FREQUENTLY ASKED QUESTIONS (FAQS) ON DATA PROTECTION

1 GENERAL

1.1 What is personal data?

Personal data is information that relates to an identifiable living individual (often referred to as a 'data subject'). It can include names, email addresses, images, bank details, etc.

1.2 What are our responsibilities under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018?

GDPR covers the processing of personal data in two ways:

1) Personal data processed wholly or partly by automated means (that is, information in electronic form); and

2) Personal data processed in a non-automated manner which forms part of, or is intended to form part of, a 'filing system' (that is, manual information in a filing system).

It does not cover unstructured paper records, such as temporary hand-written notes.

It requires us to keep all personal data secure, and use it only for the purposes intended. It also provides rights to individuals, including the right to be informed about the collection and use of their personal data, the right to access their personal data, and the right to have their personal data rectified or erased.

1.3 Isn't this intended for businesses; surely a church doesn't need to concern itself with GDPR?

GDPR also applies to churches and charities, regardless of their size.

Of particular relevance to church activities, information about a person's religion is considered to be 'special category' (i.e. sensitive) data. According to the Information Commissioner's Office:

> "*This type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.*"

For this reason, we are required to meet an additional condition for processing this data, specifically:

> *"Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects."*

Any personal data (e.g. contact details) of parishioners should therefore be treated as sensitive, protected accordingly, and not disclosed to non-parishioners without consent.

1.4 Where can I find our data protection policies, procedures and forms?

Our latest documents always can be found at http://www.douaiparish.org.uk/privacy.html; please note that any downloaded or printed copies may no longer be current.

1.5 Can I give someone another parishioner's phone number or email address?

If you are acting on your personal behalf (i.e. not as an employee, volunteer or committee member of the Church), then GDPR does not apply and you may use your personal judgement.

If acting on behalf of the Parish, it is not permitted to pass the contact details of a parishioner, volunteer or committee member (i.e. a 'data subject') to someone who is *not* a parishioner without the data subject's consent; in this case we should simply relay a message asking the data subject to contact the enquirer. However, if the contact details have already been published with consent, then they may be freely shared.

The contact details of volunteers and committee members may be shared *with other parishioners* where this is necessary for carrying out their roles. This is covered under the lawful basis of 'legitimate interest', so consent is not required. (This does not include publishing details on a website and/or newsletter, as these may be read by non-parishioners; a Consent Form should be used for this).

1.6 Can we request prayers for named individuals at Mass, or in our newsletter?

Yes, but a Consent Form should be used for this, as non-parishioners may hear or read the details.

1.7 As membership of a church is considered to be 'special category' data, must letters or documents regarding parishioners be sent by special delivery?

If large amounts of data are being sent, or if the data is particularly sensitive, it must be either hand delivered or sent by special delivery or courier. Otherwise it is acceptable to use standard mail.

1.8 Whom can I contact regarding privacy and data protection in the parish?

We can be contacted at the following addresses:

privacy.alcester@douaiparish.org.uk

privacy.kemerton@douaiparish.org.uk

privacy.ormskirk@douaiparish.org.uk

privacy.scarisbrick@douaiparish.org.uk

privacy.stratford@douaiparish.org.uk

privacy.studley@douaiparish.org.uk

privacy.woolhampton@douaiparish.org.uk

2 TECHNICAL

Please note that DAPT is not responsible for the content of external sites, links to which are provided for information only. DAPT does not endorse any particular hardware or software, and takes no responsibility for maintaining or repairing any hardware or software owned by its volunteers.

2.1 Why is it necessary to use the latest versions of software?

Electronic devices are more vulnerable to data breaches if their software is not up to date. In many cases, software is updated automatically. Because of the variety of software used, we are not able to offer advice on this.

2.1.1 Does this mean that I can no longer use Windows 7?

After January 14, 2020, Microsoft will no longer provide security updates or support for PCs running Windows 7, and it recommends moving to Windows 10. In the meantime, it is still OK to do church-related business on a Windows 7 computer, but after that date Windows 7 PCs will become more vulnerable to security risks and should not be used.

You can find more information here.

2.2 How can I password-protect a Word document?

Windows (Microsoft): Click here

iOS (Apple): Click here

2.3 How can I password-protect an Excel spreadsheet?

Windows (Microsoft): Click here

iOS (Apple): Click here

2.4 How can I password-protect a PowerPoint presentation?

Windows (Microsoft): Click here

iOS (Apple): Click here

2.5 Is it necessary to encrypt electronic devices that contain personal data?

It is not necessary to encrypt electronic devices, but it is generally advisable to do so where possible, as it makes it considerably more difficult to access their contents without authorisation.

At a minimum, electronic devices should be password-protected. But note that the *unencrypted* hard drive of a password-protected computer can be simply removed and accessed by another computer.

Storage devices such as USB sticks should be encrypted, as they are easily lost or stolen.

2.6 How can I encrypt a computer?

Windows (Microsoft): *BitLocker* encryption is available on some Windows computers (but not on Windows 10 Home). More here.

MacOS (Apple): On modern Apple Mac computers, *FileVault* encryption is turned on by default. More here.

2.7 How can I encrypt a mobile phone?

Android (Google): Since the release of Android 7.0 Nougat (August 2016), encryption is required by default, so if phone you're using originally came with Android Nougat or a newer version of Android it is already encrypted. Encrypting an older phone may cause performance issues.

iOS (Apple): iPhones are encrypted.

2.8 How can I encrypt a USB stick?

Some USB drives come with their own encryption software, and it is also possible to download encryption packages separately.

2.9 What should I do if my mobile device is lost or stolen (including how to find the device, and how to remotely wipe data)?

Android (Google): Click here.

iOS (Apple): Click here and here.

Windows (Microsoft): Click here.