Whisper, Instagram, Vine, Tumblr and all other social networking sites, internet postings and blogs, WhatsApp and AI. It applies to use of social media for organisation purposes as well as personal use that may affect our organisation in any way

**3.5.2 Personal use of social media**

**3.5.2.1** Personal use of social media is never permitted during working hours or by means of our computers, networks and other IT resources and communications systems.

**3.5.3 Prohibited use**

**3.5.3.1** You must avoid making any social media communications that could damage our organisation interests or reputation, even indirectly.

**3.5.3.2** You must not use social media to defame or disparage us, our staff or any third party; to harass, bully or unlawfully discriminate against staff or third parties; to make false or misleading statements; or to impersonate colleagues or third parties.

**3.5.3.3** You must not express opinions on our behalf via social media, unless expressly authorised to do so by your line manager. You may be required to undergo training in order to obtain such authorisation.

**3.5.3.4** You must not post comments about sensitive organisation-related topics, such as our performance, confidential information and intellectual property. You must not include our logos in any social media posting or in your profile on any social media.

**3.5.3.5** The contact details of organisation contacts made during the course of your employment are our confidential information. On termination of employment, you must provide us with a copy of all such information, delete all such information from your personal social networking accounts and destroy any further copies of such information that you may have.

**3.5.3.6** Any misuse of social media should be reported to your line manager.

**3.5.4 Guidelines for responsible use of social media**

**3.5.4.1** You should make it clear in social media postings, or in your personal profile, that you are speaking on your own behalf. Write in the first person and use a personal e-mail address.

**3.5.4.2** Be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see.

**3.5.4.3** If you disclose your affiliation with us on your profile or in any social media postings, you must state that your views do not represent those of your employer (unless you have been authorised to speak on our behalf as set out in paragraph 3.5.3.3). You should also ensure that your profile and any content you post are consistent with the professional image you present to the public and colleagues.

**3.5.4.4** If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your line manager.

**3.5.4.5** If you see social media content that disparages or reflects poorly on us, you should contact your line manager.

**3.5.5 Breach of this policy**

**3.5.5.1** Breach of this policy may result in disciplinary action up to and including summary dismissal. Any member of staff or contractor suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details.

**3.5.5.2** You may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action up to and including dismissal without notice.

**Approved: October 2025**

**Due for Review: October 2028**