# DATA PROTECTION POLICY

**CONTENTS**

# 1 Purpose

This policy establishes an effective, accountable and transparent framework for ensuring compliance with the requirements of the Data Protection (Jersey) Law 2018.

# 2 Scope

This policy applies to Jersey Eating Disorder Support (JEDS), referred to as 'we' or 'our' throughout this policy, and to all committee members, employees and volunteers, referred to as 'staff' throughout this policy that handle Personal data or deal with the public. JEDS is registered with the Jersey Charities Commissioner, number 157.

# 3 Policy Statement

We are committed to conducting our business in accordance with all applicable data protection laws and regulations and in line with the highest standards of ethical conduct.

This policy sets forth the expected behaviours of our staff and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to our staff or individuals receiving our support via group/ 1to1 per support groups (i.e. the data subject).

Personal data is any information (including opinions and intentions) which relates to an identified or identifiable natural person. Personal data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process personal data. An organisation that handles personal data and makes decisions about its use is known as a Data Controller. We, as a Data Controller, are responsible for ensuring compliance with the data protection requirements outlined in this policy. Non-compliance may expose us to complaints, regulatory action, fines and/or reputational damage.

Our Committee and Staff are fully committed to ensuring continued and effective implementation of this policy and expects all our volunteers and third parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

# 4 Governance

**Data Protection Lead (DPL)**

- To demonstrate our commitment to data protection, and to enhance the effectiveness of our compliance efforts, we have appointed a DPL for JEDS to oversee all data protection day to day matters on our behalf. The DPL duties include, but not limited to:
    - Act as the first point of contact for staff and those we support to go to for day-to-day data protection issues.
    - Monitor and collate any DSAR received by any of our staff.

- Monitor and identify any risks associated with data protection issues.

**Data Protection by Design**

To ensure that all data protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing. We must ensure that a Data Protection Impact Assessment (DPIA) is conducted, for all new and/or revised systems or processes for which it has responsibility. The subsequent findings of the DPIA must then be submitted to the Committee for review and approval.

**Compliance Monitoring**

To confirm that an adequate level of compliance that is being achieved by all our staff in relation to this policy, the DPL will carry out an annual data protection compliance audit for all such services. Each audit will, as a minimum, assess:

- Compliance with policy in relation to the protection of personal data, including:
- The assignment of responsibilities;
  - ✔ Raising awareness; and,
  - ✔ Arranging training for our volunteers;
- The effectiveness of data protection related operational practices, including;
  - ✔ Data subject rights;
  - ✔ Personal data transfers;
  - ✔ Personal data incident management;
  - ✔ Personal data complaints handling;
  - ✔ The level of understanding of data protection policies and privacy notices;
  - ✔ The currency of data protection policies and privacy notices;
  - ✔ The accuracy of personal data being stored;
  - ✔ The conformity of data processor activities; and,
  - ✔ The adequacy of procedures for redressing poor compliance and personal data breaches.

The DPL, in cooperation with our Committee, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame.

## 5 Data Protection Principles

We have adopted the following principles to govern our collection, use, retention, transfer, disclosure and destruction of personal data:

**Principle 1: Lawfulness, Fairness and Transparency**. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This means, we

must tell the data subject what processing will occur (transparency), the processing must match the description given to the data subject (fairness), and it must be for one of the purposes specified in the applicable data protection regulation (lawfulness).

**Principle 2: Purpose Limitation.** Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means we must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

**Principle 3: Data Minimisation.** Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. This means we must not store any personal data beyond what is strictly required.

**Principle 4: Accuracy.** Personal data shall be accurate and, kept up to date. This means we must have in place processes for identifying and addressing out-of-date, incorrect and redundant personal data.

**Principle 5: Storage Limitation.** Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. This means we must, wherever possible, store personal data in a way that limits or prevents identification of the data subject.

**Principle 6: Integrity & Confidentiality.** Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage. We must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

**Principle 7: Accountability.** The Data Controller (JEDS) shall be responsible for and be able to demonstrate compliance. This means the we must demonstrate that the six data protection principles (outlined above) are met for all personal data for which it is responsible.

# 6 Data collection

**Data Sources**

Personal data should be collected only from the data subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the personal data from other persons or bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the data subject or to prevent serious loss or injury to another person.

If personal data is collected from someone other than the data subject, the data subject must be informed of the collection unless one of the following apply:

- The data subject has received the required information by other means.

- The information must remain confidential due to a professional secrecy obligation
- A national law expressly provides for the collection, processing, or transfer of the personal data.

Where it has been determined that notification to a data subject is required, notification should occur promptly, but in no case later than:

- 28 days from the first collection or recording of the personal data
- At the time of first communication if used for communication with the data subject
- At the time of disclosure if disclosed to another recipient.

**Data subject consent**

We will obtain personal data only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned. Where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their personal data, we are committed to seeking such consent. The DPL, in cooperation with our Committee, shall establish a system for obtaining and documenting data subject consent for the collection, processing, and/or transfer of their personal data.

**Data subject Notification**

We will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide data subjects with information as to the purpose of the processing of their personal data. When the data subject is asked to give consent to the processing of personal data and when any personal data is collected from the data subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- The data subject already has the information;
- A legal exemption applies to the requirements for disclosure and/or consent.

The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the Data Protection Adviser. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

**External Privacy Notices**

Our website will include an online ‘Privacy Notice’ and an online ‘Cookie Notice’ fulfilling the requirements of applicable law.

# 7 Data Use

**Data processing**

We use the personal data of our clients for the following broad purposes:

- The general running and business administration of our services.
- To provide services to our clients.
- The ongoing administration and management of client services.

The use of client's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a client's expectations that their details will be used by us to respond to a client's request for information about the services on offer. However, it will not be within their reasonable expectations that we would then provide their details to third parties for marketing purposes.

We will process personal data in accordance with all applicable laws and applicable contractual obligations. More specifically, we will not process personal data unless at least one of the following requirements are met:

- The data subject has given consent to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child).

There are some circumstances in which personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. When making a determination as to the compatibility of the new reason for processing, guidance and approval must be obtained from the DPL before any such processing may commence.

In any circumstance where consent has not been gained for the specific processing in question, we will address the following additional conditions to determine the fairness and transparency of any processing beyond the original purpose for which the personal data was collected:

- Any link between the purpose for which the personal data was collected and the reasons for intended further processing;
- The context in which the personal data has been collected, in particular regarding the relationship between data subject and the Data Controller.
- The nature of the personal data, in particular whether special categories of data are being processed; or
- Whether personal data related to criminal convictions and offences are being processed.
- The possible consequences of the intended further processing for the data subject/

- The existence of appropriate safeguards pertaining to further processing, which may include encryption, anonymisation or pseudonymisation.

**Special Categories of Data**

We will only process special categories of data (also known as sensitive data) where the data subject explicitly consents to such processing or where one of the following conditions apply:

- The processing relates to personal data which has already been made public by the data subject.
- The processing is necessary for the establishment, exercise or defence of legal claims.
- The processing is specifically authorised or required by law.
- The 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.
- Further conditions, including limitations, based upon national law related to the processing of genetic data, biometric data or data concerning health.

In any situation where special categories of data are to be processed, prior approval must be obtained from the DPL, and the basis for the processing clearly recorded with the personal data in question. Where special categories of data are being processed, we will adopt additional protection measures.

**Data Quality**

We will adopt all necessary measures to ensure that the personal data it collects, and processes is complete and accurate in the first instance and is updated to reflect the current situation of the data subject. The measures adopted by us to ensure data quality include:

- Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the data subject does not request rectification.
- Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of personal data if in violation of any of the data protection principles or if the personal data is no longer required.
- Restriction, rather than deletion of personal data, insofar as:
  - ✔ a law prohibits erasure.
  - ✔ erasure would impair legitimate interests of the data subject.
  - ✔ the data subject disputes that their personal data is correct, and it cannot be clearly ascertained whether their information is correct or incorrect.

**Profiling & Automated Decision Making**

We do not profile or use automated decision making when processing personal data.

## 8 Data Retention

To ensure fair processing, personal data will not be retained by us for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed. The length of time for which we need to retain personal data is set out in our '*Data Retention Schedule'*. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule.

All personal data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

## 9 Data Protection

We will adopt physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment. A summary of the personal data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which personal data are processed.
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations.
- Ensure that personal data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the personal data was entered into, modified on or removed from a data processing system.
- Ensure that in the case where processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Data Controller.
- Ensure that personal data is protected against undesired destruction or loss.
- Ensure that personal data collected for different purposes can and is processed separately.
- Ensure that personal data is not kept longer than necessary

## 10 Data subject Requests

The DPL will establish a system to enable and facilitate the exercise of data subject rights related to:

- Information access.
- Objection to processing.
- Objection to automated decision-making and profiling.
- Restriction of processing.

- Data portability.
- Data rectification.
- Data erasure.

If an individual makes a request relating to any of the rights listed above, we will consider each such request in accordance with the Data protection (jersey) Law 2018 (DPJL). No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature. We have provided a subject access request form on our website. Data Subjects making a request will be asked to complete this form and provide identification.

The use of this form is not mandatory, requests can be made verbally, in writing, via our social media account and to any staff member of JEDS,

It should be noted that situations may arise where providing the information requested by a data subject would disclose personal data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

## 11 Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that personal data be shared without the knowledge or consent of a data subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

If we process personal data for one of these purposes, then it may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question. If we receive a request from a court or any regulatory or law enforcement authority for information relating to our contact, we must immediately notify the DPL who will provide comprehensive guidance and assistance.

## 12 Data Protection Training

All our staff that have access to personal data will have their responsibilities under this policy outlined to them as part of their induction training. In addition, we will provide regular Data Protection training and procedural guidance for our volunteers.

## 13 Data Transfers

We may transfer personal data to internal or third-party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. third countries), they must be

made in compliance with an approved transfer mechanism. We may only transfer personal data where one of the transfer scenarios listed below applies:

- The data subject has given Consent to the proposed transfer;
- The transfer is necessary for the performance of a contract with the data subject;
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the data subject's request;
- The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of the data subject;
- The transfer is legally required on important public interest grounds;
- The transfer is necessary for the establishment, exercise or defence of legal claims; and
- The transfer is necessary in order to protect the vital interests of the data subject

## 14 Complaints handling

Data subjects with a complaint about the processing of their personal data, should put forward the matter in writing to the DPL. The DPL for JEDS is Karen Dingle and can be contacted at:

**Data Protection Lead**
Cavatina
82 Miladi Farm
Longueville
St Saviour
Jersey
JE2 7QH

eatdisordergroupjersey@hotmail.com

An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The DPL will inform the data subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the data subject and the DPL, then the data subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Jersey Office of the Information Commissioner.

## 15 Breach Reporting

Any individual who suspects that a personal data breach has occurred due to the theft or exposure of personal data must notify the DPL immediately, providing a description of what occurred. Notification of the incident can be made via e-mail to: eatdisordergroupjersey@hotmail.com

The DPL will investigate all reported incidents to confirm whether a personal data breach has occurred. If a personal data breach is confirmed, the DPL will follow the relevant

authorised procedure based on the severity and quantity of the personal data involved. For severe personal data breaches, our Committee will initiate a response team to coordinate and manage the personal data breach response.

## 16 Roles and Responsibilities

**Implementation**

Our Committee will ensure that all our staff responsible for the processing of personal data are aware of and comply with the contents of this policy. In addition, we will make sure all third parties engaged to process personal data on our behalf (i.e. their data processors) are aware of and comply with the contents of this policy.

Assurance of such compliance must be obtained from all third parties, whether companies or individuals, prior to granting them access to personal data controlled by us.

## 17 Review

This policy will be reviewed by the DPL every three years, unless there are any changes to regulations or legislation that would require a review earlier.

## 18 Records Management

JEDS must maintain all records relevant to administering this policy and procedure in electronic form in a recognised JEDS recordkeeping system.

All records relevant to administering this policy and procedure will be retained for a period of 5 years.

## 19 Terms and Definitions

**Relevant Jurisdictional Laws:** See section 20.

**Data Controller:** the entity that determines the purposes, conditions and means of the processing of Personal Data (JEDS)

**Data Processor:** the entity that processes data on behalf of the Data Controller (any third-party contractor that has access to data, will be a processor)

**Data Protection Authority:** national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union. For Jersey it is the Jersey Office of the Information Commissioner (www.Jerseyoic.org).

**Data Protection Lead:** The DPL of JEDS, Karen Dingle, who deals with day to day Data Protection requests and issues.

**Data Protection Advisor (DPA):** an expert on data privacy who works independently to ensure that JEDS is adhering to the policies and procedures set forth in the DPJL. Propelfwd will act as the DPA for JEDS on an Ad-Hoc basis, so will be called upon if and when needed.

**Data subject:** a natural person whose personal data is processed by a controller or processor.

**Personal Data:** any information related to a natural person or 'data subject', that can be used to directly or indirectly identify the person.

**Privacy Impact Assessment:** a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data.

**Processing:** any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

**Regulation:** a binding legislative act that must be applied in its entirety across the Union. In Jersey it is the Data Protection (Jersey) Law 2018.

**Subject Access Right:** also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them.

## 20 Legislation and Policy

- Data Protection (Jersey) Law 2018 (DPJL)
- JEDS Data Protection Policy and Procedures

## 21 Approval and Reviews

| Approval and Review | Details |
|---|---|
| Approval Authority | |
| Data Protection Lead | |
| Next Review Date | |

| Approval and Amendment History | Details |
|---|---|
| Original Approval Authority and Date | |
| Amendment Authority and Date | |