DIOCESE OF PORTSMOUTH: GDPR Quick Factsheet

(Approved December 2020)

Collecting Personal Data

Seven Key Principles

The General data Protection Regulation (GDPR) sets out 7 key principles for collecting personal information.

These principles should lie at the heart of your approach to processing personal data.

Lawfulness, fairness and transparency

Purpose limitation

Data minimisation

Accuracy

Storage limitation

Integrity and confidentiality (Security)

Accountability

Asking for Personal Data

When asking for any personal data (anything that identifies an individual) create a form to collect the information and include the following information to inform those who are filling it in:

Do not ask for any information outside of the form (by email, telephone or in person).

state one of six lawful basis for processing (see ICO website for description of each lawful basis)

inform the individual of their privacy rights to do with personal data including:

What it will be used for

Who will have access to it

How will it be stored securely

How long will it be retained

Who they can contact to view, amend or request deletion

Confirmation that it will be disposed of securely when retention period is over

Provide a link to the Diocesan GDPR website page which includes links to our Privacy Notice and Retention Policy.

If you have any queries or would like any assistance in creating forms with this information, identifying principles or lawful basis, maintaining confidentiality please contact the Administrative Services Manager, Maria Devine at gdpr@portsmouthdiocese.org.uk

Refer to the Microsoft 365 Training website as another resource for any IT queries, as it provides quick, simple instructions on how to use each Microsoft program. You can also type keywords in the search box to find the answer for other queries.

Contact the Diocese IT Support Team for queries, working hours are 08:30-15:30 on weekdays itsupport@portsmouthdiocese.org.uk

Maintaining Confidentiality of Personal Data

Please ensure you maintain the confidentiality of personal data. The following points will help. This will protect information, minimises the risk of scams or hacking and avoids breaches which have to be reported to the ICO.

Use a diocesan email address for all official business. Please do not use personal email addresses as these are not protected by the Diocese secure server and IT cannot investigate or secure personal email addresses if they are hacked.

Do not share your password or login details with anyone.

Only save files on your SharePoint or OneDrive folders on the Diocese secure server.

Electronic files containing personal data must be password-encrypted and stored on a password-protected computer. (Open document / Click File / Info / Protect Document / Encrypt with password.)

Paper files containing personal data must be kept in a locked cabinet in a locked room with access for relevant staff only.

Use blind copy (BCC) when emailing groups so their email addresses remain private.

Consider before forwarding emails if there is any personal data content in the previous conversation, and if so send a new email instead of forwarding.

Data Breach Reporting Procedure

A data breach is whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation. Please report all data breaches as soon as possible to gdpr@portsmouthdiocese.org.uk so we can decide if it needs to be reported to the ICO within the 72-hour deadline, or if it can be recorded as a near miss and learnt from.

Please follow the Data Breach Procedure and complete the Data Breach Report Form, which are both available on the GDPR page of the Diocese of Portsmouth website.