Data Protection (GDPR) Policy

for the Benefice of Milton Abbot and Dunterton, Lamerton and Sydenham Damerel, Marystowe, and Coryton (South Tamar Mission Community) in the Diocese of Exeter

Covering the 6 churches and 4 PCCs of the Benefice
and adopted individually by the Incumbent and Parochial Church Councils (PCCs) of

- **Milton Abbot and Dunterton**
- **Lamerton and Sydenham Damerel**
- **Marystowe**
- **Coryton**

1 Introduction and Purpose

The Benefice is committed to complying with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This policy incorporates guidelines from the Diocese of Exeter Data Protection Resources and the national Church of England Parish Resources, and sets out how we collect, handle, store, and protect personal data across our Benefice.

As a united Benefice, our four PCCs and the Incumbent share administrative resources and software. Therefore, this joint policy establishes unified standards to ensure all church officers, ministry team members, employees and volunteers protect data privacy consistently.

2 Scope and Legal Status

2.1 The Data Controllers

Legally, a Benefice cannot own data. The separate **Data Controllers** are the Incumbent adn each of the four individual PCCs. They are jointly responsible for compliance.

2.2 To whom this applies

This policy applies to all trustees (PCC members), clergy, licensed ministers, retired ministers with Permission to Officiate (PTO), Parish Safeguarding Representatives, employees and volunteer coordinators/leaders across all six parishes.

2.3 Data types covered

This covers all personal data held digitally or in structured paper filing systems, including financial records, electoral rolls, safeguarding tracking, pastoral notes and contact lists.

3 Data Protection Principles

We commit to processing all personal data in accordance with the six core principles of the UK GDPR:

3.1 Lawfulness, fairness and transparency

Data is processed only with a valid legal basis, and a public Privacy Notice will always be available.

3.2 Purpose limitation

Data is only collected for specified, explicit, and legitimate church purposes.

3.3 Data minimisation

We only collect the minimum amount of data necessary for the task.

3.4 Accuracy

We will take reasonable steps to keep data accurate and up to date.

3.5 Storage limitation

Data is not kept longer than necessary. In managing records through their lifecycle we follow the national Church of England Records Retention Schedule to meet our legal, safeguarding, GDPR, and operational requirements while preserving records of historical value.

3.6 Integrity and confidentiality

Data is kept secure using appropriate technical and physical protections.

4 Operational Protocols for Benefice Systems

4.1 Centralised database and emails (currently *iKnow Church*)

Primary system: The Benefice uses the *iKnow Church* platform as its centralised data storage system and primary tool for administrative emails and updates.

Access control: The *iKnow Church* platform is tightly restricted based on the "principle of least privilege." Users are only given login access to the specific modules and contact groups necessary for their church role. Logins must never be shared between individuals, couples, or team members.

Consent mandate for emails: The *iKnow Church* is configured that emails are only sent to individual who have given explicit, trackable consent (by opt-in) to receive them. All mass emails must include an obvious, functional, "Unsubscribe" option (facilitated by the use of *iKnow Church*).

4.2 Wider email newsletters and community communications (e.g. *Mailchimp*)

Purpose: The Benefice also utilises *Mailchimp*, a third-party platform, for news and publicity mass emails.

Consent and minimisation: The same principles apply as to any other mass mailing – data must not be added without opt-in consent, and an "Unsubscribe" link is included in every email. Mailchimp lists must only hold the minimum information required for broadcasting.

Data integrity: Highly sensitive data – such as financial giving records, pastoral notes, or safeguarding statuses – must **never** be uploaded to or stored within *Mailchimp*.

Database alignment: If a subscriber updates their preferences or requests to be removed on *Mailchimp*, the Data Controller is responsible for manually syncing and updating this information within the main *iKnow Church* database (and *vice versa*) to ensure data accuracy across the Benefice.

4.3 Safeguarding data (National Dashboards and Hub)

Safeguarding compliance data, DBS tracking, and training records must be input securely into the national **Parish Safeguarding Dashboards and Hub**.

This data is processed under a legal obligation to meet the House of Bishops' statutory duties. Access is strictly restricted to the Incumbent, each PCC's designated Parish Safeguarding Representative, and the Benefice Safeguarding Coordinator.

4.4 The Ministry and Pastoral Teams (Clergy, LLMs, PTO Ministers, Anna Chaplains and the Pastoral Care Team)

Special Category Data: Members of the licensed ministry team and lay pastoral teams (including Anna Chaplains and Pastoral Care Team visitors) are routinely exposed to Special Category Data regarding individuals' health, physical or mental well-being, and religious beliefs.

Data Minimisation and Retention: To comply with the principle of data minimisation, pastoral visitors must not maintain permanent, unencrypted personal records or structured filing systems of pastoral visits. Any temporary written notes, contact details, or prayer requests recorded on paper or personal devices are classified as ephemeral records. These must be securely destroyed (e.g., cross-cut shredded or permanently deleted) immediately after the visit has taken place or the immediate follow-up action is complete.

Recording of Significant Data: Where a permanent record of a pastoral interaction is necessary for ongoing ministry or governance, this must either be logged directly within the restricted pastoral module of iKnow Church or communicated securely to the Incumbent for formal retention.

Statutory Safeguarding Escalation: Any information arising during a pastoral encounter that relates to a safeguarding concern, or the potential risk of harm to a child or vulnerable adult, falls outside ordinary pastoral confidentiality. Such information must be reported immediately to a Parish Safeguarding Representative in accordance with statutory safeguarding duties.

Policy Awareness: In place of formal contractual agreements, the Incumbent or designated Ministry Team Leaders are responsible for providing a clear, verbal briefing to all pastoral personnel to ensure they understand their obligations regarding confidentiality, data security, and the immediate disposal of temporary notes prior to commencing their duties.

4.5 Informal teams and rotas (e.g. flower, coffee, cleaning…)

To avoid unnecessary bureaucracy, local parish rotas are managed on a decentralised basis by their respective coordinators.

Coordinators may only distribute a list of contact details to group members if every person on that list has provided written or clear digital consent to share their details within that specific group.

These local lists must not be merged into the main iKnow Church or Mailchimp databases **unless** individual consent has been granted for wider benefice communications

4.6 Instant messaging groups (such as *WhatsApp*)

Purpose: The Benefice recognises that informal WhatsApp groups are a practical tool for organizing church teams, home groups, and committees.

The Transparency Rule: Because joining a WhatsApp group exposes an individual's phone number and profile photo to every other member of that group, no individual may be added to a church-related WhatsApp group without their explicit verbal or written Consent.

Group Setup: When creating a new group, the administrator must include a short introductory message stating the purpose of the group and reminding members that their numbers will be visible to others.

Content Restrictions: Group chats must be kept for functional coordination only. Special Category Data (such as highly specific prayer requests detailing a parishioner's medical condition) must never be posted in a group chat without that individual's explicit, written permission.

Right to Leave: Members have the right to leave a group at any time, and group administrators must not re-add individuals who have chosen to leave.

4.7 Social media and photography (Facebook, Instagram, Web)

Public vs. Private Spaces: While taking photos of a general crowd at a public church service does not usually require individual consent under UK GDPR, close-up, identifiable photos of individuals or small groups do.

Consent for Publication: The Benefice will not publish identifiable photos or videos of parishioners on its social media pages, websites, or in printed parish magazines without first obtaining their Consent.

Vulnerable Adults and Children: Photos of children under 16 or vulnerable adults will never be posted online without the explicit, written consent of a parent, legal guardian, or carer. Names of children will never be published alongside their photos.

Clear Signage: For major events where photography or live-streaming will take place, clear signage must be displayed at the church entrance. This signage must advise attendees of the filming and designate a "camera-free" seating area for those who do not wish to appear online.

4.8 Creating official Church accounts or groups

Prior Approval: No volunteer or staff member may set up a social media page, website, or WhatsApp group using the name or branding of the Benefice or any of its 4 PCCs, six churches or churchyards, premises or groups, without explicit written permission from the Incumbent or PCC.

Account Ownership: Any group or page created to represent the church belongs to the relevant PCC, not the individual who set it up. At least two church officers (such as the Incumbent and a Churchwarden or Administrator) must be given administrative access to the account.

Compliance: The creator of any official church group or page is responsible for ensuring it adheres to this Data Protection Policy and the wider Benefice Communications and Social Media Policy.

4.9 Incumbent and Vicarage email accounts

The Benefice recognises that the Incumbent, acting as a distinct Data Controller, utilizes dedicated office and personal email accounts to conduct day-to-day parish ministry, governance, and pastoral care. All devices accessing these accounts must be secured with a passcode, PIN, or biometric lock to prevent unauthorised access.

5 Subject Access Requests (SARs) and Data Rights

Individuals have the right to request a copy of all personal data held about them by any of our four PCCs or the Incumbent.

Any SAR received by any church officer or volunteer must be forwarded immediately to the Incumbent, PCC Secretary or Administrator.

The Benefice will respond to the request free of charge and within one calendar month, in accordance with ICO guidelines.

6 Managing Data Breaches

A data breach includes losing a parish contact spreadsheet, sending an email containing sensitive pastoral notes to the wrong person, or an unauthorised user accessing *iKnow Church*.

Any suspected or actual data breach must be reported to the Incumbent within 24 hours of discovery.

If the breach poses a high risk to the rights and freedoms of individuals, the Incumbent, in consultation with the Diocesan Registrar, must report the breach to the Information Commissioner's Office (ICO) within 72 hours.

7 Governance and Review

Each of the four PCCs formally vote to adopt this joint policy. This policy will be reviewed every three years, or sooner if national Church of England guidance or UK data protection law changes.

Resolution and Adoption

"The PCC resolved to adopt the Joint Benefice Data Protection Policy, acting as joint data controller alongside the Incumbent and the sister PCCs of the Benefice, to govern all data processing operations within this parish"

Date:

Signature:

Role: