

## GDPR PROCEDURES FOR ST. JOHN'S

Following advice from Diocesan Registrar, training workshops and the Information Commissioners Office (ICO):-

### General Precautions for all St. John's groups and individuals

- Locked filing cabinets, fire-proof safes for critical documents
- Shred/burn old data, or use a redacting pen
- Password protect computers, and all devices, esp. where shared—use high strength passwords
- Change passwords regularly
- Encrypt sensitive documents and emails
- Delete old personal data regularly, esp. when handing over roles
- Update operating system software regularly
- Use anti-virus software
- Be aware of dangers of emails and attachments going to the wrong person—check before sending them
- Be aware of dangers of wrong people copied in—**use blind copy (Bcc)**
- Do not disclose addresses/data to anyone not concerned
- Control the use and safekeeping of memory sticks
- If new IT devices—remove data from old system, destroy hard drives
- Protect IT devices from theft

### If a “Data Breach” occurs- actions for all St. John's groups and individuals

- Record and/or save all details of complaint
- No admittance of liability—just a simple acknowledgement of receipt
- Send all details to/inform Jo Whiteman and Penny Forbes, cc Rector, **immediately**
- Refer any subsequent enquiry to them, **immediately**

### St. John's Procedures (Church Administrator/PCC Secretary cc Rector) if a “Data Breach” occurs

- Immediate acknowledgement of receipt of report to data subject
- Open and compile a file record (file is in JPH office)
- PF/DC gather further information for ICO (see next section below)
- **Call ICO Helpline 0303 123 1113 within 72 hours to inform**
- If it is a “Subject Access Request”—inform Archdeacon immediately
- Act on any advice from ICO/Archdeacon/Registrar
- Plan and act on any remedial/mitigation action required
- If the breach has been caused by a procedure failure, inform other groups and/or individuals of required actions
- Record all actions in the file record
- Review Parish Data Audit records

**Reporting to the ICO if a “Data Breach” occurs—0303 123 1113**

- Description of nature of the incident
- Assessment of risks
- Categories and numbers of individuals concerned
- Categories and numbers of data records concerned
- Names of Data Compliance officers
- Likely consequences of the breach
- Description of measures taken including mitigation

This document was approved by PCC on

Jo Whiteman– updated January 16.07.25