GDPR Checklist

Introduction

The General Data Protection Regulation 2016/279, together with the Data Protection Act 2018, forms part of the data protection regime in the UK.
The GDPR applies to Data Controllers and Data Processors. Churches in Croxley Green CIO ("the CIO") is a Data Controller
The GDPR covers personal data, which means any information related to a natural person that can be used directly or indirectly to identify the person (referred to from here as an individual). This could include a wide variety of information, including a postal or mail address list for circulation of the information about the CIO, contact details for volunteers and records of donors. In addition, sensitive personal data includes information about a person's racial or ethnic origin, religious beliefs, physical or mental health or condition, and criminal offences. Information about safeguarding matters is an example of sensitive personal data that the CIO may hold.

Preliminary

1. **The GDPR requires certain bodies to appoint a data protection officer ("DPO"), who must be independent, an expert in data protection, adequately resourced, and report to the highest management level**

   Is the CIO required to appoint a DPO? Yes / No
   If no, please state the reason(s) why

   If yes, has a DPO been appointed? Yes / No
2. **The CIO is required by law to have a policy for dealing with data protection issues**

   Is a Data Protection Policy in place? Yes / No
3. **Everyone involved with the CIO with access to personal data should be familiar with the CIO's Data Protection Policy**

   Have all appropriate people been given access to the policy and instructed to familiarise themselves with it? Yes / No

4. **The CIO is required by law to have a policy for dealing with privacy**

   Is a Privacy Policy in place? Yes / No
5. **Everyone involved with the CIO with access to personal data should be familiar with the CIO's Privacy Policy.**

   Have all appropriate people been given access to the policy and instructed to familiarise themselves with it? Yes / No
6. **Unless exempt, all organisations/sole traders which process personal data are required to pay a fee to the Information Commissioner**

   Is a fee required? Yes / No
   If no, please state which exemption applies

If yes, has it been paid? Yes / No

Keeping personal data secure

- Has the CIO carried out a risk assessment and used this to assess the appropriate level of security to put in place? Yes / No
- Does the CIO use encryption and/or 'pseudonymisation' where it is appropriate to do so? Yes / No
- Is access to personal information in the CIO limited to those with a strict need to know? Yes / No
- If any individual computers, portable electronic devices or removable storage media are used to store personal data, are they encrypted? Yes / No
- Are passwords and PINs kept confidential and changed regularly? Yes / No
- Are computers locked or logged off and paper documents securely locked away when individuals are away from their desks? Yes / No
- Are computer screens positioned away from windows and gangways to prevent accidental disclosure of personal data? Yes / No
- Are offices, desks and filing cabinets/cupboards kept locked if they hold personal data of any kind, (whether on computer or on paper)? Yes / No
- When personal data is removed from an office, is it subject to appropriate security measures, including keeping paper files away from public visibility, the use of passwords/passcodes and encryption of portable electronic devices and secure storage (e.g. not left in the boot of a car)? Yes / No
- When destroying personal data, are paper documents securely shredded and is electronic data securely deleted? Yes / No
- Do you keep back-ups of information? Yes / No

Managing expectations

- Is there a policy in place to ensure that the CIO collects only as much personal data as is needed for a particular purpose? Yes / No
- When the CIO collects personal data, does it tell people why it is collecting it, what it will be used for and with whom it may be shared? Yes / No
- Do the individuals whose information the CIO holds know that the CIO has it and are they likely to understand what it will be used for? Yes / No
- Does the CIO update records promptly, (e.g. changes in contact details)? Yes / No
- Does the CIO securely delete/destroy personal data as soon as there is no more need for it? Yes / No

Awareness and training

Do Trustees/staff/volunteers:

- Know not to give out personal data over the telephone unless in very limited circumstances where they know or can verify the caller's identity and their entitlement to receive the information requested? Yes / No

- Require callers to put their requests in writing so their identity and entitlement to receive the information may be verified? Yes / No

- Ensure personal data is securely packaged and consider the most appropriate means by which the data should be sent (e.g. special delivery, courier or hand delivery)? Yes / No

Personal data breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

- Do Trustees/staff/volunteers know how to recognise a personal data breach? Yes / No

- Do Trustees/staff/volunteers understand that a personal data breach is not only about loss or theft of personal data? Yes / No

- Has the CIO prepared a response plan for addressing any personal data breaches that occur? Yes / No

- Has the CIO allocated responsibility for managing breaches to a dedicated person? Yes / No

- Do staff/volunteers know how to escalate a security incident to the appropriate person in the CIO to determine whether a breach has occurred? Yes / No

- We have in place a process to assess the likely risk to individuals as a result of a breach? Yes / No

- Does the CIO have a process to notify the Information Commissioner of a breach within 72 hours of becoming aware of it, even if all the details are not known? Yes / No

- Does the CIO know what information must be given to the Information Commissioner about a breach? Yes / No

- Does the CIO have a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms? Yes / No

- Does the CIO know that it must inform affected individuals without undue delay? Yes / No

- Does the CIO know what information about a breach it must provide to individuals and that it should provide advice to help them protect themselves from its effects? Yes / No

- Does the CIO have a process to document all breaches, even if they do not need to be reported? Yes / No

---

Methods of distribution.
Copies should be made available to all those working in any capacity on behalf of the charity

Review dates: May 2018, April 2019