Appendix 2 – GDPR Action Plan Checklist

①	**Raise awareness** – PCC members, church administrators, incumbents and other key data users should be made aware that the law is changing. Ensure they undergo training, and that records are kept. They need to know enough to make good decisions about what you need to do to implement the GDPR. **Decide who will be responsible for data protection** – The incumbent and another member of the PCC should take responsibility for compliance with data protection legislation and should have the knowledge and authority to do this effectively.
②	**Data Audit –** If you do not know what personal data you hold and where it came from you will need to organise an audit to find out. This means all personal data including employees and volunteers, service users, members, donors and supporters and more. You should document your findings because you must keep records of your processing activities. You should also record if you share data with any third parties. See ***Appendix 3 – Audit Questionnaire.***
③	**Identify and document your 'lawful basis' for processing data** – To legally process data under the GDPR you must have a 'lawful basis' to do so. For example it is a lawful basis to process personal data to deliver a contract you have with an individual. There are a number of different criteria that give you lawful basis to process and different lawful basis give different rights to individuals. Understand and document your lawful basis for processing data.
④	**Check your processes meet individuals' new rights** – The GDPR will give people more rights over their data. For example, the GDPR gives someone the right to have their personal data deleted. Would you be able to find the relevant data and who would be responsible for making sure that happened? Ensure you have the systems in place to be able to deliver the 8 rights. **Know how you will deal with 'subject access requests'** – Individuals have the right to know what data you hold on them, why the data is being processed and whether it will be given to any third party. They have the right to be given this information in a permanent form . This is known as a 'subject access request' or "SAR". You need to be able to identify a SAR, find all the relevant data and comply within one month of receipt of the request. Under the GDPR the time limit for responding to SARs is reduced from 40 days to one month and the £10 fee is abolished.
⑤	**Review how you get consent to use personal data** – If you rely on consent as your lawful basis for processing personal data, then you need to review how you seek and manage consent. Under the GDPR consent must be freely given, specific and easily withdrawn. You can't rely on pre-ticked boxes, silence or inactivity to gain consent instead people must positively opt-in. See our consent language in ***Appendix 4 – Consent Form.***
⑥	**Build in extra protection for children** – The GDPR says children under 16 cannot give consent (although this will be reduced to 13 in the UK) so you will have to obtain consent from a parent or guardian. You will need to be able to verify that person giving consent on behalf of a child is allowed to do so. Privacy notices should to be written in language that children can understand.
⑦	**Update your Policies & Notices** **Policies** – Have clear, practical policies and procedures on information governance for staff to follow, and monitor their operation. **Privacy Notices** - You must always tell people in a concise, easy to understand way how you intend to use their data. Privacy notices are the most common way to do this. You may well already have privacy notices but they will all need to be updated. Under the GDPR, privacy notices must give additional information such as how long you will keep data for and what lawful basis you have to process data. Our sample privacy notices are in ***Appendix 5 – Privacy Notices.*** **Data Retention & Disposal** – Ensure you update your data retention policy and inform all data subjects how long you will retain data. When disposing of records and equipment, make sure personal information cannot be retrieved from them. To assist, see the link to the Church of England website for 'Keep or Bin: care for your Parish Records' on page 24. **Websites** – Control access to any restricted area. Make sure you are allowed to publish personal information (including images) on website/social media.

Appendix 2

⑦

Data sharing – Be sure you are allowed to share information with others and make sure it is kept secure when shared.

CCTV – Inform people what it is used for and review retention periods. Ensure you have the correct signage on display and a suitable policy in place.

Training – Train staff on the basics of information governance, where the law and good practice need to be considered, and know where to turn for advice.

⑧

Update your contracts to deal with processing by others – Recognise when others are processing personal data for you and make sure they do it securely. You will need to ensure your contracts are updated to include the GDPR required clauses and put in place an audit programme to supervise them. Consider also how you select suppliers. There must be a written contract which imposes these obligations on processors:

1. Follow instructions of the controller.
2. Ensure their personnel are under a duty of confidence.
3. Keep the personal data secure.
4. Allow Controllers to consent to sub-contractors.
5. Flow down obligations to sub-contractors (but remain responsible for actions of the sub-contractor(s).
6. Assist the controller when individuals exercise their rights to access, rectify, erase or object to processing of data.
7. Assist the controller with privacy impact assessments.
8. Assist the controller with security and data breach obligations and notify the controller of any personal data breach.
9. Return or delete data at the end of the agreement (but can keep a copy).
10. Demonstrate compliance with these obligations and submit to audits.
11. Inform the controller if their instructions would breach the law.

⑨

Personal Data Breaches - Get ready to detect, report and investigate these - A data breach is a breach of security leading to 'accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'. You will need to have the right procedures in place to detect, investigate and report a breach. The GDPR introduces a duty to report certain types of data breaches to the ICO and in some cases to the individuals concerned. You need to be able to demonstrate that you have appropriate technical and organisational measures in place to protect against a breach.

- The Data Protection Compliance Officer and other back-ups need to be recognised by data users as those to whom any breaches should be reported. They therefore need to be briefed on the procedure for dealing with data breaches.
- All data users should be briefed on personal data breach avoidance, and on what to do in the event that a breach occurs.
- Examples of personal data breaches and steps to avoid them include:
  - Emails and attachments being sent to the wrong person, or several people – it is easy to click the wrong recipient. Slow down, check thoroughly before clicking 'send'.
  - The wrong people being copied in to emails and attachments. – Use BCC (Blind Carbon Copy) where necessary.
  - Lost memory sticks – The PCC should put protocols in place for memory stick usage
  - Malware (IT) attach – ensure up to date anti-virus software is in place.
  - Equipment theft – check security provisions.

⑩

Build data protection into your new projects - Privacy by design means building data protection into all your new projects and services. It has always been good practice, but the GDPR makes privacy by design an express legal requirement. To achieve this, data protection impact assessments should be undertaken where new technology is being deployed, where profiling may significantly affect individuals or sensitive categories of data will be processed on a large scale. Clarify who will be responsible for carrying out impact assessments, when you will use them and how to record them. See our DPIA assessment checklist in Appendix 5.