APPENDIX B

RECORDING AND STORAGE OF INFORMATION

APPENDIX B

Introduction

Good record-keeping is an integral part of safeguarding children within the Catholic Church; it should not be considered to be an optional extra. There are many reasons why all those involved in safeguarding children should keep good records. These include:

- helping to improve accountability;
- demonstrating how decisions relating to safeguarding children are made;
- supporting effective assessments;
- providing documentary evidence of actions taken;
- helping to identify risks, and demonstrating how those risks have been managed.

Good record-keeping also helps to safeguard the rights of all concerned.

Below are the primary reasons for record-keeping, as well as the processes necessary to write and maintain accurate records. Also detailed are recommendations regarding information sharing, and retention and storage of sensitive data.

Why is record-keeping important?

1. **Doing so ensures accuracy of reporting information.**
   This can be for internal use, or it can be done in circumstances where there is the necessity to report and to be accountable to external stakeholders, e.g. courts, tribunals of inquiry, Gardaí, PSNI, Tulsa (the Child and Family Agency) and HSCT (Health and Social Care Trust). Creating written records as soon as practicable after the event avoids the possibilities of memory loss and the distortion of the information.

2. **Doing so assists with decision-making and case management.**
   Accurately recording factual information facilitates an evaluation of the information and aids decision-making.

3. **Doing so protects both the subjects of recording and the recorder by having an agreed and accurate record.**
   As far as possible, recorded information should be agreed, with the subject of the recording, as constituting an accurate record of what took place.

4. **Doing so enables accountability.**
   All those who have responsibilities for safeguarding children within the Catholic Church should be and will be held accountable for their actions. Good recording is required as evidence that the safeguarding of children is treated as a priority, and that all steps have been taken to prevent and minimise risk and to manage allegations appropriately.

5. **Doing so enables the proper tracking of complaints.**
   It is important that we demonstrate through our records that complainants have been listened to and responded to in a compassionate and caring way. It is therefore vital that accurate records are kept of all complaints received and of how these have been responded to.

6. **Doing so allows for continuity where there are changes in personnel managing the case.**
   Safeguarding children can involve a number of people, including the Church authority and designated person. Personnel can also change over the course of managing a child abuse allegation. It is therefore important that good, factual details are maintained in writing to allow for a consistent and fair approach, a continuity of care for complainants, and the proper management of respondents, when required.

Principles of good record-keeping

- All records should be legible – preferably typed or word-processed.
- All entries should be signed, and the person's name and job title should be printed alongside the entry.
- All records should be dated and timed in real time. These records should be generated in correct chronological order.
- A narrative should be constructed that sets out a chronology of events and references any correspondence.
- Records should be accurate and presented in such a way that the meaning is clear.
- Records should be factual and should not include unnecessary abbreviations, jargon, opinion or irrelevant speculation.
- Judgement should be used to decide what is recorded. Is it relevant? Is it as objective as possible? Are facts and any necessary opinions clearly distinguished?
- Records should identify any risks, and should show the action taken to manage these.
- Records must not be altered or destroyed without proper authorisation. If the need for alteration arises, both the fact of such authorisation and the alteration made to any original record or documentation should be signed and dated.

Data protection legislation

The General Data Protection Regulation (GDPR) came into effect on 25 May 2018. It has general application to the processing of personal data in the EU, setting out obligations on data controllers and processors, and providing strengthened protections for data subjects. In Ireland, the national law, which, amongst other things, gives further effect to the GDPR, is the Data Protection Act 2018.

In Northern Ireland the main legislation is the Data Protection Act 2018, which is similarly tailored to meet the requirements of GDPR.

In both jurisdictions GDPR places direct data processing obligations on organisations to process personal data under certain conditions. For instance, the processing should be fair and transparent, for a specified and legitimate purpose and limited to the data necessary to fulfill this purpose. It must also be based on one of the following legal grounds.

1. The **consent** of the individual concerned.
2. A **contractual obligation** between you and the individual.
3. To satisfy a **legal obligation**.
4. To protect the **vital interests** of the individual.
5. To carry out a task that is in the **public interest**.
6. For your company's **legitimate interests**, but only after having checked that the fundamental rights and freedoms of the individual whose data you are processing are not seriously impacted. If the person's rights override your interests, then you cannot process the data.

Access to information by data subject

People have a right to know what personal information is held about them, by whom and for what purpose (See Guidance 2.2D and 2.2E). This is detailed in data protection and human rights legislation. However, despite these rights, in certain circumstances such information can be shared with others.

The data subject must be made aware of the creation of a safeguarding record. If the data subject seeks access to their record, the following should take place:

a. The contents of the file should be reviewed and assessed so that data belonging to third parties is redacted;

b. At an agreed time and place, the file should be made available for reading by the data subject, under the supervision of the bishop, superior or the designated liaison person;

c. The data subject can make notes, and can ask for notes to be included in the file. If agreed, an amendment can be made on the file note. The file manager should state in writing the reason for the amendment, and sign and date their written note. Any such amendments should also be signed and dated by the data subject;

d. If there is a disagreement concerning the amendment of any file, the details of the disagreement should be recorded, signed and dated by the file manager and the data subject.

For guidance on your obligations around data access follow link https://www.dataprotection.ie/en/organisations (ROI)

Or

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/ (Northern Ireland)

Storage of data

It is important that all sensitive or confidential materials are retained in a case file and stored securely in a place designated by the data controller, i.e. the Church authority

APPENDIX B

Files containing sensitive or confidential data should be locked away, and access to the relevant fireproof safe(s) or filing cabinet(s) and keys should be strictly controlled.

Access to the files needs to be limited to people in named roles – i.e. the Church authority– and properly designated child safeguarding personnel, who either need to know about the information in those records, and/or who have a responsibility to manage the records.

Any information of a sensitive and confidential nature – if stored electronically – must always be password protected.

Arrangements need to be made for the contents of the relevant files, as well as their location and storage arrangements, to be passed on from outgoing data controllers to their successors.

Other records with identifying personal information – e.g. parish records on recruitment and vetting, activity attendance records, consent forms, accident forms, etc. – must be stored in a secure locked cabinet in the parish office.

Retention and destruction of data

Each Church authority will need to establish its own retention periods and destruction processes.

Guidance

- Each Church authority should appoint a data protection officer who will take charge of responsibility for data protection within that organisation.
- The DPO's tasks are defined in the Data Protection Acts 2018 -, briefly these are to:
    - to inform and advise the controller, its employees, and any associated processors about their obligations to comply with the GDPR and other relevant data protection laws such as Part 3 of the Act;
    - to monitor compliance with data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits; and
    - to be the first point of contact for the Data Commission/Information Commissioner and for individuals whose data is being processed.
- The DPO with the Church authority should develop the necessary procedures and policies to ensure that the safe and secure processing of personal and sensitive data is in keeping with the principles of data protection. In developing these policies the DPO and the Church authority should be mindful of the following:

- The appointed data protection officer should ensure that all records associated with these standards and guidance are reviewed on a periodic basis for the purposes of determining whether such records, in whole or in part, should be retained.
- Ensuring that each file relating to a data subject should contain a checklist that provides for periodic reviews. The checklist should be signed and dated after completion of those reviews, with confirmation as to whether the records will be kept for a further period and the reason for same.
- The assessment of danger or harm to children arising out of the destruction of the relevant records.

Further support

For more advice and guidance on data retention and destruction, please contact:

Republic of Ireland

- Data protection commissioner: https://www.dataprotection.ie

Northern Ireland

- Information commissioner: https://ico.org.uk
- Department of Health, Social Services and Public Safety (DHSSPS): http://www.dhsspsni.gov.uk/index/gmgr.htm

APPENDIX B

Further support

For more advice and guidance on data retention and destruction, please contact:

Republic of Ireland

- Tusla information and advice officers: http://www.tusla.ie/children-first/roles-and-responsibilities/organisations/children-first-training
- Data protection commissioner: https://www.dataprotection.ie

Northern Ireland

- Information commissioner: https://ico.org.uk
- Department of Health, Social Services and Public Safety (DHSSPS): http://www.dhsspsni.gov.uk/index/gmgr.htm