Christ Church Felixstowe

Data Protection Policy

Introduction.
The PCC of Christ Church, Felixstowe is committed to compliance with the UK GDPR, Data Protection Act 2018, and the Church of England's national data protection policies.

This policy was adopted by the PCC of Christ Church Felixstowe on:___9th September 2025___ and will be **reviewed every two years, or sooner if the law changes.**

Signature of the vicar:_____Dominic Turner_____, on behalf of the PCC.

Scope.
This policy applies to PCC members, clergy, staff, volunteers handling personal data.

Principles.
We are committed to complying with GDPR principles: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality.

Responsibilities.
The PCC is the Data Controller. The PCC will appoint a Data Protection Lead from among its membership. We recognise that everyone who handles data is responsible for complying with this policy.

Data handling.
Registers and records must be kept as required by law. Other data may only be collected and stored in line with our privacy notice. Data must be kept securely in the church office in a locked filing cabinet. Digital data should be stored on the church office computer, or on the church Dropbox account. Sensitive data should be password-protected. Bulk emails must use bcc unless explicit consent given.

Consent.
After adopting this policy, consent must be explicit, recorded, and withdrawable at any time. Upon adoption of this policy, all current people on the church's contact lists and directory will be contacted, and given the option to withdraw their consent, and informed that if they choose not to do so this then grants consent from now on.

Data retention.
We follow the Church of England's 'Keep or Bin' guidance: registers kept permanently, Gift Aid kept for 6 years, safeguarding kept up to 75 years, electoral roll kept permanently, correspondence normally kept for 3 years.

Data breaches.
Data breaches should be reported immediately to the ICO, and their guidance should be followed. Serious breaches must be reported within 72 hours.

Subject Access Requests ('SAR').
Requests must be made in writing. The PCC must respond within one calendar month of receipt of the request.