APEC DATA PROTECTION

This summary is for all leaders and volunteers to read and review so that they are aware of their responsibilities on data protection, and the risk if they breach legislation.

1. Introduction

The Data Protection Act 1998 (DPA) seeks to protect an individual against the unfair use of their personal information. From 25th May 2018 the new General Data Protection Regulation (GDPR) will supersede the DPA. If a church holds personal data either on a computer or in a paper-based filing system it must follow the rules set out in the DPA and, from the 25th May 2018, the GDPR. Failure to do so could result in enforcement action being taken, by the regulator, the Information Commissioner's Office (ICO), against the church in question or against the trustees if the church is unincorporated. There are serious implications for breaching Data Protection legislation which we have outlined below. Whilst the type of personal information held by most churches is unlikely to result in a serious data breach you do need to be aware of the possible consequences. − Under the current law the ICO has a range of enforcement tools at its disposal including the imposition of a financial penalty (a 'monetary penalty notice') of up to £500,000 for the most serious breaches

2. DEFINITIONS

Data protection involves some specific terminology which it's important to be familiar with. In particular:

A **data controller** is an organisation or individual that determines the purposes for the manner in which way any personal data is processed. It is important to note that the definition of data controller also includes all leaders and volunteers within the church. Therefore, all volunteers and leaders need to read this leaflet, and be aware of their responsibilities.

A **data subject** is an individual about whom personal data is held. For example, this could be someone who attends the church who has given their personal details so that they can be contacted about church services and prayer requests.

Personal data is, broadly, of any information about a living individual which can identify that individual. Identification can be by the information alone or in conjunction with any other information in the data controller's possession or likely to come into such possession. It can apply to data held in manual or electronic form.

Sensitive personal data is personal data relating to an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health condition, sexual life, alleged or actual criminal activity and/or criminal record.

Much of the information which churches are likely to process will be sensitive personal data as it is likely to concern the data subject's religious beliefs. Where churches carry out Disclosure and Barring Service (DBS) checks on employees or volunteers, they may also process sensitive personal data in the form of criminal convictions data. Information relating to the physical or mental health of church members, employees, volunteers and other individuals may also be held by a church.

A **relevant filing system** is a system of holding manual (i.e. paper) records from which specific information about a specific individual can be readily accessed. An example of such a system would be a set of employment records consisting of a filing cabinet containing files of named individuals in surname order.

Processing is anything done with or to personal data. For example, GBXTRA – holding emergency contact details of parents.

3. PRINCIPLES OF DPA

Overview of the eight principles Schedule 1 of the DPA outlines eight data protection principles, which are paraphrased below. In summary, all personal data must be:

1. Fairly and lawfully processed in accordance with Schedules 2 and 3 of the DPA (see below).

2. Processed for limited purposes notified to the ICO and to the data subject (you cannot use data for another purpose without letting the data subject know).

3. Adequate, relevant and not more than is necessary to complete the task for which it was collected. However, keeping records for historical and research purposes is a legitimate reason for holding data.

4. Accurate and up-to-date (data subjects can request corrections).

5. Not kept for longer than is necessary to complete the task for which it was collected.

6. Processed in line with the data subject's rights (particularly the right of subject access, as described later in this factsheet).

7. Kept secure, with appropriate technical and organisational measures to protect against unauthorised or illegal processing, or accidental loss.

8. Not transferred to a country or territory outside the European Economic Area, without an adequate level of protection for the rights of data subjects.

4. What do I need to do if there is a data breach?

Under GDPR, data controllers and data processors will be jointly and severally liable for breaches and so each would be legally liable to the extent to which they are responsible in any data breach

Therefore, individual volunteers as well as the Church may be fined.

An example of a breach: - A volunteer within the church holds contact details provided by parents of children attending a Holiday Club. When parents provided this information, they were told it would be used to contact them in an emergency and to inform them of future church activities which their children might like to attend. If this volunteer then uses the information they holds to contact parents about a child-minding service they are setting up then they are in breach of Data Protection legislation.

All potential breaches should be reported to the trustees of APEC immediately by telephone: Paul Ferris on 07584178550 and email contact@apec-coventry.og.uk . Please do not try and hide anything as action may be taken to limit the effect of the breach.

A personal data breach is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Currently, data breaches do not have to be routinely notified to the ICO or others (although the ICO recommends that it is good practice so to do). The GDPR makes informing the ICO and the individuals affected compulsory in certain circumstances, (e.g. where there is a high risk to the individuals involved, for instance, through identity theft). Under the GDPR, you will have to notify the ICO of a data breach within 72 hours of finding out about this. It is important that the Trustees at APEC note this deadline and seek any advice of the diocesan registrar about any suspected breaches without delay.

More details can be provided after 72 hours, but before then the ICO will want to know the potential scope and the cause of the breach, mitigation actions you plan to take, and how you plan to address the problem.

5. Access to data requests

If anyone wishes to request a copy of the information held about themselves please can you ask them to request this via the Trustees via email: contact@apec-coventry.org.uk

6. Retention Periods of Records

See Appendix 1

If you have any queries please contact Trustees at APEC via email on contact@apec-coventry.org.uk

Version 2.0 21 November 2023

Appendix 1: Retention Periods of Records

Records	How long to keep?	Action after
Finance records including: cash books, bills, bank statements, budgets, accounting records and other subsidiary financial records and Gift Aid Declarations	As long as valid + 6 years minimum As per Charities Commission requirements	Destroy
Invoice Capital Item	10 years	Destroy
Success quotations for Capital items	permanent	Keep in safe
Legacies	6 years after estate has wound up	Destroy
Mailing list, email distribution lists, personal data on adults	As long as valid	Destroy
General correspondence	Last action + 2 years	Destroy
Gift Aid Declarations	As long as valid + 6 years	Destroy
Accident reports - Adults	3 years after last accident	Destroy
Accident reports - children	Until the child becomes 21 years old	Destroy
Risk Assessments	Keep up to date each year	
Legal documents	Keep permanently	Keep permanently in a safe
DBS Certificate information	6 months	Destroy
Records relating to concerns about those working with children and young people	Date of concern + 50 years	Destroy
Allegation of a child protection nature against a member of staff/ volunteer, including where the allegation is unfounded	Date of concern + 50 years	Destroy
Contracts/building works papers/ Successful quotations	End of contract & retain permanently	Retain permanently
Insurance policies	End of policy + 6 years [requirement]	Destroy
Trustee/Director minutes	Minimum of 10 years	Destroy