ST. PATRICK'S CENTRE, KELLS ROAD, KILKENNY

Supporting People in Communities
St Patrick's Centre

POLICY TITLE: Data Protection Policy

Prepared by: **Data Protection Officer**	Approval Date: 19th June 2019	Review Date: 19th June 2021
Policy Number	Approval By Signed: David Vidom Operations Manager	

Mission Statement

To enable people to live a good life, in their own home, with supports and opportunities to become active, valued and inclusive members of their local communities.

To enable a supported, self-directed living (SSDL) model of provision which is underpinned by our beliefs, values and vision.

Review Date: Revision No: 1	Amendments Required New Legislation New Data Protection Officer	New Revision Status _____
Reviewed By: Data Protection Officer	Approved By: Signed:_____ Operations Manager	

Table of Contents

1.0 Introduction

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of Saint Patrick's Centre, Kilkenny (SPC). This includes obligations in dealing with personal and sensitive data, in order to ensure that the organisation complies with the requirements of the relevant Data Protection legislation, the General Data Protection Regulation (GDPR) 2018 and the Data Protection Act 2018.

2.0 Rationale

SPC must comply with the Data Protection principles set out in the relevant legislation. This policy applies to all personal and sensitive data collected, processed and stored by SPC in relation to its staff, service providers and the people supported in the course of its activities. SPC makes no distinction between the rights of data subjects who are employees and those who are not. All are treated equally under this policy.

3.0 Scope

This policy covers both personal and sensitive data held in relation to data subjects by SPC. The policy applies equally to personal data held in manual and automated form.

4.0 Relevant Legislation

- EU Convention on Human Rights (1950)
- OECD Guidelines on Data Protection (1980)
- Data Protection Acts (1988 and 2018)
- General Data Protection Regulation (GDPR)

5.0 Definitions

For the avoidance of doubt and for consistency in terminology, the following definitions will apply within this policy.

Data

This includes both automated and manual data.

Automated data means data held on computer or store 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 intention that it forms part of a relevant filing system.

Personal Data

Information which relates to a living individual, who can be identified either directly from that data or indirectly in conjunction with other data which is likely to come into the legitimate possession of the Data Controller.

Sensitive Personal Data

A particular category of personal data, relating to racial or ethnic origin, political opinions, religious, ideological or philosophical beliefs, trade union membership, information relating to one's sexual orientation, information in relation to commission of a crime and information relating to conviction for a criminal offence.

Data Controller

A person or entity who, either alone or with others, controls the content and use of personal data by determining the purposes and means by which that personal data is processed.

Data Subject

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

Data Processor

A person or entity who processes personal data on behalf of a Data Controller on the basis of a formal, written contract but who is not an employee of the Data Controller, processing such data in the course of his/her employment.

Data Protection Officer

A person appointed by SPC 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 people supported and/or their representatives.

Relevant Filing System

Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers) and this is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily available.

6.0 SPC as a Data Controller

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

- People Supported by SPC
- Family members of people supported by SPC
- Staff of SPC
- Service providers to SPC

In accordance with the Data Protection legislation, this data should be acquired and managed fairly. Not all employees will be expected to be experts in data protection legislation. However, SPC 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 Data Protection Officer (DPO) is informed in order that appropriate corrective action is taken.

Due to the nature of the service provided by SPC, there is regular and active exchange of personal and sensitive data between SPC and its Data Subjects. In addition, SPC exchanges personal data with Data Processors on the Data Subjects' behalf.

This is consistent with SPC'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 an SPC staff member is unsure when such data can be disclosed.

In general terms, the staff member should consult with the Data Protection Officer to seek clarification.

7.0 Subject Access Requests

Any formal, written request by a Data Subject for a copy of their personal data (a subject access request) will be referred as soon as possible to the Data Protection Officer and will be processed as soon as possible. A subject access request form is available upon request, on the Q Drive and on www.stpatrickskilkenny.com. All manual and computer files will be checked for relevant data on receipt of a request.

It is intended that by complying with these guidelines, SPC will adhere to best practice regarding the applicable data protection legislation. Data will be released promptly and time lines are outlined on the subject access request form.

8.0 Third Party Processors

In the course of its role as Data Controller, SPC engages a number of Data Processors to process personal and sensitive data on its behalf. In each case, a formal written contract is in place with the processor, outlining their obligations in relation to the personal and/or sensitive data, the specific purpose(s) for which they are engaged and the understanding that they will process the data in compliance with the Irish Data protection legislation.

Data Processors include but are not limited to the following: -

- Zyncfree Surveys
- Microsoft Office 365
- Dropbox
- iCloud
- Sage
- TMS

- DMS
- SOS

9.0 Data Protection Principles

1. Data should be obtained and processed fairly and lawfully

   For data to be obtained fairly, the data subject will, at the time the data is being collected, be made aware of:-

   a. The identity of the Data Controller (SPC)
   b. The purpose for which the data is being collected
   c. The person to whom the data may be disclosed by the Data Controller
   d. Any other information that is necessary so that the processing may be fair
   e. Where possible, the informed consent of the data subject will be sought before their data is processed
   f. Where it is not possible to seek consent, SPC will ensure that collection of data is justified under one of the other lawful processing conditions i.e. legal obligation, contractual necessity etc.
   g. Where SPC intends to record activity on CCTV or video, a fair processing notice will be posted in full view
   h. Processing of the personal and/or sensitive data will be carried out as part of SPCs lawful activities and SPC will safeguard the rights and freedoms of the Data Subjects.

2. Data should be obtained only for one purposes or more specified legitimate purposes

   SPC 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 SPC holds their data and SPC will be able to clearly state that purpose or purposes.

3. Data should not be further processed in a manner incompatible with the specified purpose

   Any use of the data by SPC will be compatible with the purposes for which the data was acquired.

4. Data should be kept safe and secure

   SPC will employ high standards of security in order to protect the personal and sensitive data under its care. Appropriate security measures will be taken to protect against unauthorised access to, or alteration, destruction or disclosure of any personal or sensitive data held by SPC in its capacity as Data Controller.

Access to and management of records belonging to people supported and staff is limited to those staff members who have appropriate authorisation and password access.

5. Data should be kept accurate, complete and up to date where necessary

SPC will:-

a. Ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy
b. Conduct periodic reviews and audits to ensure that relevant data is kept accurate and up to date. SPC conducts a review of sample data every six months to ensure accuracy; staff contact details and details on next of kin are reviewed and updated every two years
c. Conduct review assessments in order to establish the need to keep certain personal and/or sensitive data.

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

SPC 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 retained.

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

SPC 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 manual and automated formats.

Once the respective retention period has elapsed, SPC undertakes to destroy, delete or otherwise put this data beyond use.

8. Data should 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.

SPC has implemented a subject access request procedure by which to manage such requests in an efficient and timely manner, within the timelines stipulated in the legislation.

9. Data Subject Access Requests

As part of the day to day operation of the organisation, SPC staff engage in active

and regular exchanges of information with Data Subjects. Where a formal request is submitted by a Data Subject in relation to the data held by SPC, such a request gives rise to access rights in favour of the Data Subject.

There are specific time lines within which SPC must respond to the Data Subject, depending on the nature and extent of the request. They should be processed as quickly and as efficiently as possible, but within not more than one month from date of request, unless an extension is requested.

SPC staff will ensure that, where necessary, such requests are forwarded to the Data Protection Officer in as timely a manner as possible in order that they can comply with timelines.

10.0 Implementation

As a Data Controller, SPC ensures that any entity which processes personal data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection legislation.

Failure of a Data Processor to manage SPCs data in a compliant manner will be viewed as a breach of contract and will be pursued through the courts.

Failure of SPC staff to process Personal Data in compliance with this policy may result in disciplinary proceedings.

This policy should be read in conjunction with: -

1. File Retention Policy
2. Data Breach Policy
3. Data Protection Impact Assessment Procedure

11.0 Data Breach Management

A data breach may happen for a number of reasons including but not limited to: -

- Loss or theft of equipment on which data is stored
- Inadequate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as flood or fire
- Computer hacking
- Access where information is obtained by deception

There are three elements to managing a data breach

- Incident details
- Notification of data breach
- Evaluation and response

Incident Details

Details of the incident should be recorded accurately by the person reporting same, including

- Description of the incident
- Date and time of the incident
- When was the Data Protection Officer informed
- Type of data involved and how sensitive it is
- Number of individuals affected by incident
- No of records involved
- Corroborating material
- Immediate action taken to contain/mitigate the incident

Notification of Data Breach

It is critical that on becoming aware of any breach, the staff member should take immediate action to rectify the breach before notifying the Data Protection Officer.

A data breach must be reported without delay to Data Protection Officer via the Data Breach incident form which is available upon request, or on the Q Drive and on www.stpatrickskilkenny.com. The Data Protection Officer will assess the incident details and any risk involved.

The Data Protection Officer will decide, depending on the severity of the breach, whether to notify the Data Protection Commissioner and/or the Data Subject affected. In this regard, the DPO will have regard to over-notifying as not every incident will warrant notification.

Evaluation and Response

Subsequent to any data breach, a thorough review of the incident will be made by the Data Protection Officer. The purpose of this review will be to: -

- Ensure that the steps taken during the incident were appropriate
- Describe and record the measures been taken to prevent a repetition of the incident
- Identify areas that may need to be improved
- Document any recommended changes to policy and/or procedures which are to be implement as soon as possible thereafter

12.0 Data Protection Training & Support

Data Protection support is provided by the Data Protection Officer.

Áine Forde
Data Protection Officer
St Patrick's Centre
Kells Road
Kilkenny

Tel: 056 772 2170 Mobile: 087 194 2788 Email: aine.forde@stpatrickskilkenny.ie

Data Protection Awareness Training will take place during induction of new staff and will be updated every two years thereafter. It will also feature in other training throughout the staff members' career i.e. keyworker training, record keeping and writing training. The training material will be amended in the event that the relevant legislation is amended.

13.0 Data Protection Impact Assessments

When SPC processes personal data, the data subject whose data we are processing is exposed to risks. A Data Protection Impact Assessment is the process of systematically identifying and minimising those risks as far and as early as possible. It allows SPC to identify potential privacy issues before they arise and come up with a way to mitigate them.

Under the General Data Protection Regulation (GDPR) SPC must carry out a Data Protection Impact Assessment (DPIA) where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

When the need for a DPIA is identified (with consultation with the DPO) then the DPIA form should be completed. The DPIA Form is available upon request from the DPO.

14.0 Complaints

Data Subjects are entitled to make a complaint to the Data Protection Commissioner in writing to: -

Office of the Data Protection Commissioner
21 Fitzwilliam Square South
Dublin 2 DO2 RD28

Or by email to**:** **info@dataprotection.ie**
Or by phone to tel: 0761 104 800

15.0 Appendices

- Data Subject Access Request Form
- Data Breach Form
- DPIA Form

Data Protection
Subject Access Request (SAR)
Application Form

Request for access to Personal Data under the General Data Protection Regulation (GDPR) and Data Protection Acts 1988-2018.

Notes:

1. ***In order to respond to your request for personal data, you will need to provide us with adequate Proof of Identity.***
2. ***Where a request is manifestly unfounded, excessive, of a repetitive nature or where more than one copy of the data is sought, a reasonable fee may apply.***
3. ***You may contact our Data Protection Officer to assist you in the completion of this Form.***
4. ***A copy of our Privacy Statement is available at www.stpatrickskilkenny.com***
5. ***We will endeavour to respond to you within one month of receipt of the request. This one-month period may be extended by a 2 further months, where necessary, taking into account the complexity of the request. If an extension is necessary, we will inform you of any extension within one month of receipt of the request, giving you the reason why.***

Data Retention

We will only keep a copy of these documents until your subject access request has been fully processed and issued to you and all relevant review or appeal procedure timelines have expired.

Please complete **all parts** of this Form **in full**.

Part 1 – Details of Data Subject (Your Details)

Contact Details *(in block capitals)***:**

Name: _____

Surname: _____

Address: _____

_____

_____

Eircode: _____

Contact Phone Number: _____

E-mail Address (where applicable): _____

Part 2 – Details of Request

Help Us to Help You!

To assist us in locating the data you are requesting, please include as many specific details as possible in relation to your interactions with us in the past (e.g. please state the area(s) of the organisation your data may be located or you have corresponded with/the types of applications you may have made, etc).

_____

_____

_____

Please tell us the relevant period of time or timelines involved (i.e. the relevant dates e.g. *01 January 2018 – 31 December 2018* for which you are seeking the personal data).

_____

_____

_____

Please provide us with any reference numbers relating to your contact with us in the past (e.g. previous correspondence references, case reference numbers, etc.).

_____

_____

_____

Please provide us with any other specific details that you feel are relevant in assisting us in locating your personal data. (e.g. by providing us with as much detail as possible in relation to your access request, we will be able to assist you more efficiently).

_____

_____

_____

_____

_____

_____

Part 3 - Declaration

I declare that all the details I have provided in this Form are true and complete to the best of my knowledge.

Signature of Requester: _____

Date: _____

Please return the completed Form by post to:

Data Protection Officer
S Patrick's Centre
Kells Road
Kilkenny

Or by e-mail to:
aine.forde@stpatrickskilkenny.ie

Or by phone:
056 772 2170

Further information on Data Protection:

- The website of the Data Protection Commissioner – www.dataprotection.ie or
- Make contact with the Office of the Data Protection Commissioner by phone on Tel. 0761 104 800 or by email at: info@dataprotection.ie.

Part 4 - Checklist

Please remember to check that you have:

1. Completed the Subject Access (SAR) Request form in full - YES/NO
2. Signed and dated the Declaration on page 4 - YES/NO
3. Provided us with sufficient details to locate your personal data - YES/NO
4. Provided adequate Proof of Identity - YES/NO

1 DATA BREACH INCIDENT FORM

Employee Reporting Breach:			
NAME:		**TITLE:**	
DATE:		**TIME:**	
TEL:		**EMAIL:**	
INCIDENT INFORMATION:			
DATE/TIME OR PERIOD OF BREACH:			
DATE THE DATA PROTECTION OFFICER WAS NOTIFIED:			
DESCRIPTION & NATURE OF BREACH:			
CATEGORIES OF DATA SUBJECTS AFFECTED:		Person Supported/Employee	
CATEGORIES OF PERSONAL DATA RECORDS CONCERNED:			
NO. OF DATA SUBJECTS AFFECTED:		**NO. OF RECORDS INVOLVED:**	
IMMEDIATE ACTION TAKEN TO CONTAIN/MITIGATE BREACH:			
EMPLOYEES INVOLVED IN BREACH:			
PROCEDURES INVOLVED IN BREACH:			
THIRD PARTIES INVOLVED IN BREACH:			

Signed _____ **Dated**: _____

Data Protection Impact Assessment

This assessment:

- Is required where possible, ***at the beginning*** of any proposed major project/system, or a change to an existing project/system, which involves processing of personal information.
- Should ensure that any risks to the personal information will be considered, evaluated and appropriately managed in this project/system.
- Must be undertaken by the individual/project team proposing the project/system/change. The Data Protection Officer (Áine Forde) must be consulted in the completion of this form and is happy to assist you as required.
- Can be submitted and subsequently re-assessed in light of changing information.
- Will not be published, but will be maintained on file with the Data Protection Officer for the purposes of GDPR compliance. It is important to note where safeguards to mitigate risks cannot be determined, or risks remain high, the Data Protection Officer must notify the Data Protection Commissioner ***in advance*** of undertaking the processing.

From 25th May 2018, non-compliance with this requirement is an offence under the General Data Protection Regulation (GDPR) and is subject to fines from the Office of the Data Protection Commissioner.

1. What is the project / system? *Why do we need it and what does it aim to achieve? Is this a new system or a change to an existing system? What type of personal information is processed? Will this proposal generate new personal information?*

2.	**What is the risk? What particular part of the project / system is giving rise to the risk?** *Why do you need this assessment? What risks to personal data are involved in this process? How will the project/system be carried out? Will data be shared with anyone? How will data be used, stored and deleted?*

3.	**What function will be affected by this project/system/change?** *Will it be limited to one function area?*

4. Risk Mitigation

What is the benefit of this system/procedure? Have you completed a risk/benefit analysis in terms of personal/sensitive data? Is there an alternative system/procedure? What is the level of risk based on the likelihood of occurrence?

5. Individuals/Parties affected by or involved in the process/system

Have all impacted parties been consulted/considered in this process? If not, why not? Is legal advice required?

6.	Sign Off and Measures / Notes *Signatures of the System Proposer, Operations Manager (if required) and Data Protection Officer are mandatory.*		
(a)	System Proposer	Date:	Comment
(b)	Operations Manager	Date:	Comment
(c)	Data Protection Officer	Date:	Comment