KDYS Data Protection Policy

Introduction

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of Kerry Diocesan Youth Service (KDYS). This includes obligations in dealing with personal data, in order to ensure that the organisation complies with the requirements of the relevant Irish legislation, namely the General Data Protection Regulation (GDPR) 2018, the Irish Data Protection Act (1988), and the Irish Data Protection (Amendment) Act (2003).

Rationale

KDYS must comply with the Data Protection principles set out in the relevant legislation. This Policy applies to all Personal Data collected, processed and stored by KDYS in relation to its staff, service providers and clients in the course of its activities. KDYS makes no distinction between the rights of Data Subjects who are employees, and those who are not. All are treated equally under this Policy.

Scope

The policy covers both personal and sensitive personal data held in relation to data subjects by KDYS. The policy applies equally to personal data held in manual and automated form.
All Personal and Sensitive Personal Data will be treated with equal care by KDYS. Both categories will be equally referred-to as Personal Data in this policy, unless specifically stated otherwise.

This policy should be read in conjunction with the associated documents:

- Privacy Statement – printed on Website
- Privacy Notice for Employees
- Record & Data Management Policy
- Data Schedule & Retention List
- Data Subject Access Request procedure
- Data Destruction Policy
- Data Loss/Breach Notification procedure

Definitions

For the avoidance of doubt, and for consistency in terminology, the following definitions apply within this Policy and related documents.

Data

This includes both automated and manual data.

- Automated data means data held on computer or stored with the intention that it is processed on computer.
- Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.

Personal Data

The term 'personal data' means any information concerning or relating to an living person who is either identified or identifiable (such a person is referred to as a 'data subject').
An individual could be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier (such as an IP address) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

Sensitive Personal Data

Sensitive personal data is personal data which relates to specific aspects of one's identity or personality, and includes information relating to ethnic or racial identity, political or ideological beliefs, religious beliefs, trade union membership, mental or physical well-being, sexual orientation, or criminal record.

Data Controller

The legal entity responsible for the acquisition, processing and use of the personal data. In the context of this policy KDYS is the data controller.

Joint Controller

A 'joint controller' relationship arises where two or more controllers jointly determine the purposes and means of the processing of personal data. This might be because they are processing personal data for the same purpose or they are processing personal data for closely linked or complementary purposes.

Data Subject

A living individual who is the subject of the personal data, i.e. to whom the data relates either directly or indirectly.

Data Processor

A "data processor" refers to a person, company, or other body which processes personal data on behalf of a data controller.

Data Compliance Officer

Nicola O'Sullivan was appointed by KDYS to monitor compliance with the appropriate data protection legislation, to deal with Subject Access Requests, and to respond to data protection queries from staff members and the general public.

KDYS Area of Work

The department or team to which each KDYS worker is aligned. Each KDYS Area of Work is managed by a Line Manager or Team Co-ordinator.

Pseudonymisation

Pseudonymisation is defined within the GDPR as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable individual"

KDYS as Data Controller.

In the course of its daily organisational activities, KDYS acquires, processes and stores personal data in relation to:

- Employees of KDYS
- Service Users of KDYS
- Volunteers of KDYS
- Third party service providers engaged by KDYS

In accordance with the Irish Data Protection legislation, this data must be acquired and managed fairly. Not all staff members will be expected to be experts in Data Protection legislation. However, KDYS is committed to ensuring that its staff have sufficient awareness of the legislation in order to be able to anticipate and identify a Data Protection issue, should one arise. In such circumstances, staff must ensure that the KDYS Data Compliance Officer (DCO) is notified, and in order that appropriate corrective action is taken.

Due to the nature of the services provided by KDYS, there is regular and active exchange of personal data between KDYS and its Data Subjects. In addition, KDYS exchanges personal data with Data Processors on the

Data Subjects' behalf. This is consistent with KDYS's obligations under the terms of its contract with its Data Processors.

This policy provides the guidelines for this exchange of information, as well as the procedure to follow in the event that a KDYS staff member is unsure whether such data can be disclosed. In general terms, the staff member should consult with the DCO to seek clarification.

The Data Protection Rules
The following key rules are enshrined in Irish legislation and are fundamental to KDYS' data protection policy and practice. In its capacity as data controller, KDYS ensures that all data shall:

1. Be obtained and processed fairly and lawfully
For data to be obtained fairly, the data subject will, at the time the data are being collected, be made aware of:

- The identity of the data controller (KDYS);
- The purpose(s) for which the data is being collected;
- The person(s) to whom the data may be disclosed by the data controller;
- Any other information that is necessary so that the processing may be fair.

KDYS will meet this obligation in the following way:

- Where possible, the informed consent of the data subject will be sought before their data is processed;
- Where it is not possible to seek consent, KDYS will ensure that collection of the data is justified under one of the other lawful processing conditions – legal obligation, contractual necessity, etc.;
- Where KDYS intends to record activity on CCTV or video, a Fair Processing Notice will be posted in full view, prior to the recording;
- Processing of the personal data will be carried out only as part of KDYS' lawful activities, and it will safeguard the rights and freedoms of the data subject;
- The data subject's data will not be disclosed to a third party other than to a party contracted to KDYS and operating on its behalf, or where KDYS is required to do so by law.

2. Be obtained only for one or more specified, legitimate purposes
KDYS will obtain data for purposes which are specific, lawful and clearly stated. A data subject will have the right to question the purpose(s) for which KDYS holds their data, and it will be able to clearly state that purpose or purposes. Specifying the purpose or purposes of obtaining particular data at the outset is likely to help an organisation to be in a position to justify its use of the data (see Rationale above).

3. Not be further processed in a manner incompatible with the specified purpose(s)
Any use of the data by KDYS will be compatible with the purposes for which the data was acquired.

4. Be kept safe and secure
KDYS will employ high standards of security in order to protect the personal data under its care. KDYS' data management policies guarantee protection against unauthorised access to, or alteration, destruction or disclosure of any personal data held by KDYS in its capacity as data controller.

Access to, and management of, staff and service user records is limited to those staff members (paid and unpaid) who have appropriate authorisation and password access. In the event of a data security breach affecting the personal data being processed on behalf of the data controller, the relevant third-party processor will notify the data controller without undue delay.

5. Be kept accurate, complete and up to date where necessary
KDYS will:

- Ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy;

- Conduct periodic reviews and audits to ensure that relevant data is kept accurate and up to date. KDYS conducts a review of sample data every six months to ensure accuracy;
- Ensure that staff contact details and details on next-of-kin are reviewed and updated every two years, or on an 'ad hoc' basis where staff members inform the office of such changes;
- Conduct regular assessments in order to validate the need to keep certain personal data.

6. Be adequate, relevant and not excessive in relation to the purpose(s) for which the data were collected and processed

KDYS will ensure that the data it processes in relation to data subjects are relevant to the purposes for which those data are collected. Data which are not relevant to such processing will not be acquired or maintained.

7. Not be kept for longer than is necessary to satisfy the specified purpose(s)

KDYS has identified an extensive matrix of data categories, with reference to the appropriate data retention period for each category. The matrix applies to data in both a manual and automated format. Once the respective retention period has elapsed, KDYS undertakes to destroy, erase or otherwise put this data beyond use.

8. Be managed and stored in such a manner that, in the event a data subject submits a valid Subject Access Request seeking a copy of their personal data, this data can be readily retrieved and provided to them

KDYS has implemented a Data Subject Access Request procedure by which to manage such requests in an efficient and timely manner, within the timelines stipulated in the legislation.

Personal Data and Legal Basis

The personal data that KDYS collects, the purpose for the collection and the legal basis for processing said data is outlined in the Data Schedule and Retention List.

Data Subject Access Requests

As part of the day-to-day operation of the organisation, KDYS' staff engages in active and regular exchanges of information with data subjects. Where a valid, formal request is submitted by a data subject in relation to the personal data held by KDYS which relates to them, such a request gives rise to access rights in favour of the Data Subject.

KDYS staff will ensure that such requests are forwarded to the Line Manager/ Data Compliance Officer in a timely manner, and they are processed as quickly and efficiently as possible, but within not more than 40 calendar days from receipt of the request.

Contact details

For all queries relating to Data Protection, please contact our Data Compliance Officer (DCO) at dataprotection@kdys.ie.

This policy was approved by the Board of KDYS on 1st March 2022 and is effective as and from that date.