Loreto Sisters

Data Protection Policy

Loreto is required under the Data Protection Acts 1988 & 2003 to ensure the security and confidentiality of all personal data it collects and processes on behalf of its volunteers and employees.

Personal data must be obtained and processed fairly, kept only for one or more specified explicit and lawful purpose, used and disclosed only in ways compatible with the purpose for which it was obtained and, kept safe, secure, accurate, complete and up to date, adequate, relevant and not excessive, retained for no longer than is necessary for the purpose or purposes for which it was collected, not transferred to countries without adequate protection and may be given to an individual upon receipt of request.

Record keeping is important to:

- Ensure accurate reporting information.
- Assist with decision making and case management.
- Protect both the subject of reporting and the recorder by having an agreed and accurate record.
- Enable the proper taking of complaints.
- Ensure accountability.
- Allow for continuity where changes in personnel managing a case have been made.

Principles of good record keeping:

- Records should be legible – preferably typed or word - processed.
- Entries should be signed. The person's name and job title should be printed alongside the entry.
- Records should be dated and timed in real time and generated in chronological order.
- A narrative that sets out a chronology of events and correspondence should be created.
- Records should be accurate and presented in such a way that the meaning is clear.
- Records should be factual and not include jargon, opinion or speculation.
- Judgement is needed to decide what to record, what is relevant and as objective as possible.
- Records should identify any risks and the action taken to manage them.
- Records must not be altered or destroyed without proper authorisation. If alteration is needed both the fact of such authorisation and the alteration made should be signed and dated.

Retention and security of records:

- File records which contain personal information should be stored in a secured locked file in the LSR's office.
- All personal files must be locked away securely from unauthorised access.
- Access to locked cabinets/filing cabinets must be on a need to know basis only.
- The LSR or her nominee are the only persons who are approved to access personal files.
- All computer/laptops used for record keeping must be password protected and encrypted.
- Persons who store information on computers/laptops for the purpose of Loreto records must use individual passwords and access must only be by the LSR or her nominee.
- Keys to filing cabinets/locked cabinets should be strictly controlled with access provided only to LSR or one named nominee.

Retention and destruction of data:

- All case management safeguarding files should be retained for a period of 100 years.
- All other files pertaining to safeguarding should be stored for a period of 20 years with the exception of Garda vetting which should be retained for the duration of employment and then destroyed.
- When volunteers/employees retire from positions/posts, files should be moved to archive storage however the same security arrangements as outlined above must apply to these records.
- Where there is no legal requirement to retain records beyond closure, destruction should be undertaken as follows -

    √ An inventory should be completed indicating name of file, location of file, destruction date, method of destruction, signed approval for destruction to be signed off by the data controller or nominated persons.

    √ Destruction of waste paper/records containing personal information must be by way of incineration or cross shredding.

Access to information by subject:

- Persons wishing to access records should be provided with a copy of their own personal information only.
- Such applications must be in writing.
- Files should be reviewed and assessed so that third party data is redacted.
- At an agreed time and place, the file should be made available for reading by the data subject, under the supervision of the province leader or DLP.
- The data subject can take notes or ask for notes to be included in the file. If agreed an amendment can be made to the file. The file manager should state in writing the reason for the amendment, sign and date their written note. Any amendments should be signed and dated by the data subject.
- 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.

The right of access does not apply in certain circumstances, where it is likely to prejudice an ongoing investigation.

Data protection legislation:

The principle legislation in the Republic of Ireland dealing with data protection is the Data Protection Act 1988. The 1988 Act was amended by the Data Protection (Amendment) Act 2003.

In Northern Ireland the main legislation is the Data Protection Act 1988.

The Data Protection Acts 1998 – 2003 in the Republic of Ireland set out eight principles that define the conditions under the processing (recording, storage, manipulation and transmission) of personal data can be determined to be legally acceptable or otherwise. These eight principles are outlined above.

May 2018