

# PCC Of Moulton Parish Church

---

## Acceptable Use Policy – Information & Communication Technologies (ICT)

### Introduction

Moulton Parish Church recognises the important role ICT plays in the day to day running of church business. With the rapid growth of technology, particularly with regards to access and exchange of information it is necessary to ensure that appropriate controls are in place to the appropriate use by staff, volunteers and others in order to protect the Church's interests. This Policy seeks to provide appropriate guidelines and controls to ensure that users utilise our ICT in a proper and lawful manner.

This policy document explains the guidelines on the permitted and inappropriate use of our ICT facilities and what action may be taken if this policy is breached. This policy applies to you if you use any computers, phones, laptops, other computing devices or the MPC Wi-Fi for your work for MPC, or have access to any MPC Email addresses or shared electronic or online resources such as Office365. It should be read in conjunction with our Social Media, Safeguarding, Mobile Phone Use and Staff Code of Conduct policies.

By using MPC ICT you are agreeing to the terms of this policy.

### Permitted use

All ICT equipment is the property of Moulton Parish Church and must be used for legitimate Church business only.

Users are given access to assist them in the performance of their duties and for Church business. The type and level of access will depend on the specific needs of the user which may be reviewed regularly.

Reasonable personal use is permitted. This will be subject to the provisions of this policy well as all relevant policies as stated above. The misuse of ICT including electronic communication and shared resources may result in the restriction of access or disciplinary procedures (for staff) or criminal accountability where applicable.

### Responsible Persons

#### Church Wardens

The Church Wardens have overall responsibility for the allocation, use and maintenance of MPC ICT. This work may be delegated to an ICT officer elected by the PCC.

#### The ICT Officer

The ICT officer, in addition to the above will supervise the allocation, and management of user accounts as well as the administration of access to the Church's ICT resources. They will also be responsible for the network systems maintenance, security and relevant updates in liaison with a qualified external professional as appropriate. They will advise on the procurement of relevant subscriptions and updates for the smooth running and the continual development of ICT in line with new technological developments and best practice.

## **Line Managers and Supervisors**

Line managers and supervisors have a responsibility to ensure awareness for both staff and volunteers in complying with the guidelines set out in this policy. This will include guests or visitors under their care.

They will approve user requests for access to both devices and resources.

They will report any unauthorised or inappropriate use to the ICT officer or to the Vicar as appropriate.

## **Individual Users**

All users have a responsibility to adhere to organisational policies for ICT use and to promptly report any unauthorised use to their line manager, the ICT officer or to the Vicar

## **Personal use**

Personal use may include the use of the Internet, computing equipment, and telephones. Users will be able to access the Internet for personal use at no charge, and reasonable private telephone calls may be made using MPC phones. The private use of MPC mobile phones should not incur additional charge exceeding the inclusive amounts.

Personal use of any MPC device is authorised at the discretion of the PCC and must not interfere with the ability to do a job or bring disrepute to the Church.

## **Privacy**

All ICT resources are the property of MPC and may be used for Church business only except for such personal use as is permitted within the terms of this policy. There is no expectation of privacy for any user in anything they create, store, send or receive using MPC ICT.

The Church has the right to monitor and log any aspects of its ICT, including, but not limited to, monitoring Internet sites visited by users, monitoring Email correspondence, phone usage, chat, blog sites, newsgroup postings, and file transfers.

MPC will routinely archive certain data as appropriate. The discovery of any unauthorised use may result in suspension of access, disciplinary procedures and criminal liability as appropriate.

The user expressly waives any right of privacy in anything they create, store, send or receive using the Church's ICT systems.

The user consents to allow authorised Church personnel e.g. the ICT Officer or the Vicar to access and review all materials created, stored, sent or received by the user through any Church IT equipment, network or Internet connection.

## **Data and audit retention**

Data created, stored, sent or received, including system audit logs generated using the Church's ICT equipment may be archived or held in backups. Deleting a file or an Email does

not necessarily guarantee its removal from the IT systems. The Church will have control and responsibility for data retention as appropriate.

## **Inappropriate use**

The following uses of MPC ICT are prohibited:

### **Sharing user logins and passwords**

Allowing others access to IT facilities through their own login by the sharing of their passwords, except in instances where the ICT officer approves the use of shared login. Passwords must be kept secure at all times. Any compromise must be reported to the ICT officer or Church administrator immediately.

### **Hacking**

Attempting to access user accounts, files, Emails and/or any other materials including hardware and software without permission. This includes the use of hardware or software tools intended to defeat software copy protection, discover passwords, identify security vulnerabilities, decrypt encrypted files, or compromise information security by any other means.

### **Viruses**

Intentionally accessing or transmitting computer viruses and similar software and hindering or disabling security software such as Anti-Virus software.

### **Software**

Downloading or installing software (including, freeware, shareware, games and screensavers) without prior agreement. All software must be installed by, or with the agreement of the ICT officer as appropriate.

### **Other misuse**

Intentionally accessing or trying to access, distributing and disseminating or storing images, text or materials that might be considered obscene, sexually explicit, pornographic, racist, defamatory, intended to deceive, harassing, malicious, which incites or depicts violence or hatred, or describes techniques for criminal or terrorist acts or anything illegal.

Personal political lobbying or promoting or maintaining a personal or private business.

Any activities that could cause disruption of network and systems such as the playing of games, inappropriate Emailing or use of unauthorised software.

Illegal copying of material protected under copyright law or making that material available to others for copying.

## **Confidentiality**

Information handling must be in accordance with the relevant Data Protection regulations. Users must take reasonable steps to safeguard any confidential information in their possession or control.

Users will not use any confidential information for their own purposes, or for any other purposes other than performing their approved duties.

Confidential information must not be shared with third parties without appropriate authorisation. Unauthorised dissemination of such material will result in the Church's disciplinary procedures being initiated as well possible criminal liabilities where applicable.

Confidential data and information must not be taken off-site or uploaded onto non-Church computers or devices without proper authority and risk assessment.

Users must take care when conducting financial transactions or disclosing personal information when using MPC network. It is their responsibility to protect their personal privacy, and MPC will not be held responsible for any financial, personal or emotional loss or distress caused.

### **Content Management**

The Church may utilise software that makes it possible to identify and block access to Internet sites containing material deemed inappropriate in the workplace.

### **Breaches of Policy**

MPC reserves the right to restrict users' access to any computer systems and communications services, including the Church Wi-Fi, and to remove or substitute hardware or software used to access any ICT services at any time and for any reason.

If a breach of the policy is suspected, the ICT officer may isolate the computer or device from the network and remove it for further investigation which may involve other qualified professionals as appropriate.

The Church may respond to breaches of the policy in one or more of the following ways:

- Denial or restriction of computer access for a period
- Denial or restriction of computer access permanently
- Initiate disciplinary procedures which could result in disciplinary action being taken in line with the church's disciplinary policy (applicable for staff)
- Provision of information to the police for possible criminal proceedings if appropriate.

<b>Version History</b>		<b>Author &amp; Approvers</b>	
Creation Date	April 2024	Author	Eric Anakwa
Approved Date	April 2024	Approver	PCC
Next Review Date	April 2025	Responsibility	PCC

### **Relevant contacts:**

MPC Vicar: [n.alexander@moultonchurch.co.uk](mailto:n.alexander@moultonchurch.co.uk)

MPC ICT Officer: [admin1@moultonchurch.co.uk](mailto:admin1@moultonchurch.co.uk)

MPC Church Administrator: [admin@moultonchurch.co.uk](mailto:admin@moultonchurch.co.uk)

MPC Safeguarding Officer: [safeguarding@moultonchurch.co.uk](mailto:safeguarding@moultonchurch.co.uk)