General Data Protection Regulation (GDPR)
ACTION PLAN

| No. | Action | Due Date | Responsibility | Comment |
| --- | --- | --- | --- | --- |
| **1.** | **Data Audit**Identifies all data that we hold about people and includes:* Why the data is held (e.g. electoral roll, stewardship details)
* The basis for holding the data (e.g. is it a legal requirement?)
* Who holds the data in the church (Data Owners) and who can access it
* What security controls are in place
* How long the data is kept for
* Whether it should be covered by a Privacy Notice
* Actions required
 |
| 1.1 | Produce draft Data Audit document | 13 April |  |  |
| 1.2 | Review and update draft Data Audit document | 27 April | All PCC Members |  |
| 1.3 | Finalise Data Audit document | 4 May |  |  |
| 1.4 | PCC approves Data Audit | 29 May | All PCC Members | At next PCC meeting. |
| 1.5 | Schedule ‘Actions Required’ | 31 May |  | See also Section 6. |
| 1.6 | Implement ‘Actions Required’ | To be confirmed | All PCC Members and Data Owners | The Due Date will depend on the data identified and the Actions Required. |
| **2.** | **Privacy Notice**Tells our Data Subjects (e.g. Stewardship members) about what we are using data for, where it is held, who we share it with and how they can contact [Name] PCC. **This document needs to be sent to each Data Subject.** |
| 2.1 | Produce draft Privacy Notice document | 13 April |  | We can use and adapt a template provided by the Diocese. |
| 2.2 | Review draft Privacy Notice | 27 April |  |  |
| 2.3 | Finalise Privacy Notice | 4 May |  |  |
| 2.4 | PCC approves Privacy Notice | 29 May | All PCC Members | At next PCC meeting. |
| 2.5 | Issue Privacy Notice to each Data Subject | 15 June | Data Owners | How the Privacy Notice is issued will depend on the data identified. |
| **3.** | **Data Protection Policy**Tells everyone why we use data and how we hold it. This includes details of how we will deal with data breaches, data retention and subject access requests. **The Diocese suggests separate policies for data breaches and data retention, but a single all-encompassing Data Protection Policy is probably most appropriate for** [Name]**.** |
| 3.1 | Produce draft Data Protection Policy | 13 April |  | We can use and adapt a template provided by the Diocese. |
| 3.2 | Review draft Data Protection Policy | 27 April |  |  |
| 3.3 | Finalise Data Protection Policy | 4 May |  |  |
| 3.4 | PCC approves Data Protection Policy | 29 May | All PCC Members | At next PCC meeting. |
| 3.5 | Pin Data Protection Policy to noticeboard | 30 May |  |  |
| **4.** | **Gaining Consent**In these initial stages it is not clear what additional consent we need to get from our Data Subjects. Provided we are contacting Data Subjects only where there is ‘legitimate interest’ or ‘reasonable expectation’ then we shouldn’t need further consent (e.g. if someone subscribes to the parish magazine, we can say that they have legitimate interest in what is happening in the church in [Name] and reasonable expectation that they receive details of future services and events).The requirement for getting additional consent will be reviewed after the Data Audit and, if necessary a Consent Form will be produced and issued. |
| 4.1 | Review requirement for additional consent | 4 May |  |  |
| 4.2 | If necessary, produce Consent Form(s) | 18 May |  |  |
| 4.3 | Issue Consent Form to all relevant Data Subjects | To be confirmed | Data Owners |  |
| **5.** | **Bring Your Own Device (BYOD) Policy (use of personally-owned devices for PCC work)**Gives guidance to everyone who works with church data (e.g. PCC Members, volunteers) on how they should manage their own devices (PC, tablet, etc.). |
| 5.1 | Produce draft BYOD Policy | 13 April |  | We can use and adapt a template provided by the Diocese. |
| 5.2 | Review draft BYOD Policy | 27 April |  |  |
| 5.3 | Finalise BYOD Policy | 4 May |  |  |
| 5.4 | PCC approves BYOD Policy | 29 May | All PCC Members | At next PCC meeting. |
| 5.5 | BYOD Policy circulated to everyone that works with church data | 15 June |  |  |
| **6.** | **Training and implementation** |
| 6.1 | Assess the requirement for GDPR training | 4 May |  |  |
| 6.2 | Check and delete all old/unnecessary data  | 29 June | All PCC Members and Data Owners |  |
| 6.3 | Implement data security measures as outlined in the Data Audit ‘Actions Required’ and BYOD Policy | 29 June | All PCC Members and Data Owners |  |
| 6.4 | Periodic audit (testing and evaluating) of data security measures | Quarterly? |  | Does this need to be someone independent of the PCC’s GDPR? |
| 6.5 | Respond to Subject Access Requests | As required |  |  |
| 6.6 | Review GDPR requirements and documentation to ensure it continues to be fit for purpose | 31 May 2019 |  |  |