



CATHOLIC DIOCESE OF PORTSMOUTH: UK GDPR Quick Factsheet

(Last reviewed Jun 2021)

Collecting Personal Data

SEVEN KEY PRINCIPLES

The **UK** General data Protection Regulation (**UK** 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

Retention

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](#) which includes links to our [Privacy Notice](#) and [Retention Procedure](#).



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 Data Compliance Officer (DCO) at gopr@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.



If you have a diocesan email address, **please use it** 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. **We are aware not all volunteers may have a diocesan email address, if so, please take extra care in emailing sensitive information (eg Safeguarding, financial) such as encrypting files.**



Do not share your password or login details with anyone.



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

Volunteers who do not have access to the Diocese server must take extra care in saving sensitive files (Safeguarding, financial, contact details etc.) such as encrypting files.



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.)

Refer to the Retention Schedule for how long each type of document should be kept and see the Data Protection policy (Appendix B) for a sample form to record when any personal data is disposed of.



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 gdp@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 website](#).