St. Peter's Church
Live for Christ, Advance the Gospel

Registered Charity 1133803
Church Lane, Ardingly, West Sussex, RH17 6UR
www.ardinglychurch.co.uk

Secure storage of safeguarding records during a clergy vacancy.

During a clergy vacancy (interregnum) in the Church of England, the **Parochial Church Council (PCC)**, working with the **churchwardens**, is responsible for ensuring all safeguarding information is securely stored. The **Parish Safeguarding Officer (PSO)** usually becomes the primary custodian of these records until a new incumbent is in place.

• **Security:** Records, whether paper or electronic, must be kept securely to prevent unauthorised access, loss, theft, or damage.

• **Confidentiality and Accessibility:** Access must be strictly limited to relevant, authorised individuals (e.g., churchwardens, PSO, Diocesan Safeguarding Advisor (DSA)) on a "need-to-know" basis.

• **Continuity:** Arrangements must ensure the continuity of safeguarding management and safe handover to the new incumbent.

• **Compliance:** All procedures must comply with the Church of England's safeguarding policies, the House of Bishops' practice guidance, and current data protection legislation (UK GDPR and Data Protection Act 2018).

Procedures During the Vacancy

1. Handover from the Departing Incumbent

The departing incumbent must give all existing safeguarding information to the PSO before they leave.

2. Designated Custodian and Responsibility

The PCC must formally designate the PSO (and potentially churchwardens) as the temporary custodian(s) of all safeguarding records.

3. Storage Arrangements

• **Paper Records:**

Records should be stored in a locked filing cabinet or safe on church premises, not in a private home if it can be avoided.

Confidential information should be placed in an inner envelope marked "confidential" before being stored in the secure cabinet.

Records should be kept separate from general parish administration records.

- **Electronic Records:**

Electronic files must be stored on a secure, password-protected system or folder with strictly controlled access.

Regular backups of digital records should be made and stored securely, ideally off-site.

Password protection should also be applied to individual sensitive documents or emails containing personal data.

4. Record Keeping and Retention

Records must be kept up-to-date, accurate, and include a full chronology of events, actions taken, and decisions reached.

When records are no longer needed for legal or operational purposes, they must be destroyed securely (e.g., by cross-cutting shredder or confidential waste service).

5. Transfer to the New Incumbent

Upon the new incumbent taking up their role, the PSO will formally pass on all safeguarding information and a detailed summary of any ongoing concerns or historical cases.

This transfer should be documented and acknowledged by both parties.

The new incumbent must review the information and discuss it with the Diocesan Safeguarding Team to ensure a smooth transition of safeguarding responsibilities.

Policy review by PCC dated