Archdiocese of Southwark

# GDPR Training Session

# WHAT WE ARE GOING TO COVER

1. Legislation and Principles
2. Personal Data
3. IT Policy and Practice
4. Subject Access Requests
5. Breaches
6. Roles and Responsibilities
7. Privacy Notices and Consent
8. Right to be Forgotten
9. Cameras
10. Insurance

# 1. LEGISLATION

- Overview
- Key Elements of GDPR
- Terminology
- Lawful Basis for Processing Data
- Direct Marketing
- GDPR Principles

# OVERVIEW OF THE LEGISLATION

- **What is GDPR?**
- The *General Data Protection Regulation (GDPR)* are the new regulations that require all organisations to strengthen their protection of personal data. GDPR builds upon the existing data protection legislation.
- This new legislation is effective from *25th May 2018.*
- We will be expected (by this date) to, at the very least, demonstrate that we are working in the right direction in terms of the way that we protect the personal data they are responsible for.
- If the requirements put in place by this new legislation are not met, then we will potentially face large fines as a consequence and risk damage to our reputation.

# KEY ELEMENTS OF GDPR

- **Lawful basis for processing** – we must now specify a legal basis for processing personal data – **consent** can no longer be presumed
- **Security breaches** – large fines are now imposed for loss or theft of data and/or data being viewed by people who shouldn't see it.
- **Storage of data** – we need to take more stringent steps to store hard copy and electronic data securely.
- **Subject access requests** – these will now have to be completed within 30 calendar days, with no charge and will be easier to make.
- **Right to be forgotten** – people can request certain data to be eliminated from their records.
- **Audit** – we need to be able to demonstrate that we have handled our data correctly.
- **Roles and responsibilities** – we all have a responsibility to look after the personal data of others.

# TERMINOLOGY

- **Data Controller** – this is the Roman Catholic Archdiocese of Southwark. Parishes will be responsible for their local data, acting as an agent of the Archdiocese.
- **Data Processor** – a person or organisation who processes our data on our behalf. This will include third parties such as solicitors and accountants.
- **Data Protection Officer (DPO**) – this is a role which will act on behalf of the Archdiocese in managing our relationship with the Information Commissioners Office (ICO)
- **Personal Data** – is defined as any data by which a living individual can be identified. Even if the person has been anonymised if we hold the data by which that person can be identified it is still classed as personal data. Some types of personal data will be classed as Special Personal Data, and that would include things like medical conditions, DBS disclosures, etc.
- **Whose personal data do we have** - clergy, parishioners, employees, volunteers and others associated with the parishes or agencies, for example, club members.
- **Legal Reason for Processing**

# LAWFUL BASIS FOR PROCESSING PERSONAL DATA

**1. Consent:** the data subject has given clear consent for you to process their personal data for a specific purpose.

- The GDPR sets a high standard for consent. It must be freely given, specific, informed, active, explicit and able to be withdrawn. For example, individuals should be asked to tick a box and sign to confirm their consent to particular actions. If you rely on consent, you must keep a record of when and how the consent was given.
- It is preferable not to rely solely on consent where possible because consent can be withdrawn at any time, which can cause difficulties with keeping data up-to-date. We will use consent only in a limited number of specific instances – eg fundraising and images.

**2. Contract:** the processing is necessary for a contract you have with the data subject, or because they have asked you to take specific steps before entering into a contract.

- For example, requesting an employee's bank account details in order to make their salary payments, which you have to do under their contract of employment.

# LAWFUL BASIS FOR PROCESSING PERSONAL DATA

**3. Legal obligation:** the processing is necessary for us to comply with the law (not including contractual obligations).

- For example, in certain circumstances we would be under a legal obligation to report certain personal data to the statutory authorities – e.g. police investigation.

**4. Vital interests:** the processing is necessary to protect someone's life.

- Note that this only applies in 'life or death' situations, (e.g. you could inform paramedics of an individual's medical condition if they are unable to do so).

# LAWFUL BASIS FOR PROCESSING PERSONAL DATA

**5. Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

- e.g maintaining marriage records.

**6. Legitimate interests:** the processing is necessary for the Data Controller's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

- This is likely to be the biggest reason for us in processing personal data – e.g including the processing of personal data about parishioners and volunteers by parishes, so that volunteer rotas can be compiled and information about services, news and events can be provided to parishioners. Gift aid processing will fall under legitimate interest.

# LAWFUL BASIS FOR PROCESSING SPECIAL CATEGORY PERSONAL DATA

- For **special category data** you need to identify both a lawful basis for processing ( as set out above) **and** an additional condition for processing this type of data. The most relevant condition will be that you have the **explicit consent** of the data subject. However, there is also a 'charities' condition which means that consent is not required where special category data is being processed:
- in the course of the Diocese's legitimate activities;
- with appropriate safeguards;
- relating solely to the members or former members of the diocese or to persons who have regular contact with the diocese in connection with its purposes; and
- the personal data is not disclosed outside the diocese without the consent of the data subjects

# DIRECT MARKETING

- There are special data protection rules around direct marketing and these come under the Privacy and Electronic Communications Regulations (**PECR**), which sit alongside GDPR
- Electronic Direct Marketing does not just apply to goods and services but also to the promotion of aims and ideals
- Fund raising will fall under the PECR
- Specific consent is required for electronic direct marketing
- Guidance on PECR will be provided on the website

# SIX DATA PROTECTION PRINCIPLES

**1. Processed fairly, lawfully and in a transparent manner.**

- We must identify the legal basis on which we are relying to process each category of personal data and we must inform Data Subjects what we are doing with their personal data by giving them a 'Privacy Notice'.

**2. Collected for the specific purposes about which you have informed the data subject and not used for any other purposes.**

- e.g. if we collect personal data about a job applicant, we cannot then use that data to send them news about the Diocese and its activities.

**3. Adequate, relevant and limited to what is necessary to achieve your stated purposes.**

- Ensure the data collected is really needed for the purpose for which it is collected, e.g. you do not need details of a parishioner's medical history, GP or next of kin to send them a newsletter, but you may if they are going on the diocesan pilgrimage to Lourdes.

# SIX DATA PROTECTION PRINCIPLES

**4. Accurate and, where necessary, kept up to date.**

- All personal data is to be checked at appropriate intervals (eg annually) to ensure it is still required for the purpose for which it was obtained and that it remains accurate. Any data which is out of date or inaccurate should be corrected immediately and data which is no longer required (retention periods) should be securely deleted or destroyed.

**5. Kept in a form which permits identification of data subjects for no longer than is necessary to achieve the stated purposes.**

- The retention schedule in the policy gives guidance on how long personal data must be retained.

**6. Kept safe and secure. This includes protecting the data against unauthorised processing and against accidental loss, destruction or damage.**

- Security of data is imperative. As so much personal data is stored electronically, we must ensure that our IT systems are secure against malicious attacks and that we have appropriate IT security systems and procedures in place to guard against accidental loss or disclosure. This includes up-to-date anti virus software.
- Physical security measures are also essential – all paper files must be kept under lock and key and if they contain Special Data they must be in a safe.
- Unauthorised access must also be prevented – ie only those who have a genuine need to see the data should be allowed to see it

# 2. PERSONAL DATA

- Current Situation
- Retention Periods
- Hard Copy Data

# PERSONAL DATA
# CURRENT SITUATION

- **Parish Audit** – following the online questionnaire we sent out, it is apparent that in most parishes some personal data is being held at home (primarily by volunteers) in both hardcopy and electronic formats.
- **Getting Control** – as long as personal data is held at people's homes (or anywhere else offsite), we don't have control over it. For example, other family members may use the laptop or PC or have a shared email address, which means that personal data may be viewed by people who should not see it. This is a breach. We need to know where the data is and how it is being used.
- **Retention** – different types of data need to be retained for certain periods – this is known as a retention period – after this period it can be securely destroyed. If you keep it, you need to keep it securely and keep it up-to-date, so don't keep what you don't need to.
- **Disposal** – a disposal register must be maintained to demonstrate what data has been destroyed. This is a simple list of what data is destroyed on what date. Your contact for disposal is on the Contacts page.

# HARD COPY DATA

- We should be aiming to minimise the amount of hardcopy data we retain on a regular basis.
- We should be working towards scanning documentation and only keeping hardcopies when we really have to – what MUST be kept, where and for how long.
- All personal data must be kept under lock and key, however, for special category personal data it will need the added security of being attached to the walls or floor, e.g a safe. This is to prevent the risks of loss or theft.
- Safeguarding and Marriage Tribunal records and registers MUST be kept in such devices.
- Physical copies of data can no longer be kept at home. You should all now be taking the steps recommended to gain control of hard copy data.
- If any personal data is lost, stolen or seen by someone who shouldn't see it, this will be a breach and we could face fines of varying degrees depending on the nature of the personal data. Breaches of special category personal data will attract a larger fines.
- You should operate a **Clear Desk Policy** – i.e. NO documents containing personal data should be left on your desk

# 3. IT POLICY AND PRACTICE

- IT Policy
- IT Changes
- Standardised Email Addresses
- Electronic Records
- IT Changes Time Frame
- Dependencies

# IT POLICY AND PRACTICE

- **IT Policy** – will be available in the website www.rcsouthwark.co.uk which details how you should handle personal data held in an electronic format.
- **Changes to IT** – we are introducing a number of changes to software and hardware. These include common email addresses, office 365, encryption software and remote access.
- **Impact on parishes** – these changes may require your parish to make some changes to your IT set up.
- **ChurchSuite** – some parishes are using (or intending to use) ChurchSuite for their parish database. Please check that any bespoke package is GDPR compliant.

# STANDARDISED EMAILS

- Starting in June 2018 we will be introducing a *Diocesan standardised email address*. This means that everyone's emails will have the common extension of: **** @rcaos.org.uk
- Clergy will have a personal @rcaos.org.uk email address – e.g. peterpaul@rcaos.org.uk and parishes will have function specific email addresses – e.g. doverga@rcaos.org.uk for gift aid at Dover parish
- Safeguarding will have a separate domain to ensure independence and that the Special Category Personal Data has an extra level of security: doversg@safeguardrcaos.org.uk
- All users will be required to use these accounts for sending and receiving correspondence which is diocesan based.
- ON NO ACCOUNT should users use non-diocesan email accounts.
- Users should ALWAYS password-protect any attachments which contains personal data. This can be done by creating the message in say, Microsoft Word.

# STANDARDISED EMAILS

- POST HOLDER DETAILS – will be maintained centrally so that we know to whom each email address belongs: Name and main phone contact number (could default to the parish phone number). We will require their external email account so as to send the registration details and how to access their Office 365 account.
- IT WILL BE THE RESPONSIBILITY OF THE PARISH to inform IT Support of change of incumbent.
- This will also ensure a proper back up of emails and will make responding to subject access requests quicker and easier.

Archdiocese of Southwark

# ELECTRONIC RECORDS

- It is increasingly easy to store all types of data electronically and we want to encourage that where ever possible.
- This enables us to store the data more securely and access it more readily. However we do need to update our electronic storage and access to meet current security standards.
- Office 365 will be implemented across the Diocese.
- Office 365 provides each user with up to 1 terrabyte of free storage. Parishes and users will start to receive their registration information from the beginning of June 2018.

# IT CHANGES TIME FRAME

- All parish roll outs to be done in alphabetical order
- June 2018 - commence roll out of diocesan email addresses using Office 365
- June 2018 – Parishes and agencies to complete the IT Equipment Form available on the website. If help is needed after completion please contact ICTsupport@finance-rcdsouthwark.org
- June/July 2018 - Introduction of a standard anti virus software application
- November 2018 - introduction of remote access

# WHAT YOU WILL NEED TO DO ..

- In order to operate Office 365, you will require a web browser which is running its latest version. Access is via a URL link: https://outlook.office365.com
- In order for your PC to be prepared for encryption, it should have Windows 7 Enterprise (minimum) or Windows 10 PRO (preferred) loaded
- Office 2016 Pro is the recommended software application suite
- MACS: latest operating system version is recommended. Together with latest version of Microsoft for MACS.

# WHAT YOU WILL NEED TO DO ..

- Please contact ICTsupport@finance-rcdsouthwark.org if you need help in checking any of this information
- If you need to upgrade any hardware or software please do so via the Finance Office
- If you have a parish website please check that the company which hosts your website is GDPR compliant

# 4. SUBJECT ACCESS REQUESTS

- A ***subject access request (SAR)*** is a request by an individual to see what information an organisation holds about them. A SAR is a right under the *GDPR* legislation, that enables individuals to see the data and also to verify that their data is being lawfully processed.
- Currently the SAR has to be a formal request in writing. After 25th May, the SAR no longer needs to be formal although still needs to be in writing. The request could now be made via *email* or through social media platforms such as *Facebook and Twitter.* If you have any of these locally you will need to check them regularly.
- Currently we have 40 calendar days to respond to a SAR, after 25th May we will only have 30 calendar days to respond in full.
- We will also no longer be able to charge for a SAR.
- If you receive a subject access request please pass it immediately to the DPO. He/she will make the necessary ID checks and put the wheels in motion.

Archdiocese of Southwark

# 5. BREACHES

- Breaches MUST be reported in 72 hours – this means they must be reported to the Data Protection Officer (DPO) asap
- Failure to report a breach will result in a fine even if the breach is not material. You MUST NOT make any decisions about whether or not the breach is material.
- Material breaches can attract punitive fines – up to 20m euros – dissuasive!!
- Fines are not covered by insurance
- Examples of breaches include: loss or theft of a mobile device containing personal data – whether or not it is material depends on encryption; somebody reading the contents of a letter left on a desk (or kitchen table); publishing the photograph of first Holy Communion children without their parents consent; others in FAQs

# 6. ROLES AND RESPONSIBILITIES

- The *GDPR* introduces the duty for organisations to appoint a *Data Protection Officer(DPO)* if they are a public authority or of a certain size. We meet this criteria so we will be appointing a *DPO*.
- The *DPO* will be an expert in data protection and will advise us on our data protection obligations and provide advice on how to protect data.
- We will be appointing a *DPO* who is external to the Diocese to avoid any potential conflicts of interest. The *DPO* has a direct reporting line to the Information Commissioners Office (ICO).
- We also intend to recruit someone internally to manage the day to day demands of GDPR.
- We all have a duty to protect personal data

# 7. PRIVACY NOTICES AND CONSENT

- Under the new legislation we need to update our records about how we use personal data. Consent to use personal data can no longer just be presumed and may not necessarily be the best lawful basis in all circumstances. If you seek consent, you need to ensure that it remains current.
- If consent is not given, you must delete the data for that particular use.
- Privacy notices must be issued to advise data subjects about how their data is being used.
- Consent Forms and Privacy Notices will be provided.

# 8. RIGHT TO BE FORGOTTEN

- This element of the *GDPR* legislation originates from social media and provides a right for individuals to have their personal data erased from an organisation in certain circumstances.
- The right to be forgotten applies to:

❑ When the personal data is no longer necessary in relation to the reason it was originally collected,

❑ When the individual withdraws consent

❑ When the individual objects to the processing and there is no overriding, legitimate reason to continue with it.

- Legitimate interest or legal reasons mean that we do not necessarily have to comply with a request to be forgotten – all cases will be considered on their own merits.

# 9. CAMERAS

- CCTV
- Photographs and Live Streaming

# 9. CCTV SIGNAGE

- *CCTV Signage* is now a necessity. If you have *CCTV* cameras in operation, you must make sure that the public are aware, and have been notified appropriately about *CCTV* cameras operating in their vicinity.
- The signage for the *CCTV* cameras should be:

❑ Clear and easy to read,

❑ Legible in context – larger signs for people in moving vehicles to see,

❑ Visible anywhere people can appear on camera, even if this is slightly outside your grounds,

❑ Labelled with the organisation that's operating the system,

❑ Labelled with the name and details of the company who manages the camera in public places.

❑ Labelled with the details of the Data Controller and the DPO.

# PHOTOS AND LIVE STREAMING

- If you take photographs or live stream services or events, you should bring people's attention to this beforehand.
- Display a sign permanently in the parish advising that, on occasions, there may be photographers present at church services and, by attending those services, individuals give their permission to use any general crowd shots they appear in for parish or diocesan printed publications and websites.
- Display specific signs prominently on days when photographs or live streaming is taking place.
- You **should not** use individual or small group shots of people without asking for consent first.

# 10. INSURANCE

Our current insurance with CIS covers us for:

- Legal costs and expenses of pursuing or defending actions under the Data Protection Acts 1984 and 1998. This will be upgraded for GDPR.
- Includes appeals to the ICO following a refusal of an application to alter registered particulars or against any enforcement, de-registration or transfer prohibition notice.

The insurance will not pay for:

- Cases without reasonable prospect of success.
- Legal expenses arising from the policyholder's intentional wrongdoing.

So, we must be able to prove that we have taken all reasonable steps to comply with the legislation.

# CONTACTS

- ❑ Email: GDPR@finance-rcdsouthwark.org or
- ❑ ictsupport@finance-rcdsouthwark.org
- ❑ Telephone: 020 7960 2500
- ❑ Website: www.rcsouthwark.co.uk
- ❑ Data Protection Officer: Name & Contact Details
- ❑ Updates: Finance Office News
- ❑ Secure data disposal:
  - Restore Datashred - Account Number 4955234
  - Contact Martin Vodden 07523 514798 or

martin.vodden@restore.co.uk