

Preparing for GDPR

AWARENESS

Create a Project Team consisting of decision makers and key people.

Steve Kelly, Helen Goff, Hywel R-J, Derek Bish, Jo Smith, Renee Dixon, Serena Yong, Diana R-J

Group created 5th February 2018

DATA AUDIT – Information we hold

Carry out a data audit (map and order data flows):

- What kind of data is being collected, stored and why?
- Which different church groups might store their own data?
- How is the data used both internally and externally?
- How long is the data retained?
- Who has access to the data both inside (staff) and outside (congregation)? Any others?
- What procedures and controls are in place to keep data safe?

Meeting arranged to discuss 20th February 2018. For retention there are exemptions from GDPR such as for IR (gift aid forms) and safeguarding

PRIVACY NOTICE – ensure this is in line with GDPR

When we collect personal data we are obliged to give data subjects certain information such as our identity and how we intend to use their information. **Additional information** is now necessary eg we need to explain our lawful basis for processing (using) data, retention periods, the right to complain to the ICO if deemed necessary, and information must be provided in concise, clear, easy to understand language.

Process of writing a Privacy Notice has begun with a deadline to finalise 31st March 2018

GDPR rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- The right not to be subject to automated decision-making including profiling

REVIEW OUR PROCEDURES

We need to review our procedures to ensure they cover all the rights individuals have and clearly explain the process we undertake to carry out these rights. For example: the right to erasure – how do we go about locating personal data and deleting it – what is the time frame following a request and who is responsible for deleting it?

We need to update and document our procedures for handling requests ensuring the rights of individuals are carried out to include how this needs to be communicated by the data subject, the time frame in which to carry it out (I have put 30 days on consent form) and who is responsible for doing it. Deadline 30th April 2018

Preparation for GDPR

IDENTIFY the lawful basis for processing (using) personal data

We should IDENTIFY, DOCUMENT and REVIEW the lawful basis for how we use personal data. IE. Data subjects must give clear consent to process (use) their personal data for one or more specific purpose/s. This needs to be explained in our Privacy Notice.

CONSENT

We need to review how we seek, record and manage consent and if we need to make any changes. Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in. Consent cannot be assumed. And we must have a simple way for people to withdraw consent. Consent must be specific, granular (separate consent for separate things). We need to document and keep records of how we obtain consent. Consent needs to be given from 16+. Under 16, consent must be obtained from parents/guardians.

CHILDREN

We need to think about what systems we have in place to verify individuals' ages and to obtain parental/guardian consent for data processing.

GDPR has special protection for children's personal data, particularly in the context of commercial internet services such as social networking. If we offer online services to children which relies on consent to collect information about them then we need to gain consent. Children at 16 years can give their own consent. This may be reduced to 13 years in the future.

A new consent form has been drawn up which needs approving by PCC and Vicar. Suggest obtain consent from all individuals in church community and to allow 4-6 weeks for this process to complete. ie from mid April. Physical presence in church to encourage people to complete after services.

I assume we need to put together a different consent form to cover this??

Preparation for GDPR

DATA BREACHES

We need to make sure we have the right procedures in place to detect, report and investigate a personal data breach

To be discussed with PCC and Vicar

DATA PROTECTION BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS

This is now a legal requirement under GDPR for situations where data processing is likely to result in high risk to individuals. We should start to assess the situations where it will be necessary to conduct a DPIA (Data Protection Impact Assessment).

To be discussed in project team meeting and PPC