General Data Protection Regulation

Manual

Diocese of Meath

Part 1 – GDPR Overview 4

Diocesan Data Protection Officer: David O'Brien

Tel: 086 792 7844 Email: dpo@dioceseofmeath.ie .

Part 1 – GDPR Overview

1 Introduction

1.1 Purpose

The Diocese is committed to operating a robust Data Protection ("DP") framework which, through embedded culture, practice and accountability, will:

- Put data subjects and their DP and privacy rights first;
- Ensure that the Diocese operates in accordance with the relevant data protection legislation;

The objective of this policy document is to provide an overview of our DP framework to illustrate how we comply with our DP obligations and to ensure that clergy and laity understand their role and responsibilities in the context of DP.

1.2 Scope & Applicability

This policy applies to the processing of personal data by all clergy and laity working as employees or volunteers in the Diocese and Parishes.

1.3 What is Data Protection?

Data Protection relates to the protection of personal data, which is any information that can be used to identify a living person or any information relating to an identifiable living person.

That “living person” is known as a Data Subject and can be a member of the clergy, a lay person, applicants for sacraments, an employee, job applicant, volunteer, or any other individual. The Diocese intends that the capture and handling of personal data should be kept to a minimum. It can be in any format or medium, including data held on our I.T. systems or on paper records, photographs, CCTV and audio.

1.4 How does Data Protection impact the Diocese and Parishes?

Instances where we encounter Data Protection applies:

- The Sacraments: both preparation and the sacrament itself e.g. information gathered as part of preparation and photographs taken for parish purposes.
- Capturing information about donors e.g. in relation to Tax Rebate Scheme.
- Capturing information of volunteers and employees e.g. names, addresses and PPS numbers.
- Safeguarding – case files; vetting files; records of attendance at training events; records on recruiting; consent forms; accident/incident report forms; disciplinary or grievance proceedings.
- CCTV
- Webcam
- Websites, Social Media platforms, etc

The above list should not be considered exhaustive.

1.5 Sensitive Data

The Diocese treats the following types of personal data as sensitive and therefore requires everyone to apply additional care and protection when Processing:

- Children: (i.e. individuals under the age of 18): The Diocese recognises that children may be less aware of the risks involved in the processing of their personal data and therefore will apply particular protection in the event that any personal data of children is processed.
- Other vulnerable people's personal data: We consider the following to be "vulnerable":
    - mentally ill persons; and
    - on some occasions, employees or volunteers, where there is potentially an imbalance in the relationship;

A vulnerable person is defined as *'Any person in a state of infirmity, physical or mental deficiency, or deprivation of personal liberty which, in fact, even occasionally, limits their ability to understand or to want or otherwise resist the offence'*. (Vos Estis lux mundi [VELM])

- Special categories of data:
    - This includes the types of personal data that reveal any of the following information relating to an individual: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership.

Special Category Personal Data also includes the processing of genetic data, biometric data (for example, fingerprints or facial images), health data, data concerning sex life or sexual orientation.

- Information linked to household and private activities. For example, additional personal data about family relationships as part of sacramental preparation.

For more guidance or assistance when processing sensitive personal data, please contact the DPO.

2 Communication and Contact

The Diocesan Data Protection Officer (David O'Brien) can be contacted by phoning 086 792 7844 or via email at dpo@dioceseofmeath.ie .

3 Roles and Responsibilities

Everyone is accountable for their own behaviour and is responsible for the way personal data is used and protected. Employees and volunteers have the following responsibilities:

- To ensure all processing of personal data is undertaken in accordance with this policy.
- To keep personal data secure.
- To complete all assigned DP training.
- To report any Data Subject Rights request or suspected data breach immediately to the DPO.

- To report to the DPO anything that may put personal data or compliance with this policy at risk.
- **To consult the DPO at an early stage in all new projects and initiatives.**

4 Data Protection Principles

Whenever personal data is processed in any way, everyone involved is responsible for ensuring that all personal data is processed in accordance with the following principles:

- Obtaining and processing the information fairly
- Keeping it for one or more specified, explicit and lawful purpose
- Using and disclosing the information only in ways that are compatible with these purposes
- Keeping the information safe and secure
- Keeping the information accurate, complete and up-to-date
- Ensuring that the information is adequate, relevant and not excessive
- Retaining the information for no longer than is necessary
- Give a copy of the personal information to an individual following the Data Subject Access Request. If in receipt of a request, please contact the Diocesan Data Protection Officer by phoning 086 792 7844 or via email at dpo@dioceseofmeath.ie .

5 Legal basis for processing data

The legal basis for the Diocese and Parishes for processing data is as follows:

- Explicit consent [1] of the data subject so that they can be informed about news, events, activities and services, for processing donations and keep them informed about events in the Parish / Diocese.
- Processing of personal data is necessary for carrying out obligations under employment law, financial laws and other legal requirements.
- Processing is carried out by a not-for-profit body with a religious aim provided that the processing relates to congregation members or former members (or those who have regular contact with the Parish / Diocese in connection with those purposes) and
- There is no disclosure to a third party without consent except to comply with legal and statutory obligations. [2]

6 Data retention

Data is retained in accordance with the guidance set out within Irish data protection legislation and other relevant laws. For example:

- records of donations and associated paperwork are retained for 6 years after the calendar year to which they relate.
- Parish registers such as Baptisms, Marriages, Confirmations are kept permanently.

- Records of Garda vetting are retained until the conclusion of the Garda vetting process. Thereafter, all documentation gathered during the vetting process will be returned to the applicant or destroyed.
  A record that a Garda vetting check has been carried out is retained in line with data protection legislation.
- In relation to safeguarding documentation.

7 Transparency

The Diocese is legally obliged to provide specific information to Data Subjects about how their personal data is being processed. This information is typically shared via a "privacy policy" and/or "privacy statement". [3]

The DPO is responsible for ensuring that appropriate privacy notices are maintained for all personal data processing activities that relate to data subjects. Diocesan entities and parishes are responsible for ensuring that such policies or privacy statements are available to and are accessible to data subjects in electronic or paper format.

The minimum information to be made available to data subjects when collecting personal data directly from them is:

- The identity and the contact details of the relevant Data Controller at diocesan or parish level;
- The purposes and legal bases for the processing;
- The recipients or categories of recipients of the personal data;

- Retention periods, or the criteria for determining the retention periods;
- The data subject's rights under data protection legislation;
- The process available to Data Subjects to withdraw consent;
- Any obligations on the Data Subject to provide the personal data and the possible consequences of failing to do so;
- Reporting requirements on mandated persons.

8 Data Subject Rights

Under the GDPR, an individual has the right to request access to the personal information held about them. Any requests should be addressed to the Parish Priest. Requests should be dealt with, within 30 days of receipt, unless there is a justifiable reason for the delay. Data subjects have the following rights:

- *Right of Access* – They have the right to access information that is held about them.
- *Right of Correction* – They have the right to correct information that is inaccurate or incomplete.
- *Right of erasure* – In certain circumstances they have the right to ask for data held about them to be erased i.e. the right to be forgotten.
- *Right to Restriction of Processing* – Where certain conditions apply they have the right to restrict processing of personal data.
- *Right of Portability* – Subject to certain circumstances, they have the right to have any data that is held about them

transfer to another organisation, where it is held in electronic form.

- *Right to Object* – They have the right to object to certain types of processing of data.
- *The Right to lodge a complaint* with the Data Protection Commissioner's Office.

If in receipt of a request in relation to these rights, please contact the DPO as soon as possible to ensure that such requests are dealt with appropriately.

9 Data Security

One of the key tenets of the GDPR legislation is keeping data secure. This requirement exists whether we are working in an office, at home or elsewhere. The following practices are recommended:

- There should be no login / password sharing. Each individual should have a unique login.
- All laptops / computers should be encrypted as well as password protected. Encryption is the process of converting data on a computer/laptop into a code to prevent unauthorised access and provides a further layer of security to the data stored. Encryption software should be installed by the firm that supplied your equipment.
- If transporting a diocesan or parish laptop, care must be taken to ensure they are not visible in a car and that the car is locked. If travelling on public transport it should be kept with you at all times. No other members of your household should be permitted to use it.
- Ensure anti-virus software is installed, up to date and enabled on all computers. As far as possible ensure you are

using the latest version of operating systems that your equipment will support.

- Ensure the laptop is stored securely both in the office and at home.
- Ensure the device is locked when not in use.
- Only use diocesan or parish e-mail accounts for 'work' matters.
- Always double check when sending an e-mail in order to ensure:
    - It is going to the correct recipient.
    - BCC (Blind Carbon Copy) is used when sending e-mails to multiple individuals. An e-mail address is personal data and should not be shared with other people/ organisations.
    - If there is an attachment, that the correct document is attached.
    - If replying all, ensure:
        - such an action is necessary;
        - BCC is used
          (even if the original sender did not use BCC)
- Ensure data is securely backed up at all times.
- If a computer device is lost or stolen, it should be immediately reported to:
    - The Parish Priest if it is in relation to a Parish; or
    - The Diocesan Secretary, if a diocesan device;
    - and in all cases to the DPO in order to determine whether a data breach has occurred.

- Paper records which include confidential or private information, should also be carefully protected by:

- Ensuring that all paper files are stored securely when not in use.
- Keeping records in a locked file when transporting. They should not be visible in a car. Transporting paper records should be kept to a minimum and a record of who has removed the records and the timing of their return should be maintained (i.e. a sign out/sign in sheet).
- Ensuring paper records are destroyed in accordance with the diocesan data protection policy.

10 Data Breaches

A "Data Breach" is where personal data has been accidentally or unlawfully lost, stolen, damaged, altered or disclosed to an unauthorised person. This includes sending personal data about someone to the wrong person. It also includes a cyber-attack (such as our systems being hacked) and where a device with access to personal data has been lost (such as leaving a laptop on public transport).

All Diocesan and Parish personnel must immediately report any potential data breach to the DPO as soon as it is identified and, as required, assist the DPO with the management of the data breach.

The obligations of the Data Controller include:

- notify the DPC of any data breach which presents a risk to the affected data subjects within 72 hours of becoming aware of the data breach; and
- where that risk is high, to notify affected data subjects in the case of certain types of data breaches.

The DPO is responsible for notifying the Data Protection Commissioner (DPC) and will support the Controller in determining if the breach should be considered a high-risk breach.

11 Key Actions for Diocesan Organisations / Parishes

Please ensure the following:

- An up-to-date Data Protection Notice is prominently displayed in a public area.
- If using livestream and / or CCTV equipment, have appropriate notices prominently displayed in a public area.
- **If any formal requests are received in relation to Data Privacy of GDPR matters, e.g. Data Subject Access Requests, requests for erasure/rectification, contact the DPO for guidance.**

Footnotes

1. **Explicit Consent**
   - *A specific type of consent where an individual is clearly and expressly asked to agree to a particular use of their data.*
   - *It involves a direct and unambiguous action, such as signing a consent form or checking a box that is not pre-checked.*
   - *Explicit consent is often required for processing sensitive personal data.*
   - *It must be freely given, specific, informed, and unambiguous.*

2. **Mandatory Reporting**
   The provision of information to statutory authorities for the protection of children is not a breach of confidentiality or data protection.

   Mandated persons (as defined in the Children First Act 2015) are people who have contact with children and/or families and who, because of their qualifications, training and/or employment role, are in a key position to help protect children from harm. Mandated persons include professionals working with children in the education, health, justice, youth and childcare sectors. Certain professionals who may not work directly with children, such as those in adult counselling or psychiatry, are also mandated persons.

   The list also includes registered foster carers and members of the clergy or pastoral care workers of a Church or other religious

community. All clerics and religious are to be considered mandated persons. Volunteers are not mandated persons under the Children First Act 2015. However, DLPs or Deputy DLPs who are volunteers are classed as mandated persons under Church standard.

The Criminal Justice (Withholding of Information on Offences against Children and Vulnerable Persons) Act 2012 requires that any person who has information about a serious offence against a child, which may result in charges or prosecution, must report this to An Garda Síochána. Failure to report under the Act is a criminal offence under that legislation. This obligation is in addition to any obligations under the Children First Act 2015.

3. **To access the Diocesan Privacy Policy/Privacy Statement**, click on, https://www.dioceseofmeath.ie/dataprotection

Part 2: Key Notices and Forms for Organisations / Parish

There are a number of notices, procedures and forms which are required for GDPR purposes. These may be downloaded from the Diocesan website as required on,

https://www.dioceseofmeath.ie/dataprotection

They are included here for information purposes.

12 Data Protection Notice

[Insert name of Parish] - Data Privacy Notice

[Insert Name of Parish Priest & Parish Contact Details]

The document provides a policy statement regarding the data protection obligations of our Parish, thus ensuring that we comply with Data Protection Regulations within Irish Legislation. This policy applies to all personal data collected and stored in the course of its activities.

What is Personal Data?

Personal Data relates to a living individual and from this data an individual can be identified. This policy covers both personal and sensitive personal data held in relation to data subjects of the Parish. This policy applies to personal data held in any format. The processing of personal data is governed by the General Data Protection Regulations (GDPR).

How we Process your Personal Data?

_____ is the Data Controller. The Parish complies with its obligations under GDPR by;

- Obtaining and processing the information fairly.
- Keeping it for one or more specified, explicit and lawful purpose.
- Using and disclosing the information only in ways that are compatible with these purposes.

- Keeping the information safe and secure.
- Keeping the information accurate, complete and up-to-date.
- Ensuring that the information is adequate, relevant and not excessive.
- Retaining the information for no longer than is necessary.
- Giving a copy of the personal information to an individual following the data subject access request procedure.

What do we use your Personal Data for?

Data is collected from parishioners, employees, volunteers and contractors.

- To administer records held by us on members of the congregation e.g Baptismal, Confirmation and Marriage Records.
- To manage rotas for altar servers, Extraordinary Ministers of Holy Communion, Ministers of the Word etc.
- To manage our employees and volunteers.
- To maintain our accounts and records including the processing of donations and tax rebates.
- To fundraise and promote the interests of the parish.
- To inform you of any news, events and activities that are running in the Parish.

What is the Legal Basis for Processing your Personal Data?

- Explicit consent of the data subject so that you can be informed about news, events, activities and services, for processing your donations and keep you informed about events in the Diocese.
- Processing of personal data is necessary for carrying out obligations under employment law, financial laws and other legal requirements.
- Processing is carried out by a not-for-profit body with a religious aim provided that the processing relates to congregation members or former members (or those who have regular contact with the Parish in connection with those purposes) and
- There is no disclosure to a third party without consent except to comply with legal and statutory obligations. [3]

Sharing your Personal Data

Your personal data will be treated as strictly confidential and will only be shared with other clergy or staff of the parish for purposes connected to the Parish. We will only share your data with third parties outside the parish with your consent.

How long do we keep your Personal Data?

We retain data in accordance with the guidance set out within Irish Data Protection Legislation. Specifically, records of donations and associated paperwork are retained for 6 years after the calendar year to which they relate. Parish registers such as Baptisms, Marriages, Confirmations are kept permanently.

Your Rights and Your Personal Data

Under the Data Protection Regulations, you have the right to request access to the personal information held about you. Any requests should be addressed to the Parish Priest (contact details below). Requests should be dealt with, within 30 days of receipt, unless there is a reason for the delay, which is justifiable. **You have the following rights:**

- **Right of Access** – You have the right to access information we hold about you.
- **Right of Correction** – You have the right to correct information that is inaccurate or incomplete.
- **Right of Erasure** – In certain circumstances you can ask for data that we hold about you to be erased i.e. the right to be forgotten.
- **Right to Restriction of Processing** – Where certain conditions apply, you have the right to restrict processing of your personal data.
- **Right of Portability** – Subject to certain circumstances, you have the right to have any data that we hold about you transferred to another organisation where we hold it in electronic form.
- **Right to Object** – You have the right to object to certain types of processing of data.
- **The Right to lodge a complaint** with the Data Protection Commissioner's Office.

Further Processing

To exercise any relevant rights, queries or complaints please contact:

Parish Priest: _____

Phone: _____ **E-mail**: _____

You may also contact the Data Protection Commissioner Office on 00-353-57-8684800 or Lo-call 1890-252-231 or by e-mail info@dataprotection.ie or by Post to; Data Protection Commissioner, Canal House, Station Road, Portarlington R32 AP23 Co. Laois or their Dublin Office, 21 Fitzwilliam Square, Dublin 2 D02 RD28.

13 CCTV Procedure

_____ Parish CCTV Procedure

The Parish of _____ is committed to protecting your privacy. This CCTV procedure explains our data processing practices in relation to CCTV.

CCTV (Closed Circuit Television) captures images of identifiable living people (Data Subjects), for security purposes. This identifiable imagery is considered as personal data under GDPR and therefore from a data protection perspective, requires the same level of care that is given to paper and electronic personal data.

A surveillance camera system includes:

- Closed Circuit Television.
- Any other system for recording or viewing visual images for surveillance purposes.
- Any systems for storing, receiving, transmitting, processing or checking images or information obtained by a system failing in (a) or (b) above.
- Any other system associated with, or otherwise connected with systems failing in (a), (b) or (c) above.

Purpose of CCTV in the Parish

Under GDPR Regulations, the processing of Personal Data needs to be lawful, fair and transparent. CCTV in our Parish is for security purposes only.

Informing Data Subjects about CCTV

Our parishioners, staff, volunteers, visitors who are all data subjects are informed of the existence of CCTV by placing signs near entrances and other areas where CCTV cameras are located. These signs are easy to read and contain the name of the security operator and their contact details. The CCTV sign clearly states that the purpose of the CCTV is for security purposes only.

Storing of CCTV data

CCTV images are captured onto a secure server which is only accessible to the Parish Priest or those whom the parish priest has authorised access for security purposes. Images are deleted every _____days.

An Garda Siochana is allowed to view CCTV footage if a crime has been committed and this does not pose any data protection issue. In situations where a crime has been committed, the images may need to be retained longer as evidence. If a copy of images is requested by An Garda Siochana, they must provide a written authorisation by the Local Superintendent. For practical purposes, and to expedite a request speedily in urgent situations, a verbal request may be sufficient to allow for the release of the footage sought. However, any such verbal request should be followed up with a formal written request. This ensures the chain of evidence is not compromised if images are needed for legal purposes.

Storage or access to CCTV images is considered processing personal data, so it is imperative that the parish and security operators (if applicable) uphold the integrity and confidentiality of the footage captured.

Screens displaying live or recorded footage should only by viewed by authorised individuals and not be visible to members of the public.

Back up tapes/disks are stored in a secured environment with an access log maintained and access should be restricted to authorised personnel only. If back-ups are cloud based, the parish will ensure that the cloud data centre is based in the EU.

Your Rights as a Data Subject

As with any aspect of personal data, data subjects have a right to access any images captured of them. The person must complete a Subject Access Request Form which will require a form of personal identification (Forms available from the Parish Priest) and as much information as possible should be gathered from the individual regarding dates, times when their image may have been captured. The Parish and security operators (if applicable) will need to ensure that the data requestor is present in the footage and that in supplying the footage that they do not disclose any personal data of another data subject. This may involve blurring parts of the footage such as other persons or licence plates. The Parish will endeavour to respond to your request for CCTV footage within **30 days** from receipt of the Subject Access Form and an appropriate form of identification enclosed.

14 GDPR Guidelines on Photography for Diocese and Parishes

GDPR Guidelines on Photography for Diocese & Parishes

The following guidelines have been developed to help Diocese/Parishes comply with GDPR when using photography at events. Personal data is any information relating to a living individual, which is capable of identifying that individual. As photos capture the personal data of an individual, they are subject to GDPR legislation.

If a Diocese/Parish uses photography at an event, consideration should be given as to the appropriate means of obtaining consent or permission.[4] A photograph that can uniquely identify an individual or a group of people, cannot be published without consent. Consent must be obtained before the photograph is taken and publication extends to parish newsletters, journals, magazines, websites or social media.

Consent must also be given if a photograph is taken of a child (under the age of 16 years) or a vulnerable adult. Article 8 GDPR states

"where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility of the child".

Consent is **not required** if you cannot uniquely identify a person or group if the shot is a long shot, people present are aware that a photographer is present at the event and no names are published.

Consent is also **not required** if a photograph is being taken for personal use like a parent taking a photograph of **their** child.

How do you gain consent?

At the Diocesan/Parish event, all attendees must be **informed** that photographs are going to be taken.

Consent can be obtained in a number of different ways:

1. If an invitation is sent out in advance of an event, attendees should be notified that:
   (a) A photographer will be present at the event.
   (b) Detail the reason why the photographs are being taken e.g. to document, record and share the event.
   (c) Who to contact at the event if a person does not want their photograph to be used?
2. By displaying a prominent notice containing the information in point 1 (a)-(c) above informing the attendees at the event. This notice could be published on the newsletter, website and displayed at the entrance of the church or location of the event.
3. A clear announcement is made before a group photo is taken and attendees have the opportunity to step out of the photo.
4. The photographer asks the individual for consent to take their photograph and keeps a written record that consent has been given.

Photographs of Children and Vulnerable Adults

Consent is always required when taking photographs of children under 16 years of age or vulnerable adults. Consent must always be given by the individual as well as a parent/guardian or carer by a consent form before photographs are taken. If a parent/guardian/carer is present at an event, they can give verbal consent to take a photograph. The photographer should record that explicit consent has been given.

Prevention of Data Breaches

A personal data breach **is a breach of security** leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to **personal data**. It can be described more simply as an incident whereby information is stolen or taken from a Diocese/ Parish without permission or consent. This includes breaches that are the result of both accidental and deliberate causes.

Photographs taken on behalf of a Diocese/ Parish should be treated in the same way as personal data held in hard or soft copy in the Diocesan/Parish Office. Photographs should be securely stored in the Diocesan/Parish office adhering to the same safeguards as other personal data. Images on cameras should be transferred to a secure location and deleted from memory cards. Phones and tablets should be protected by the use of passwords and encryption. If Diocesan/Parish photographs are subject to a data breach, please contact the DPO immediately.

15 GDPR Guidelines for Parishes using Webcams

Webcam Guidelines for Live Streaming of Liturgies (no recording)

Web cams stream images of identifiable individuals over the internet via a web camera and no recordings take place. Their use, however is regarded as the processing of personal data and is subject to the GDPR. One of the key provisions regarding the processing of personal data is that it should be done with the consent or knowledge of the individuals concerned. The following guidelines will help you with GDPR compliance:

- Place notices in the parish newsletter that a web cam is in operation and inform parishioners of the liturgy schedule that will be live streamed on the internet.
- Place signage at each entrance to the church and in other prominent locations informing people that web cameras are in operation. Also inform parishioners of the liturgy schedule that will be live streamed.
- A sign should also be placed in the Sacristy to inform visiting priests and others of web cam use.
- Cameras should only be switched on for the duration of Mass or Liturgy and switched off at the end.
- During any broadcast it should be possible to stop transmission, if necessary, by quickly accessing the control panel of the system. If this cannot be done by the priest from near the altar, someone should be delegated to break transmission when necessary.

- Camera images of the congregation should be wide shots minimising the possibility of easily identifying individuals with close up shots. This is particularly relevant for funeral ceremonies.
- No live streaming should take place once the ceremonies have finished.
- With regard to altar servers and others children taking part in Liturgies it is advised that consent is obtained from their parents/guardians. [6] The parental/guardian consent given for the use of media/webcams in the Safeguarding Forms (Altar Server Applications Form or Child & Parent/Guardian Joint Activity and Media Consent Form) will be sufficient for parental/guardian consent.
- Cameras should be installed with due care and respect in church buildings. They should not be permanent fixtures. They should be easily removable without any impact on the building.
- The installer and operator of the web cam system is known as a Service Provider or Data Processor (third-party) under the GDPR. You are required to have a Service Provider Agreement in place with them. This Agreement details what you allow them to do with your data; what security standards should be in place and what verification procedures may apply. It ensures that any sub-contractors they employ, e.g. maintenance engineers, follows this agreement. The parish will be open to data breaches if the Service Provider or one of their sub-contractors can distribute or remove personal data in the form of images without following your agreement.

- Service providers may be able to access the web cams remotely and they may be able to give regular, accurate information regarding the number of people who actually log on to view Liturgies from a parish in order to assess the value of web broadcasting. ***This will have to be included as part of a parish's Privacy Statement as people are entitled to know this information.***

Webcam Guidelines for Recording Liturgies and/or Recording for Security Purposes.

If a webcam is used to record, this is considered processing of data and therefore subject to the GDPR. Prominent notices should be placed in the newsletter and on church entrances, informing parishioners that recording is taking place for a particular service or liturgy with dates and times given.

If a webcam is recording for security purposes, ensure CCTV signs are visible.

Any act of storage or access is considered processing and it is imperative that the Parish and security operators uphold the confidentiality and integrity of any footage.

Back-up tapes/discs should be stored in a secure environment with an access log maintained (similar to CCTV). Access should be restricted to authorised personnel only. If back-ups are being stored on the Cloud then the Parish Priest needs to know where the Cloud data centre is based. If it is in the European Economic Area (EEA) there is no problem but if it is located outside of the EEA then you will have to get your system operators to move it.

16 Guidelines using Social Media to Broadcast Mass and Religious Ceremonies

Many parishes have put in place or are considering the use of social media such a Facebook Live or Instagram Live to stay connected to parishioners.

With any technology, one has to consider the data protection implications. While not advocating any particular social media technology, data protection will be considered with regard to Facebook Live in these guidelines.

What is Facebook Live?

Facebook Live is a feature of Facebook social media, that uses the camera on a computer to record a mass or religious ceremony. The video is subsequently uploaded on to a parish Facebook page, allowing parishioners to view it.

Once a video is uploaded it is being live streamed on the internet. Facebook will then automatically save a parish's live broadcasts after they end, so the video will remain in the video section of the parish's Facebook page allowing parishioners to view at any time.

Data Protection Considerations

- Before commencing broadcasting, ensure settings are set to the intended audience – public view to any subscriber of Facebook or limited transmission to a particular group?
- Set a retention period for uploaded videos and then delete them. They should only be retained for as long as required.

- If it is possible for viewers to post comments on the uploaded video, this should be monitored.
- If any third parties are present in a video, it is important to gain their consent before uploading the video on to the parish social media page.
- In some cases, family members are requesting to live stream a funeral service. In these circumstances, the video can be uploaded to the family member's social media page. The parish in this case does not need to obtain consent from any third party that is present in the video.
- If the parish is livestreaming the funeral service, at the request of the family, they must obtain the consent of any third parties present in the video, before the video is uploaded on to the parish's social media page.

17 E-mail guidelines for Diocese and Parishes

E-mail is an effective way of communicating to large groups of people. However, care must be taken to ensure that GDPR is not inadvertently breached. The following guidance should be adopted where possible:

- The 'BCC' function should be used wherever possible when sending information to a groups as:
    - This prevents sharing of e-mail addresses which may be against a recipients wishes.
    - This will also prevent any accidental or inappropriate use of the 'reply all' function.
- Care should be taken to ensure any e-mails are only sent to the intended recipients. Be wary of the 'autocomplete' function in email programs as the proposed address my not be the one you wish to use. You should carefully check the recipients of an e-mail before pressing send.
- Use of e-mail groups can reduce the risk of sending an e-mail to the wrong person. However, care should be taken to ensure that the group is kept up to date and that anyone who requests to be removed from the group is deleted from the e-mail group promptly.
- If an attachment is being sent then care should be taken to ensure that the correct item is being sent. If the information in the attachment is confidential or sensitive then it should be protected with a strong password that cannot be easily guessed. The password should be communicated to the recipients via another method and not in the e-mail.

18 Guidelines for Dealing with Requests for Baptism, Confirmation and Marriage Certificates

Parishes may receive requests for copies of Baptism, Confirmation and Marriage Certificates. A new standard request form has been compiled to make it easier for Parishes to deal with such requests and to comply with GDPR Regulations **(Please See Form A002).**

Please adhere to the following guidelines:

- Please ensure that Form F001 is completed by all persons requesting a Sacramental Certificate.
- If the person requesting the certificate is known to you, they are not required to produce up to date photographic identification. However, it would be advisable to note on the Request Form that the person requesting the certificate is known to you.
- If the person requesting the certificate is **not** known to you, the person must produce an up to date form of photographic identification. You do not need to take a copy of the photographic identification.
- If the person authorised to **collect** the Sacramental Certificate is not known to you, photographic identification must be produced. You do not need to take a copy of the photographic identification.
- Always ensure that the photographic identification is **in date.**

- Parishes also receive requests via e-mail or telephone requiring copies of Sacramental Certificates. Such requests will be dealt with in the same way. If the person requesting the certificate is for example living abroad, e-mail the Request Form, which they must fill in and also scan in a copy of up-to-date photographic identification. Once you have seen a copy of the up to date photographic identification, please ensure to then **delete** it from your records.
- The same rules will then apply as in point 4 above re collection of certificates.
- You can retain this request form for a period of 12 months and then dispose safely by shredding.

19 Privacy Notice for Pre-Nuptial Enquiry Form, Supporting Documentation & Marriage Register

This information is gathered to facilitate your wish to get married in the Roman Catholic Church.

The Pre-Nuptial Enquiry Form (PNEF) is normally completed by a priest or deacon *(amend as per your parish)* in your parish of residence. It is his record of his preparation with you and your freedom to marry. The PNEF and supporting documentation (baptism certificate, letter of freedom to marry, marriage preparation certificate etc.) are stored in the place of marriage.

The entry in the Marriage Register is a permanent record. To facilitate the issuing of Marriage certificates, the information is also retained on the Pastoral Management System *(amend as to your parish).* The information will not be used for any other purpose.

20 Volunteer Confidentiality Agreements

Please see Agreement A001 Volunteer Confidentiality Agreement for Diocese to help them comply with GDPR. Volunteers at Diocesan level may have access to a lot of personal data and sensitive personal data about parishioners, finances and diocesan business etc.

Any person that carries out voluntary work for the Diocese, please get them to complete this form to comply with GDPR and return to the Diocesan Office. Again, if the person ceases volunteering for the Diocese, please ensure to dispose of this form safely by shredding.

Footnotes

4. Media Permission Form S4.12
   https://www.meathsafeguarding.ie/section-4/#toggle-id-1