Data Protection Handbook Diocese of Achonry

February 2019

Foreword

The Catholic Church recognises that good pastoral care and respect for the dignity of every person requires that personal data should be sourced, stored, processed and eventually disposed of in an appropriate manner and welcomes the essential principles underlying the GDPR.

Important Terms (Non Exhaustive)

Personal Data is understood as "any information relating to an identified or identifiable natural person".

Data Processing refers to any activity undertaken involving interaction with a Data Subject's personal data. Data Subjects are afforded far reaching rights under Data Protection legislation.

A **Data Subject** is the natural person whose personal data is being processed.

The **Data Controller / Data Processor** is the person or organisation involved in data processing activities. A large amount of responsibility is imposed on data processors and controllers under Data Protection legislation.

The **Data Protection Officer** is the person nominated by the Diocese to support all activities in relation to Data Protection compliance.

Informed, explicit and unambiguous **consent** are required in order for us to process personal data, unless we are, for example, processing data in the **legitimate interests** of our Diocese. Where contact with a Parishioner falls outside of this e.g. an email address given for Parish Readers' Rota is used to contact a Parishioner about an upcoming fundraising event, we have fallen outside the scope of legitimate interest and must instead seek the explicit consent of the Parishioner to gather and use their contact details. Data subjects are entitled to **withdraw** their consent at any time.

We define **retention periods** to determine how long we can store Personal Data in our Diocese. During the annual review, retention periods apply to hard and soft copies of all documents and files, as well as any back-ups which may exist. This means that archives and old storage devices/locations are also subject to the annual review.

Under current legislation, all Data Subjects have the **right to erasure**, more commonly known as the "right to be forgotten"

If you are in doubt as to the potential Data Protection implications of a task you are about to undertake, please complete a **Data Protection Impact Assessment** in order to determine your next steps.

A **data breach** occurs where a breach of security leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to,

personal data which we as a Diocese have transmitted, stored or otherwise processed

When a data subject submits a **Subject Access Request** to receive a copy of all the information we hold on them, we must respond within one month of receiving their request. If information relating to the data subject references a third party we may not be required / allowed to disclose.

D**ata Protection in the Diocese**

Data Protection is embraced at all levels across our Diocese. In our day to day activities, the following activities ensure that we are data aware and data compliant:

Consent:

- All application and registration forms for lay ministry, fundraising activities, pilgrimages, etc., will now include a paragraph on consent, which will also mention how the Parishioner can **"opt out"** of receiving communication.
- Where a Parish / Diocese can categorically say that they will not contact a Parishioner for any other reason than that for which they have signed up, they do not have to gather consent. However, all instances where a Parishioner's name is published, e.g. Website or Parish Newsletter will require consent.

Contracts and third parties:

- Absolutely **all** third party service providers and contractors **must comply** with current Data Protection legislation.
- When engaging in contract negotiations with any third parties who will be processing personal data on behalf of the Parish or Diocese, it will be ensured that they take a rigorous and proactive approach to maintaining data security.
- Contracts and Service Level Agreements must feature a paragraph on Data Protection to ensure our and our contractors' compliance with legislation.

Computers and laptops:

- Only suitable Authorised Persons have access to files and databases containing personal data. Where Employees or Volunteers carry out their

work externally, due care must still be taken in relation to the security of personal data.
- Access rights to files and databases containing personal data are regularly reviewed and updated.
- Passwords in use are unique and are not shared.
- Files are saved in suitable folders, protected where necessary and not readily accessible e.g. saved on desktop.
- Computers are regularly locked when unattended or not in use.
- Email addresses which are used are those that have been assigned to them, avoiding unsafe platforms like Gmail or Yahoo.
- Email signatures feature a confidentiality disclaimer.
- Printouts containing personal data are disposed of by shredding only.
- Files containing Personal Data are regularly checked for accuracy and relevance. Any Personal Data which is no longer in use should be removed from files. Personal Data should only be retained for a period of time that is perceived to be **reasonably necessary**. Retention of Personal Data on a "just in case" basis poses a risk to GDPR compliance.
- Parish and Diocesan websites include a comprehensive and up to date Privacy Policy.
- Where databases and software solutions are provided by third party contractors, compliance is guaranteed through the SLA.

Accounts:

- Only Authorised Persons shall have access to files in the Accounts department. Where Employees or Volunteers carry out their work externally, due care must still be taken in relation to the security of personal data.
- Retention periods for files kept in the Accounts department should be in line with Revenue requirements (See Payroll/Personnel Files below).
- Access to Accounts Files will be physically restricted by means of secured storage, e.g. locked filing cabinets or combination safes.
- Information relating to financial contributions received will be treated in the strictest confidence to avoid potential data breaches.
- Invoices / Bills / Purchase Orders must be kept for a **minimum of 6 years before being destroyed** in line with Revenue requirements. Please note that this means six years after the transaction or project has been completed as opposed to started.

- Monthly/Annual reports sent from Parishes to the Diocesan Accounts department will be password protected and/or saved into a secured shared folder.
- Where accounts are managed by means of a software system, e.g. Surfaccounts, care should be taken to regularly change passwords in order to avoid unauthorised access. This is particularly important when Employees / Volunteers have external access to accounts e.g. from their own home.

Buildings, Property and Projects:

- Deeds and documents relating to property in the Parish or Diocese's portfolio are retained by the Diocese. Access to these documents will be physically restricted by means of secured access, and only Authorised Persons shall have access to these files.
- Documents relating to ongoing or past building projects in the diocese shall be subject to the following retention periods:
    - Tender documents, contracts and agreed specifications for minor and repair works to existing buildings should be retained for **6 years after completion of works**.
    - All documents relating to major building works should be **retained indefinitely and transferred to the Diocesan archive.**
    - Any documents relating to Parish boundaries should be **retained indefinitely and transferred to the Diocesan archive.**

Payroll and Personnel Files:

- Due to the sensitive nature of Personnel File content, only Authorised Persons shall have access to Personnel Files, e.g. only the Parish Priest will have access to the Personnel Files for his Parish.
- Where Employees or Volunteers carry out their work externally, due care must still be taken in relation to the security of personal data.
- Access to Personnel Files will be physically restricted by means of secured storage, e.g. locked filing cabinets or combination safes.
- An annual check of the content of all Diocesan / Parish Personnel Files will be undertaken by the relevant Authorised Persons.
- The following retention periods will apply to Personnel file contents:
    - Application details for candidates who were unsuccessful in a recruitment campaign should be kept for **12 months from date of rejection**.

- Terms and conditions of employment must only be retained for the duration of employment. These records should be kept for no longer than **12 months after the cessation of employment.**
- Payslips / proof that an employees was paid in line with the National Minimum wage should be kept for **6 years after cessation of employment**.
- Records of weekly worked hours, the name and address of employee, the employee's PPS numbers and a statement of their duties as prescribed under the *Organisation of Working Times Act 1997* should be kept for **3 years after cessation of employment.**
- Records relating to employees who were under the age of 18 (if applicable) for the period of their employment should be retained for a period of **3 years after cessation of employment**.
- In cases of collective redundancies (if applicable), records should be retained for **3 years from the date of redundancy**.
- Where an employee avails of parental or force majeure leave during the course of their employment, the *Parental Leave Acts 1998-2006* provides for retention of records for **8 years from cessation of employment**.
- Employee tax records must be kept for **6 years from cessation of employment**.
- Signed Confidentiality Agreements should be kept for **6 years from cessation of employment**.
- Where an employee is involved in a workplace accident, records of this should be kept for **10 years from cessation of employment**.

- A common sense approach will also be taken. Personnel files should contain only factual information pertaining to a person's employment, and should not contain any notes or subjective opinions in relation to any of the records mentioned above.

Child Safeguarding Files:

- Only Authorised Persons shall have access to Safeguarding Information, e.g. the Bishop, Chancellor, Director of Safeguarding and Designated Liaison Officer.
- Access to the files will be physically restricted by means of secured storage, e.g. locked filing cabinets or combination safes. This same level of security is applied to **all** Safeguarding related documents in archives.

- Safeguarding records are held in perpetuity. This includes the information recorded in each Parish's sacristy register.
- In general, a common sense approach to the contents of documents related to Safeguarding must be taken. These records should contain only factual and relevant information, and should not contain any personal notes or subjective opinions.
- An annual check of the content of all Diocesan / Parish Safeguarding records will be undertaken by the relevant Authorised Persons.

Parish Files and Records:

- Only Authorised Persons shall have access to files containing Personal Data at a Parish level, e.g. the Parish Priest and/or Secretary.
- Access to these files will be physically restricted by means of secured storage, e.g. locked filing cabinets or combination safes. Particular care will be taken in relation to Safeguarding files.
- An annual check of the content of files containing Personal Data will be undertaken by the relevant Authorised Persons. This content check will ensure that information held in each Parish is relevant, accurate and not being retained for longer than necessary.
- The following retention periods will apply to Parish Files and Records – every effort will be made to keep this list accurate and up to date:
    - Safeguarding files, e.g. application forms: Held **in perpetuity**.
    - Parish Sacramental Registers: Parish Sacramental Registers have a permanent reference and should be held **in perpetuity**.
    - Sacramental Application Forms: Sacramental Application Forms are intended for the purpose of facilitating sacramental preparation, celebration and registration, and have no purpose once the sacrament has been celebrated and registered. They should be destroyed **within 12 months of celebration**.
    - HR/Personnel Files: Please see Policy on Personnel File Management for specific information.
    - Contact details and other personal data of lay ministers, fundraisers, etc.: these should only be retained for **as long as the Parishioner is engaged in ministry or other activities on behalf of the Parish**.
    - Minutes from Meetings: Meeting minutes should only contain a factual account of what was discussed and agreed during a meeting, without referring to opinions expressed by individuals.

Minutes should be kept for **as long as is deemed reasonably necessary**. During the annual content check, the Authorised Person for the Parish or Diocese should use their judgement to decide on this. **Keeping minutes on a "just in case" basis poses a risk to GDPR compliance.**

- Records of one to one meetings: Insofar as is possible, please apply the same logic as above.
- Records of contributions and donations: these should be anonymised insofar as is practical, and access to contributor details should only be assigned to Authorised Persons. These details should be kept for **as long as is deemed reasonably necessary**, giving due consideration to Revenue requirements.
- Correspondence to and from parishioners or others about the activity of the parish: details of correspondence must only be retained **where and for as long as is reasonably necessary**.

Planned Giving Envelopes

- Planned giving envelope boxes containing the name and address of a Parishioner are effectively an example of sensitive personal data, as they show a person's religious affiliation. As a result, the Parish should take reasonable care that this Personal Data is protected when the boxes are being distributed. If boxes are collected by Parishioners, they should not be left in the Church outside of Mass times, but rather locked in the Sacristy. If they are distributed by Employees or Volunteers, please ensure they have signed confidentiality agreements with the Parish.
- Software and/or files linking Planned Giving envelope numbers with the name of the Parishioner should be password protected and only accessible by suitable Authorised Persons.

CCTV, Webcams and Livestreaming:

- CCTV recording takes place in order to detect intruders, and will not be used for the purposes of monitoring employees or volunteers.
- All buildings and surrounding areas covered in the scope of CCTV cameras will be clearly outlined on a Risk Assessment / overview which will be made available upon request.
- Notices will be put in place to inform all potential Data Subjects of the presence and purpose of CCTV cameras.
- CCTV footage will be retained for a period of 30 days, **unless required for the purposes of an investigation**.

- Outsourced CCTV services must comply with the above requirements.
- Webcams and Livestreaming have been introduced solely as an alternative means for Parishioners to enjoy the celebration of Mass and the Sacraments. Webcams in Churches are not used to monitor Employees or Parishioners.
- Notices will be put in place to inform all potential Data Subjects of the presence and purpose of the webcams. The scope of the webcam(s) will be indicated at the entrance to the Church, to afford Parishioners the opportunity to "opt out" of streaming or recording.
- Recordings of a small number of celebrations will be retained for one month, e.g. Christmas. In these instances, the Parish Priest will make an announce at the beginning of the celebration to ensure the consent of Parishioners present. Where children or vulnerable adults are taking part in a celebration, consent and/or parental consent will be sought in advance.
- Outsourced Webcam and Livestreaming services must comply with the above requirements.

Social Media and Websites

- Social Media sites e.g. Facebook or Instagram operated by the Parish or Diocese should have restricted edit access.
- Posts or photographs which contain personal data must have the prior consent of the Data Subject before being posted on social media or websites.
- Posts or photographs which contain personal data must be deleted or archived after **one year**. If the information is archived, suitable location and access must be defined.

Requests for Certificates

Copies of certificates held in the Parish or Diocesan offices can only be requested in writing and registers are not to be made accessible to the public. These written requests should be destroyed once processed. If you have any doubts regarding the identity of the person requesting the information, reasonable means should be used to confirm identity. The "100-year rule" will be used to reasonably assume whether someone is dead or still protected by Data Protection legislation.

Subject Access Requests

Subject Access Requests must be received in writing and referred **immediately upon receipt** to the Data Protection Officer. If a SAR is made verbally, please advise the Data Subject to send their request in writing to a suitable postal or email address. The DPO can be informed via phone or email of the SAR, and should be forwarded a copy of the written request as soon as possible. The DPO will then work together with the impacted Diocese / Parish to ensure that the SAR is completed at no cost to the Data Subject, within one month of receipt. Certain exceptions will apply, whereby the Diocese may not be required or legally permitted to release certain data, but this will be discussed and clarified with the DPO and, where necessary, the Diocese's appointed legal counsel. If you have any doubts regarding the identity of the person requesting the information, reasonable means should be used to confirm identity.

Right to Rectification

All Data Subjects have the right to have their information updated or removed where it is not accurate, provided it will not impact on the rights and freedoms of another natural person. Again, these requests should be received in writing and processed at the earliest convenience. If you have any doubts regarding the identity of the person requesting the information, reasonable means should be used to confirm identity.

Data Protection Impact Assessments

DPIAs should form the basis for all new processes in the Diocese which will involve data processes. DPIAs are similar to Risk Assessments, in that they will identify the potential challenges posed by implementing new processes, and also identify potential solutions to offset these challenges. The DPO can provide a DPIA checklist.

Data Breaches

First and foremost, we must all be completely committed to the avoidance under all circumstances of Data Breaches. Data Breaches must be reported to the Office of the Data Protection Commissioner within 72 hours, unless the breach poses no risk to the rights or freedoms of any natural person. Where we do not report the breach within 72 hours, we must inform the Data Protection Commissioner of the reasons for the delay. If you suspect or, even accidentally, cause a Data Breach, please contact the Data Protection Officer **immediately** to discuss next steps.

All third party service providers associated with the Diocese are obliged to comply with this requirement.

Right to Erasure

All Data Subjects have a right to be forgotten, where requested. This can pose certain difficulties for the diocese under Canon Law. The Right to Erasure cannot be invoked in cases of legal disputes or investigations, e.g. in Child Safeguarding matters. Where a Parishioner, for example, requests to be forgotten by virtue of leaving the Catholic Church, it is our current understanding that we may retain certain factual records, e.g. entries on baptismal records. This may be subject to change following future guidance from the Data Protection Commissioner.

Annual Reviews

Annual reviews should be completed at times which are practical and convenient for the Parish or Diocese, but **must be completed**. To this end, the Parish or Diocese may choose to split their full Annual Review over three separate review periods, which is facilitated in the annual review template. The responsibility for full completion will lie with the Parish or Diocese themselves.

Implementation and Assurance

Every effort will be made to ensure adherence to this handbook. To this end, the Data Protection Officer will carry out ad hoc, unannounced visits to Parishes in order to provide feedback on the current status of compliance. This is foreseen to begin within 12 months of the initial rollout of the handbook, and will be purely on a support / assurance basis. Earlier visits can be planned with the DPO where additional support with implementation is required. Feedback will be provided by way of a report, which will be provided to the Parish Priest and Bishop/Archbishop.

Contact

For all queries relating to the above, please contact the Diocesan Data Protection Officer, Darina Ryan-Pilkington, at dpo@elphindiocese.ie or 0852848825.

CCTV

Re: CCTV Policy

Morning All,

Hope you're well. Please see template CCTV Policy attached. Please distribute where applicable.

It is absolutely essential that appropriate signage is in place where CCTV is in operation.

It is also important that all Parishes and Dioceses where CCTV is in operation contact their CCTV provider to ensure that they are DP compliant and can facilitate the following:

- Subject Access Requests, i.e. have the appropriate technology to pixelate out images if one Data Subject requests their recordings

- A detailed breakdown of camera specification (see policy template)

- Automatic or supervised deletion of recordings: we will struggle to justify keeping recordings for more than 30 days outside of an ongoing investigation. CCTV providers should ensure automatic deletion of data OR be on site every 30 days to manually ensure same.

- Access to CCTV systems is clearly defined. If access to the CCTV system does not or cannot match the template attached, please agree appropriate system access with the provider. If in doubt, contact me directly.

Please edit this policy where appropriate to ensure it is fit for your purposes.

I'm working on a webcam/livestreaming policy at the moment and would appreciate contact details for Parishes (except Knock Shrine) using webcams to see what their current setup / policy is.

As always, please feel free to contact me with any queries. Thanks for your help!

Best Regards,

Darina Ryan-Pilkington

dpo@elphindiocese.ie <mailto:dpo@elphindiocese.ie>

0852848825

CCTV Policy – Diocese/Parish of XXXXX

Closed Circuit Television cameras operated on this premises are regulated in accordance with the GDPR and the Data Protection Act, 2018. This Policy was last reviewed in May 2018 and is subject to change.

Purpose of recording

CCTV recording on this premises takes place for the safety and security of employees and visitors, and in order to detect intruders.

CCTV will only be used for the purposes of monitoring employees and visitors where there is an established risk to their Health & Safety, e.g. in locations where accidents have previously happened. Notices will be put in place should such monitoring take place.

CCTV will not be used for covert surveillance unless in conjunction with an investigation and where approved by legal counsel and/or An Garda Síochána.

System Access

Our system is operated and maintained by _____. Access to the CCTV is only as necessary and by suitably authorised personnel e.g. Security manager, staff of _____ and the Parish Priest. Equipment is tested and monitored in a planned and coordinated manner.

System Specifications

The CCTV system is a conventional static system. It records digital images and is equipped with motion detection. It records any movement detected by the cameras in the area under surveillance, together with time, date and location. There are no pan and tilt cameras in operation on this premises. ***** PLEASE CONFIRM SYSTEM SPEC WITH PROVIDER AND UPDATE ACCORDINGLY***** Images which are recorded are of sufficient quality to support identification of individuals captured.

Cameras are in operation 24 hours a day, 7 days a week.

Cameras will not overlook or record any external spaces or property. Where this cannot be avoided, the relevant owner will be consulted.

Signage

Appropriate signage is displayed in prominent locations on the premises to ensure awareness of employees and visitors.

Retention of Data

CCTV recordings are retained for no longer than 30 days, unless required as evidence in legal proceedings. Access to recordings is restricted to the Security Manager, the Parish Priest and suitable personnel from the CCTV service providers, who are bound by the same privacy standards as ourselves. We require all security staff to have signed non-disclosure / confidentiality agreements prior to gaining access to CCTV recordings. ***Please confirm CCTV provider can delete every 30 days***

Subject Access Requests

Data Subjects who have been recorded on CCTV must submit Subject Access Requests in writing (emails are also sufficient). Once received, the requested data will be issued within one month. CCTV service providers must be suitably qualified to pixelate images of other Data Subjects captured in recordings. ***Please ensure CCTV provider can facilitate this***

An Garda Síochána

Access to CCTV recordings can be granted to members of an Garda Síochána when submitted via the appropriate Garda Data Protection form for the purposes of an investigation.

CONSENT FORM

Memo

To: All Parishes, All Dioceses

From: Darina Ryan-Pilkington, DPO (dpo@elphindiocese.ie)

Re: Generic Consent Form

Hi All,

Attached is a template consent form for distribution across the Diocese. Gathering consent allows us to continue processing Personal Data as we had before, but in a way that is now compliant with Data Protection legislation.

- The priest in each Parish should make copies of this form available beside the sacristy register and ask that all Parishioners involved in lay ministry, altar serving, etc. sign this form.
- The Parish Priest should take responsibility for ensuring that all relevant Parishioners complete the form, and that they are only contacted for the purposes to which they have consented.
- The completed forms should be kept as a record of consent for as long as the Parishioner is involved in the work of the Parish.
- Going forward, we should reference the consent we have gathered if we decide to use a Parishioner's contact information, e.g. "You are receiving this email because you have consented to us contacting you in relation to.."
- In a similar way, we have offered and must continue to offer the opportunity to "opt out" of this communication, e.g. "If at any time you wish to opt out of receiving these emails, please contact.."

Note: It is my opinion that including all Employees / Lay Ministers / Altar Servers / Volunteers / Choir Members allows us to ensure a stronger level of data compliance. If you can categorically exclude any of these groups from the

requirement for consent, it is at your discretion to do so, but please consider the resulting Personal Data processing restrictions.

Note: It is at the Parish's / Diocese's discretion to post these forms instead of managing them through the sacristy, but please consider the time and cost involved.

Note: Consent is an essential element of Data Protection compliance. Please treat the completion and storage of these forms as a priority.

Please feel free to contact me with any questions relating to the implementation of the above.

Thank you!

Darina Ryan-Pilkington

Consent Form for Employees / Lay Ministers / Altar Servers / Volunteers / Choir Members (where applicable)

Parish / Diocese _____

Name _____

Address _____

Email _____

Phone No. _____

Your privacy is important to us. As part of the new Data Protection legislation governing Ireland, we are required to keep a record of your consent to process your personal data. Your personal data includes your name, email address, address and phone number. We will only keep your personal data for as long as it is necessary, i.e. for as long as you are involved in the work of our Parish, and it will not be passed on to any unauthorised third parties.

Thank you for taking the time to participate in and enhance the work of our Parish/Diocese.

We would like to continue to contact you in relation to the activities you undertake with us. Please tick this box to confirm your consent ☐

From time to time, we will include details of the work you undertake on our Newsletter / Bulletin Board / website, e.g. serving and reading rosters. Please tick this box to confirm that you consent to this ☐

On certain occasions, e.g. the celebration of Sacraments, Christmas etc., we would like to publish images from our celebrations on our website and/or Social Media platform. Please tick this box to confirm that you consent to this ☐

We would also like to contact you in relation to other activities we feel might be of interest to you, e.g. Pilgrimages, Faith Formation, fundraising, etc. Please tick this box to confirm that you consent to this ☐

If at any time you would like to withdraw your consent to any of the above, please contact your Parish Priest.

Signed _____

Date __ /__ /__

In cases of Children (under 18), please provide a parent/guardian signature below:

Signed _____

Date __ /__ /__

Issued June 2018

In relation to Baptismal Certs and genealogy related requests that come into the Parish. I've clarified these points with a fellow DPO and Archivist in another Diocese, so am happy for this to be our approach going forward:

- Records held by the Church are private and should not be made available to the public. Requests for certificates should be made in writing, via letter or email.

- The "100 year Rule" in assuming a person is deceased is based on both Canon Law and Archiving principles. We will continue to use this as a means of reasonably assuming a person is dead and thereby not subject to Data Protection law.

- A living person requesting a copy of a certificate must be named on that certificate – again, the request should be submitted in writing. If the person is not known to the Parish Priest, they should take reasonable means to verify the person's identity. For example, somebody living abroad requesting a certificate should scan a copy of their ID to verify their identity. Once the certificate has been issued, the request can be deleted / disposed of.

- Given the time that may be involved in researching these requests, it is at the Parish's discretion to charge for this.
-

In relation to planned giving envelopes; I would be satisfied that the envelopes can be made available in Churches during Mass times, but should be removed to the Sacristy afterwards to risk exposure to third parties. Where the envelopes are distributed by Volunteers, it would be best practice that these Volunteers sign confidentiality agreements. It is at the discretion of the PP / Volunteer to leave a box of envelopes at a neighbour's house, once they can be confident that this is in the best interests of the Parishioner for whom the box is intended.

Any contact with Lay Ministers / Volunteers / Servers, etc. falls within the exception of "legitimate interests" in relation to consent, **provided there is no risk of exposure of their sensitive personal data e.g.**

named on newsletters, photos posted online, etc. Furthermore, without specific consent, we cannot contact these parties in relation to any other activity than the one they are involved in. I still strongly advise use of the consent forms.

I think it would be wise to seek consent of couples getting married, baptising children, etc. before publishing their details on a Parish newsletter / bulletin. I will be reviewing the various sacramental application forms with a view to standardising and including this requirement for consent. In relation to the Pre-Nuptial Enquiry form, I have started researching its contents and will follow up once I have a satisfactory answer.

I hope this goes some of the way to answering the outstanding questions. Thank you all for your time!

Best Regards,

Darina Ryan-Pilkington

dpo@elphindiocese.ie

085 284 8825

EMAIL SECURITY

Memo

To: All Parishes, All Dioceses

From: Darina Ryan-Pilkington, DPO (dpo@elphindiocese.ie)

Re: Email Security

Morning All,

FYI – last week we had our **first data breach** in the form of a compromised email account. The user in question has been proactive in notifying and taking first steps in relation to this breach. We are following the guidance of the Office of the DPC in relation to next steps. A **data breach** occurs where a breach of security leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data which we as a Diocese have transmitted, stored or otherwise processed.

I would like to once again stress the importance of email security. The most secure way of managing email accounts is having your own diocesan email address, supported and secured by a provider, e.g. secureparish@proactivediocese.ie ! Most Dioceses have an email domain name; it will be a matter of transitioning parishes onto these.

Please remember that when you use an email address whose security standards you can't vouch for, **you are putting the personal data of others at risk**. This is

particularly important for us, because by in large we are processing “sensitive” personal data – alluding to a Data Subject’s religious affiliation.

I would also suggest adding a privacy statement to the end of your email signature – like the one below which I copied from my colleagues in Elphin.

“Best Regards,
Joe Bloggs
secureparish@proativediocese.ie
0831234567

STRICTLY PRIVATE, CONFIDENTIAL AND PRIVILEGED
This e-mail and any files transmitted with it are strictly private, confidential and/or privileged. They are intended solely for the sole use of the intended recipient. The content of this e-mail and any files transmitted with it may have been changed or altered without the consent of the author. If you are not the intended recipient, please note that any review, dissemination, disclosure, alteration, printing, copying or transmission of this e-mail and/or any file transmitted with it is strictly prohibited and may be unlawful. If you have received this e-mail and any file transmitted with it in error, please notify JOE BLOGGS, secureparish@proactivediocese.ie and then delete it from your system.

It is possible for date transmitted by e-mail to be deliberately or accidentally corrupted or intercepted. For this reason, where the communication is by e-mail, PROACTIVE Diocese do not accept any responsibility for any breach of confidence that may arise through the use of this medium.”

Please feel free to contact me with any questions relating to the implementation of the above.

Thank you!

Darina

CONFIDENTIALITY AGREEMENTS

Memo

To: All Parishes, All Dioceses

From: Darina Ryan-Pilkington, DPO (dpo@elphindiocese.ie)

Date: 26/06/18

Re: Confidentiality Agreements

Morning All,

In order to firmly underpin our commitment to Data Protection across the organisation, it is essential to ensure that Staff and Volunteers acting on behalf of the Parish / Diocese have signed a Confidentiality Agreement. This gives us an added level of security when entrusting the processing of Personal Data and "sensitive" Personal Data to staff and volunteers.

A template Confidentiality Agreement has been attached for distribution. Please feel free to edit the CA as you see fit, taking care not to exclude any essential elements.

Note: It is important to clarify that the requirement for a CA is in no way a detraction from the very sincere trust we place in all Staff and Volunteers, or our gratitude for the excellent work they do.

Note: I would suggest that as best practice a confidentiality clause be worked into all contracts of employment where not already in place. If Staff / Volunteers have already signed a CA, there is no requirement for a second CA to be signed if the CA encompasses the same points as covered in the template.

Please feel free to contact me with any questions relating to the implementation of the above.

Thank you!

Darina

Confidentiality Agreement

DIOCESE/PARISH OF XXXXX

The Diocese/Parish of XXXXX is committed to protecting the Personal Data of all Employees, Volunteers and Parishioners in line with current Data Protection legislation. The Diocese/Parish acknowledges that Personal Data identifying is categorised as “sensitive” personal data and is therefore afforded a higher level of protection.

The Diocese/Parish of XXXXX is committed to protecting all information relating to the business, products, affairs and finances of the Diocese/Parish as well as trade secrets including, without limitation, technical data and know-how relating to the Diocese/Parish or any of its contacts.

To this end, the Diocese/Parish require that all Volunteers/Employees OBSERVE THE STRICTEST CONFIDENTIALITY when handling any personal or confidential information by virtue of their role within the Diocese/Parish.

Volunteers / Employees shall not directly or indirectly disclose any personal or confidential information which may come into their possession or procurement by virtue of their role to any person, body or corporation outside of the Diocese/Parish, unless directed to do so by Revenue authorities, a Court of Law or by the Diocese/Parish in the particular matter.

Volunteers/Employees shall, upon termination of their service or employment in whatever manner and for whatever reason, deliver

forthwith and without prior request, all documents, reports, specifications, charts, papers and other records (the property of the Diocese/Parish) which are in their possession, power or procurement.

Volunteers/Employees shall show due discretion when handling Diocesan/Parish information and shall not use or attempt to use, disclose or attempt to disclose, any Diocesan Information in any manner which may cause injury or loss to the Diocese/Parish or any other person/body.

Volunteers/Employees who process personal data or confidential information on behalf of the Diocese/Parish from their own home or any external location are required to keep this information secure to avoid unwanted or unlawful loss or disclosure.

I, the undersigned, being a Volunteer / Employee of the Diocese/Parish of XXXXX have read and understood the above statement, and agree to be bound by its terms both for the duration of my involvement in the work of the Diocese/Parish and indefinitely thereafter:

Signature: _____ Dated: _____

In line with our Data Protection Policy, this signed agreement will be kept by the Diocese/Parish for the duration of the Volunteer/Employee's role and for six years thereafter.

SERVICE LEVEL AGREEMENTS

Memo

To: All Parishes, All Dioceses

From: Darina Ryan-Pilkington, DPO (dpo@elphindiocese.ie)

Date: 24/07/18

Re: Service Level Agreements

Morning All,

In order to ensure that contractors who process personal data on our behalf are compliant with the new GDPR and Data Protection Act, an updated contract or service level agreement should be in place.

Attached is a template Service Level Agreement / Contract Addendum for your use. Examples of contractors who process personal data on our behalf are: CCTV providers, Webcam/Livestreaming hosts, email hosts, computer repair companies, printing companies, etc.

The template can be supplementary to your existing terms of engagement and filed as an addendum until the next negotiation of terms, and/or the text can be incorporated into your contract template for future use.

Please edit to insert the name of your Diocese / Parish where necessary.

Feel free to contact me with any questions relating to the implementation of the above.

Thank you!

Darina

TEMPLATE Service Level Agreement / Contract Addendum on Data Protection

This agreement between the Diocese of XXXXX and _____ comes into effect on the date of signing below and will be binding for an initial period of 12 months, with an automatic rollover period of an additional 12 months unless terms are renegotiated or cessation is invoked by either party.

The Diocese of XXXXX, giving due regard to GDPR and the Data Protection Acts 1988-2018, requires that all contractors processing personal data on its behalf are doing so on a lawful basis.

The Diocese understands itself to be the Data Controller in the context of third party contracts and/or agreements, while contractors fulfil the role of Data Processors.

The Diocese understands personal data as "any information relating to an identified or identifiable natural person". Personal data processed on behalf of the Diocese remains **at all times** the property of the Diocese.

The Diocese understands personal data processing as "any activity undertaken involving interaction with a Data Subject's personal data."

All Personal Data processed on behalf of the Diocese shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to the minimum range necessary in relation to the purposes for which they are processed;
- kept accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard

to the purposes for which they are processed, are erased or rectified without delay;

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

To this end, the Diocese requires that Data Processors ensure the following when processing personal data on its behalf:

- Data Processors employ suitably qualified staff, and/or provide all necessary training to ensure compliance
- Data Processors use appropriate, regularly updated technical resources when processing data for the Diocese
- Data Processors respond promptly and adequately to all requests in relation to personal data received from the Diocese
- Data Processors react promptly and adequately in notifying the Diocese where there is a suspected or actual personal data breach, allowing the Diocese to take necessary next steps
- Data Processors will facilitate any compliance based audit requested or undertaken by the Diocese during the term of the contract or agreement
- Upon cessation of the contract or agreement by either party, the Data Processor will either return all existing personal data to the Diocese, or delete the personal data in its entirety from their systems and files.
- Data Processors are at all times obliged to be able to demonstrate compliance with the GDPR and Data Protection Acts 1988-2018 (the obligation of ‘accountability’).

I, the undersigned Data Processor, have read and understood the Diocese's Service Level Agreement / Contract Addendum on Data Protection and agree to be bound by its terms for the period outlined above.

Signed: _____

On behalf of: _____ (Company Name where relevant)

Date: _____

Signed: _____

On behalf of: _____ (Diocese)

Date: _____