



DATA PRIVACY NOTICE

(April 2024)

1. About the Safeguarding Service

The Safeguarding Service is a service within Limerick Diocese, which aims to promote the welfare of children and adults who may be vulnerable in all their involvements with the Diocese. The service also aims to ensure that all safeguarding complaints are responded to within the context of relevant legislation and National Catholic Church Safeguarding Policies and Standards.

2. Personal Data

The Safeguarding Service processes personal data and special category personal data. Personal data is information about a living person which reveals the identity of that person. Examples include a person's name, phone number and date of birth. It is personal data if the person can be identified from the information or if, when the information is put together with other easily acquired or available information, the person's identity is revealed. The Safeguarding Service collects, retains, stores and shares information about living persons. It does so in accordance with the requirements of the Data Protection Act (2018) and the General Data Protection Regulation, (2016), known as the GDPR.

The Bishop of Limerick is the data controller of the Diocese and, therefore, he is the data controller of personal data held by the Safeguarding Service. Staff employed as part of the safeguarding team act on behalf of the controller (the Bishop) and manage personal data on a day to day basis.

The Safeguarding Service processes personal data about the following individuals:

- (i) complainants, victims of abuse and others who the Safeguarding Service provides a service to, including survivors of abuse;
- (ii) respondents who are the subject of abuse complaints;
- (iii) family members and advisors of complainants, alleged victims and respondents;
- (iv) witnesses of alleged instances of abuse;
- (v) individuals involved in working with children and adults who may be vulnerable in the Diocese, in parishes in the Diocese and in Diocesan agencies, including Diocesan safeguarding trainers and parish safeguarding representatives;
- (vi) training attendees.

The persons about whom the Safeguarding Service holds personal data are referred to in this Notice as data subjects.

3. Data Processing in the Safeguarding Service

The Safeguarding Service complies with its obligations under Data Protection Law by keeping personal data up to date, by storing it securely, by not collecting or retaining excessive amounts of data (no more than is needed for the purposes for which it was gathered), by protecting it from loss, misuse, unauthorised access and disclosure, by ensuring that appropriate technical measures are in place to protect it and by destroying personal data safely when it is no longer required for the purpose for which it was gathered.

4. The Purposes for which Data is Processed

Data is processed in order to facilitate the Safeguarding Service to discharge its functions. These are:

- Case management. The Safeguarding Service gathers, retains, stores and shares information on complainants (those who disclose child or adult abuse) and respondents (those alleged to have abused children or adults) in accordance with national legislation (including but not limited to the Children First Act, 2015) and civil and Church guidelines on the management of allegations of the abuse of children and adults;
- Support of victims and survivors of abuse. The Safeguarding Service gathers, retains, stores and shares information about those who experienced abuse as children or as adults who are vulnerable to abuse; and their families in order to offer them support directly and in order to refer them to other support services;
- The creation and maintenance of safe environments for children and adults who may be vulnerable to abuse involved in Church activities. This involves processing data on those who work in parishes and diocesan offices and agencies, including the information processed through Garda vetting. It also involves processing data on those who cooperate with the Safeguarding Service in the discharge of this function, including diocesan safeguarding trainers, training attendees and parish safeguarding representatives.
- To enhance the capacity of the Safeguarding Service to deal with further complaints or disclosures.

5. The Data Processed

The Safeguarding Service gathers and retains information including a person's name, date of birth, current address, email address, phone number and role with the parish or diocesan office or agency. For certain persons, additional personal data or special category data, such as information about events in their past, legal documents and medical and psychological reports are also gathered and retained. This list is not exhaustive.

6. The Legal basis for Processing Personal Data

The legal bases on which the Safeguarding Service relies for processing personal data are the following:

- a. Explicit consent is sought from those with whom the Safeguarding Service communicates in order to share information about news, events, activities and programmes;
- b. Compliance with a legal obligation, as when those members of the team who are mandated reporters, report child protection concerns to Tusla, the Child and Family Agency in accordance with the requirements of the Children First Act, 2015;
- c. In order to protect the vital interests of a person, as when it shares information with those who need to know it in order to prevent the abuse of a child or adults who may be vulnerable to abuse;
- d. In the public interest, as when it processes personal data for the prevention of the abuse of children and adults who may be vulnerable to abuse;
- e. In the pursuit of the legitimate interest of the Diocese of Limerick as it acts to create a safe environment for children and adults who may be vulnerable to abuse.

7. Sharing of Personal Data

Personal data is treated as strictly confidential. It is shared, only when required,

- with other diocesan staff, with the civil and regulatory authorities and with others in accordance with the requirements of law and national and Church child and adult protection guidelines; or
- as otherwise required for the protection of children and adults who may be vulnerable to abuse; or
- by consent.

(See also Appendix 1 and Appendix 2).

Consideration will be given to relevant policies and guidance of statutory agencies in particular that of Tusla, The Child & Family Agency, and the Health Service Executive. Personal information is also shared with some service providers, such as those who provide support services for survivors of abuse, but only with the consent of the data subject. All processing of such data is done in compliance with current legislation.

8. Retention of Personal Data

Personal data is retained for as long as it is required for the discharge of the functions outlined in 4 above. All data is held in accordance with the data retention policy of the Diocese of Limerick which may be amended from time to time.

9. Storage and Accuracy of Personal Data

The Safeguarding Service is committed to ensuring information is stored securely. In order to prevent unauthorised access or disclosure, suitable physical, electronic and managerial procedures to safeguard and secure information have been put in place. The service uses technical and organisational security measures to protect data from accidental or intentional manipulation, loss,

destruction or access by unauthorised persons. The security measures are continuously adapted in line with technological developments.

The Safeguarding Service seeks to ensure that personal data is accurate and up to date. However, the data subject is responsible for informing the service of any changes to personal data and other information. Unfortunately, the transmission of information via the internet is not completely secure. Although every effort is made to protect personal data, any transmission via the internet is ultimately at the data subject's own risk. Once the Safeguarding Service has received personal information, strict procedures and security features are in place to prevent unauthorised access to or unlawful processing or disclosure of such data.

10. The Rights of the Data Subject

The data subject (the person whose information is processed by the Safeguarding Service) has the following rights:

- To request a copy of his/her personal data held by the Safeguarding Service;
- To request that the Safeguarding Service corrects any inaccuracies in the data held;
- To have the data erased when it is no longer required for the purpose for which it was gathered;
- To request the data controller to provide the data subject with a copy of his/her data and, where possible, transmit it to another data controller (this is the right to data portability and only applies when the processing is done by consent or is necessary for the performance of a contract with the data subject and the data controller processes the data by automated means);
- To object to the processing of personal data. This right only applies in a limited number of situations. Those that apply to the Safeguarding Service are when data is being processed to protect the vital interests of a person, data is being processed in the public interest or data is being processed in pursuit of the legitimate interest of the Diocese (6c, 6d, 6e, above).

All of the above rights are subject to limited exceptions in certain specified circumstances.

11. Further Processing

If the Safeguarding Service needs to process personal data for a purpose not covered by this Data Privacy Notice a new notice will be issued prior to commencing the processing setting out the relevant purposes and processing conditions. Where and whenever necessary, the service will seek the prior consent of the data subject/s to the new processing.

12. Vetting and Training

When an individual is Garda vetted by the Diocese for a role in the Diocese or in a parish within the Diocese, the individual's name, contact details and data generated during the vetting process are stored and retained in our database. This data includes, your current address, date of birth, role within the Diocese/parish, the date and outcome of your vetting. We process this information for administration purposes in connection with your vetting and also to determine when you next require to be vetted.

Only a very small number of employees have access to the vetting section of our database. Each employee has their own secure password for entry to the database. We use the Azure database operated by Microsoft to store and retain your information. This is stored in the cloud.

If you undergo safeguarding training in the Diocese, your name and date of training will also be stored in the database. The purpose of the Diocese processing this data is so that we can administer training and determine when an individual must attend refresher training

13. Addition to Data Privacy Notice Safeguarding Service Diocese of Limerick

When an individual is Garda vetted by the Diocese for a role in the Diocese or in a parish in the Diocese, the individual's name, contact details and data generated during the vetting process are stored and retained in our database. This data includes, previous addresses, your date of birth, your role within the Diocese/parish, the date and outcome of your vetting. We process this information for administration purposes in connection with your vetting and also to determine when you next require to be vetted.

Only a very small number of employees have access to the vetting section of our database. Each employee has their own secure password for entry to the database. We use the Azure database operated by Microsoft to store and retain your information. This is stored in the cloud.

If you undergo safeguarding training in the Diocese, your name and date of training will also be stored in the database. The purpose of the Diocese processing this data is to that we can administer training and determine when an individual must attend training again.

14. Addition to Vetting Procedures (Parishes) Diocese of Limerick

When an individual is Garda vetted by the Diocese for a role in the Diocese or in a parish in the Diocese, the individual's name, contact details and data generated during the vetting process are stored and retained in our database. This data includes, previous addresses, your date of birth, your role within the Diocese/parish, the date and outcome of your vetting. We process this information for administration purposes in connection with your vetting and also to determine when you next require to be vetted.

Only a very small number of employees have access to the vetting section of our database. Each employee has their own secure password for entry to the database. We use the Azure database operated by Microsoft to store and retain your information. This is stored in the cloud.

15. Contact Details

If you have any queries or complaints please contact the Director of the Safeguarding Service at the Diocesan Centre, St Munchins, Corbally, Limerick V94 925C. Tel: 061 350000 or ger.crowley@limerickdiocese.org

Further information on data privacy rights is available on the website of the Data Protection Commissioner: www.dataprotection.ie.

For queries relating to data protection please contact the Diocesan Data Protection Officer at Diocesan Centre, St Munchins, Corbally, Limerick V94 925 or by email at: michelle.oriordan@limerickdiocese.org

The Privacy Policy of the Diocese of Limerick can be found at <https://www.limerickdiocese.org/policies/privacy-policy/>

Appendix 1: Information Sharing

This section sets out in more detail the position of the Safeguarding Service in relation to the sharing of information relating to the protection of children and adults who may be vulnerable to abuse in a church context.

A1.1 The Safeguarding Service reports concerns regarding the abuse of children and adults who may be vulnerable to abuse to the civil authorities. The Safeguarding Service is legally required to report allegations of child abuse to TUSLA under the Children First Act, 2015 and such mandatory reporting is covered by (i) GDPR Article 6 (c) *compliance with a legal obligation*.

Mandatory reporting can also apply to sharing certain information about an alleged offence committed against a child or vulnerable adult with An Garda Síochána (Criminal Justice (Withholding of Information on Offences against Children and Vulnerable Persons) Act 2012).

A1.2 In certain very restricted circumstances, the Safeguarding Service shares such concerns with other Dioceses and church authorities. For example, if there is information that a member of a religious order has abused or is alleged to have abused a child or adult vulnerable to abuse, that information is shared with the provincial of the order or the order's designated liaison person (DLP) so that s/he can take whatever steps are required to prevent further abuse. This is covered by GDPR Article 6.1 (d) - *processing is necessary in order to protect the vital interests ...of another natural person* (i.e. the child/children or adult/s at risk) and/or GDPR Article 9 (2) (c) - *processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent*.

Such sharing of data is only to persons who need to be aware of, and take action to mitigate, these concerns and is done with appropriate measures in place to protect the data.

A1.3 Information is shared with others when required for the protection of children or adults vulnerable to abuse, for example, when the placement of respondent priests in residential institutions is being arranged. The managers of the institutions concerned may, for example, be informed that the respondent ought not to have unsupervised contact with children or vulnerable adults. This is also covered by Articles 6.1(d) and/or Article 9 (2) (c).

A1.4 Information is shared with families of respondent priests. Priests often have contact with children in their extended families and the Safeguarding Service has a duty to protect these children from abuse. The practice is to encourage the respondent priests themselves to talk to their families in the first instance and then follow up with family members to ensure that they have sufficient information to protect their own children and vulnerable family members. This is also covered by Article 6.1(d) and /or Article 9 (2) (c).

Ordinarily, the Safeguarding Service will consult with Tusla, The Child & Family Agency, regarding disclosures to extended family members.

These disclosures of personal data could also be considered to be covered by GDPR Article 6.1 (f) - *processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party*¹.

¹ Recital 47 provides: *The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding [sic], taking into*

The Bishop of Limerick has a legitimate interest in the activities of those who serve as priests of the Diocese and has a legitimate interest in safeguarding children and adults who may be vulnerable to abuse.

A1.5 Information is shared with the civil authorities in the investigation of historic allegations of abuse.

This is covered by Section 41 of the Data Protection Act 2018: *the processing of personal data and special categories of personal data for a purpose other than the purpose for which the data has been collected shall be lawful to the extent that such processing is necessary and proportionate for the purposes—*

(b) of preventing, detecting, investigating or prosecuting criminal offences.

Section 55 (1) of the Data Protection Act 2018 – elaborating on GDPR Article 10, *Processing of personal data relating to criminal convictions and offences – also provides a legal basis for such sharing of data: personal data referred to in Article 10 may be processed— where...*

(b) (iv) processing is necessary to prevent injury or other damage to the data subject or another person or loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or another person.

Appendix 2: The Safeguarding Structure of the Diocese of Limerick

This section sets out in more detail the position of the Safeguarding Service in relation to the sharing of information relating to the protection of children and adults who may be vulnerable to abuse from abuse in a context other than a Church one. Such a situation arises, for example, when a priest learns of abuse within a family context and contacts the Safeguarding Service for advice and guidance.

The Diocese of Limerick, like many organisations that provide services to children, operates a designated liaison person (DLP) system. That is, there are people designated by the Diocese to receive child protection concerns (information that a child has been abused, is being abused or is at risk of abuse) and to report them to the civil authorities. The DLP for the Diocese of Limerick is the Director of the Safeguarding Service.

When mandatory reporting was introduced in 2017, a question arose as to whether the DLP structure should be retained. Since a priest is a mandated reporter, if he knows of a child protection concern, he is legally obligated to report the matter to Tusla himself with no requirement to come through the DLP. Tusla, however, advised that the DLP structure ought to be retained for a number of reasons. The diocesan DLP is a professionally qualified social worker with experience of operating the child protection system. They have a greater understanding of both the thresholds for reporting concerns and the means of doing so than those without such qualifications and experience. There is, therefore, a better chance that information vital to the protection of children will reach those with the authority to act on it by retaining the DLP structure. The legal obligations on mandated persons such as priests

consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller.

“Third Party” is defined as: a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

can be discharged by doing joint reports on behalf of the DLP and the mandated reporter who first hears of the concern.

In order to report child protection concerns that do not relate to alleged abuse within a Church context, the Safeguarding Service is required to gather information about the child/ren at risk and, where known, the alleged perpetrator of abuse. In addition, *Children First, National Guidance for the Protection and Welfare of Children, 2017* refers to the recording of the concern and of the actions taken in relation to it. Thus, the Safeguarding Service is required to process data on child protection concerns that do not relate to the Diocese that come to the attention of diocesan personnel in the course of their work.

The GDPR Article 6.1 (c) *legal obligation* provision applies to transmitting child protection concerns via the DLP (designated liaison person) on the grounds that the Children First Act 2015 imposes obligations on *mandated persons* who include, not only social workers and clergy, but also *a safeguarding officer, child protection officer or other person (howsoever described) who is employed for the purpose of performing the child welfare and protection function of religious, sporting, recreational, cultural, educational and other bodies and organisations offering services to children.*

Mandatory reporting does not apply to concerns that relate to adults that may be vulnerable but the considerations about following the correct reporting procedures are just as valid. The purpose of going through the DLP is to ensure correct reporting procedures are followed and this transmission is covered by GDPR Article 6.1 (d) – *processing is necessary in order to protect the vital interestsof another natural person* (i.e. the child/children or adult/s who may be at risk).