Diocese of Elphin – HR Policy Handbook

Document Name: **Data Protection Policy**
Document No: **3.1.1 (original)**
Effective Date: **15th February 2019**
Written By: **Frank Mitchell, HR Advisor**
Approved By: **+Kevin Doran, Bishop of Elphin**

Operating under the patronage of Our Lady of the Immaculate Conception, the Diocese of Elphin aims to provide staff members with a safe, caring and supportive Christian environment in which to carry out their work. Work objectives are to be advanced with due regard to the needs and dignity of each staff member and with due regard for the individuals and communities the diocese serves.

This document outlines the Diocesan policy on Data Protection. It is applicable to parishes, offices, agencies and any entity operating under the governance of the Diocese of Elphin (hereafter referred to as "the employer"). Line Managers (Bishop, Priests, Deacons, Religious, Lay Personnel who supervise staff members) are responsible for communicating this policy and having it signed off by their staff member(s).

Our Commitment
The Data Protection Acts 1988 and 2003 and General Data Protection Regulation (GDPR) [May 2018], apply to the processing of personal data. "The employer" is committed to complying with its legal obligations in this regard. "The employer" collects and processes personal data relating to its staff members in the course of business in a variety of circumstances, eg, recruitment, training, payment, performance reviews, and to protect the legitimate interests of "the employer".

This policy covers any individual about whom "the employer" processes data. This may include current and former staff members. Processing of data includes: collecting, recording, storing, altering, disclosing, destroying and blocking. Personal data kept by "the employer" shall normally be stored on the staff member's personnel file or HR electronic database. Highly sensitive data, such as medical information, will be stored in a separate file, in order to ensure the highest levels of confidentiality. "The employer" will ensure that only authorised personnel have access to a staff member's personnel file.

It may be necessary to store certain other personal data outside a staff member's personnel file, eg, salary details will be stored in the payroll department. The staff member's manager or supervisor may have access to certain personal data where necessary. "The employer" has appropriate security measures in place to protect against unauthorised access.

Collection and Storage of Data
"The employer" processes certain data relevant to the nature of the employment regarding its staff members and, where necessary, to protect its legitimate interests. We will ensure that personal data will be processed in accordance with the principles of data protection, as described in the Data Protection Acts 1988 and 2003 and General Data Protection Regulation (GDPR) [May 2018]. Personal data is normally obtained directly from the staff member concerned. In certain circumstances, it will, however, be necessary to obtain data from third parties, eg, references from previous employers. Where relevant to the nature of the work, "the employer" may make an application to the Garda Vetting Bureau for Garda clearance of a staff member.

Personal data collected by "the employer" is used for ordinary personnel management purposes. Where there is a need to collect data for another purpose, "the employer" shall inform you of this. In cases where it is appropriate to get your consent to such processing, "the employer" will do so.

Diocese of Elphin – HR Policy Handbook

Document Name: Data Protection Policy
Document No: 3.1.1 (original)
Effective Date: 15th February 2019
Written By: Frank Mitchell, HR Advisor
Approved By: +Kevin Doran, Bishop of Elphin

Staff members are responsible for ensuring that they inform their manager of any changes in their personal details, eg, change of address. We endeavour to ensure personal data held by "the employer" is up to date and accurate. "The employer" is under legal obligation to keep certain data for a specified period of time. In addition, "the employer" will need to keep personnel data for a period of time in order to protect its legitimate interests.

Security and Disclosure of Data
"The employer" will take all reasonable steps to ensure that appropriate security measures are in place to protect the confidentiality of both electronic and manual data. Security measures will be reviewed from time to time, having regard to the technology available, the cost and the risk of unauthorised access. Staff members must implement all diocesan security policies and procedures, eg, use of computer passwords, locking filing cabinets.

HR data will only be processed for employment-related purposes and, in general, will not be disclosed to third parties, except where required or authorised by law or with the agreement of the staff member. HR files are kept in the safekeeping of the manager and staff members who have access to these files must ensure that they treat them confidentially. Staff members working in the payroll department must treat all personal data they receive confidentially and must not disclose it, except in the course of their employment.

All staff members are likely to have access to a certain amount of personal data relating to colleagues, parishioners, contractors and other third parties. Staff members must play their part in ensuring its confidentiality. They must adhere to the data protection principles and must not disclose such data, except where necessary in the course of their employment, or in accordance with law. They must not remove or destroy personal data except for lawful reasons.

Any breach of the data protection principles is a serious matter and may lead to disciplinary action up to and including dismissal. If staff members are in any doubt regarding their obligations, they should contact the HR Advisor/Data Protection Officer.

Medical Data
"The employer" may carry out pre-employment medicals as part of the recruitment process. This data will be retained by "the employer".

Occasionally, it may be necessary to refer staff members to a doctor nominated by "the employer" for a medical opinion and all staff members are required by their contract of employment to attend in this case. "The employer" may receive certain medical information, which will be stored in a secure manner with the utmost regard for the confidentiality of the document. "The employer" does not retain medical reports on job applicants who do not become staff members for longer than is necessary.

Staff members are entitled to request access to their medical reports. Should a staff member wish to do so, please contact the HR advisor, who will consult with the doctor who examined you and request the data. The final decision lies with the doctor. Staff members are required to submit sick certificates in accordance with the sick pay policy. These will be stored by the diocese, having the utmost regard for their confidentiality.

Diocese of Elphin – HR Policy Handbook

Document Name: Data Protection Policy
Document No: 3.1.1 (original)
Effective Date: 15th February 2019
Written By: Frank Mitchell, HR Advisor
Approved By: +Kevin Doran, Bishop of Elphin

Email Monitoring
"The employer" provides email facilities and access to the internet. In order to protect against the dangers associated with email and internet use, screening software is in place to monitor email and web usage. Mailboxes are only opened:

- upon specific authorisation by a manager in cases where the screening software or a complaint indicates that a particular mailbox may contain material that is dangerous or offensive;
- where there is a legitimate work reason or in the legitimate interest of "the employer.

Please refer to the email and internet usage policies for further details.

Closed Circuit Monitoring (where relevant)
In certain parishes, web-cams are used to broadcast religious services, and closed circuit television cameras are used for the security of parishioners and people using church property and in order to protect against damage, theft or pilferage. Access to the recorded material will be strictly limited to authorised personnel. Closed circuit surveillance is not used to manage performance. See policy on CCTV.

Data Protection Officer
Data Protection Officer (DPO) for the Western Province is Darina Ryan-Pilkington. The DPO bears overall responsibility for ensuring compliance with data protection legislation. All staff members must co-operate with the data protection officer when carrying out their duties.

The data protection officer is also available to answer queries or deal with staff members' concerns about data protection.

Access Requests
Staff members are entitled to request data held about them on computer or in relevant filing sets. "The employer" will provide this data within 30 days. There is no charge for requesting this data.

A staff member should make a request in writing to the data protection officer, stating the exact data required. Staff members are only entitled to access data about themselves and will not be provided with data relating to other staff members or third parties. It may be possible to block out data relating to a third party or conceal his or her identity, and if this is possible "the employer" may do so.

Data that is classified as the opinion of another person will be provided unless it was given on the understanding that it will be treated confidentially. Staff members who express opinions about other staff members in the course of their employment should bear in mind that their opinion may be disclosed in an access request, eg, performance appraisals.

A staff member who is dissatisfied with the outcome of an access request has the option of using the diocesan grievance procedure.

Diocese of Elphin – HR Policy Handbook

Document Name: **Data Protection Policy**
Document No: **3.1.1 (original)**
Effective Date: **15th February 2019**
Written By: **Frank Mitchell, HR Advisor**
Approved By: **+Kevin Doran, Bishop of Elphin**

Right to object
Staff members have the right to object to data processing that is causing them distress. Where such objection is justified, "the employer" will cease processing the data unless it has a legitimate interest that prevents this. "The employer" will make every effort to alleviate the distress caused to the individual.

An objection should be made in writing to the data protection officer, outlining the data in question and the harm being caused to the staff member.

Transmission of data outside the State
It may be necessary in the course of business to transfer staff member's personnel data within the 'diocese' and to other organisations in countries outside the European Economic Area, which do not have comparable data protection laws to Ireland. The transfer of such data is necessary for the management and administration of your contract of employment and to facilitate the overall administration of the 'diocese' when this is necessary, "the employer" will take steps to ensure that the data has the same level of protection as it does inside the State. "The employer" will only transmit to companies that agree to guarantee this level of protection. For more information, please contact the data protection officer.

Review
This policy will be reviewed from time to time to take into account changes in the law and the experience of the policy in practice.

For further information please contact:

HR Advisor
Elphin Diocesan Office
St. Mary's
Temple Street
Sligo F91 KTX2
Email: hr@elphindiocese.ie
Mobile: 087 240 4882