# General Data Protection Policy

Finglas Addiction Support Team (FAST)

**QuAD 004 -02**

**Revision Period : 2 Years**

Reviewed:20/05/2019

Revision date: 20/05/2020

| | |
|---|---|
| 1.Responsibility for approval of policy | **Board/CEO** |
| 2.Responsibility for implementation | **Senior Management Team (SMT)** |
| 3.Responsibility for ensuring review | **CEO/ SMT** |

## 1. Policy Statement

FAST places high importance on the correct, lawful and fair handling of all personal data and is fully committed to protection of the rights and privacy of individuals whose personal information it holds. This commitment is underpinned by compliance with the statutory measures that ensure these rights. FAST has put in place a range of systems and procedures, which it reviews on a regular basis, in order to protect these rights.

## 2. Purpose

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of FAST. This includes obligations in dealing with personal data, to ensure the organisation complies with the requirements of the relevant Irish legislation, namely the General Data Protection Regulation (the "GDPR") and the Irish Data Protection Acts 1988 to 2018 (the "Acts").

## 3. Scope

3.1. This policy covers all Personal and Sensitive Data held in relation to data subjects by FAST and applies to Personal Data that comes within the scope of Article 2(1) the GDPR. The policy covers both personal and sensitive personal data held in relation to data subjects of FAST. Both personal and sensitive personal data will be treated with equal care by FAST and will be equally referred to as personal data in this policy, unless specifically stated otherwise.

3.2. FAST makes no distinction between the rights of Data Subjects who are employees, and those who are not. All are treated equally under this policy.

3.3. The policy applies equally to personal data held in manual and automated form.

3.4. This policy should be read in conjunction with :

- SOP 007 Subject Access Request
- SOP 008 Data Retention and Destruction, *including Data Loss Notification and Data Retention Periods List*.
- SOP 009 ICT Infrastructure
- SOP 010 Data Breach

## 4. Responsibility

4.1. The Board Members of FAST are ultimately responsible for ensuring that FAST meets its legal obligations.

4.2. The Audit, Finance and Governance committee (AFG) are responsible for managing any Data protection issues in the first instance, via the senior management team. Where necessary, an external expert will be contracted.

4.3. All staff have responsibility for ensuring that data is collected, stored and handled appropriately.

4.4. Staff, Contractors and Board Members of FAST are also required to take appropriate precautions to ensure that personal information is not disclosed deliberately or accidentally either orally or in writing to any unauthorised third party.

## 5. Glossary of Terms and Definitions:

| Term | Definition |
|---|---|
| **Data** | This includes both automated and manual data.<br>Automated data means data held on computer, or stored with the intention that it is processed on computer.<br>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** | Any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person |
| **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 mental or physical health, information in relation to one's Sexual Orientation, information in relation to commission of a crime and information relating to conviction for a criminal offence. |
| **Pseudonymous Data** | This data is still treated as personal data because it enables the identification of individuals albeit via a key. |
| **Anonymous Data** | This data is rendered anonymous because there is no way that an individual can be identified from this data. Therefore, the GDPR does not apply to such data. |
| **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 who 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. |
| **Relevant Filing System** | Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers), and that 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 retrievable. |

## 6. Rationale

Under General Data Protection Regulations FAST are required to provide data subjects with the legal grounds or lawful basis that they are relying on for processing personal data. The legal grounds for processing personal data are as follows:

1. Consent;
2. Performance of a contract;
3. Legal obligation;
4. Vital interest;
5. Public interest;

Explicit consent or an alternative limited lawful basis is required where special categories, also known as sensitive personal data are being processed. If there is no justification for retaining personal information, then information should be routinely deleted. Information should never be kept "just in case" a use can be found for it in the future. To retain information about our clients to help us to provide a better service to them in the future, we must obtain their consent in advance. ***This is recorded on Form F014, Explicit Consent and attached to the participant's database record.***

## 7. FAST as a Data Controller

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

- Employees of FAST
- Participants of FAST
- Third party service providers engaged by FAST
- BOM members of FAST

In accordance with the Irish Data Protection legislation, this data must be acquired and managed fairly. FAST are committed to ensuring staff has 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 the Data Protection Officer is informed, to ensure appropriate corrective action is taken.

Due to the nature of the services provided by FAST, there is regular and active exchanges of personal data between FAST and its Data Subjects. In addition, FAST shares personal data with Data Processors on Data Subjects' behalf. This is consistent with FAST obligations under the terms of its contract with its Data Processors.

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

## 8. Data Protection Principles

GDPR sets out the following principles with which any party handling Personal Data must comply. **Article 5** in the GDPR states that all Personal Data must be:

| | |
|---|---|
| **1.** | **Processed lawfully**, fairly and in a transparent manner in relation to the data subject; |
| **2.** | **Collected for specified, explicit and legitimate** purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes subject to appropriate safeguards, and provided that there is no risk of breaching the privacy of the data subject; |
| **3.** | **Adequate, relevant and limited** to what is necessary in relation to the purposes for which it is processed; |
| **4.** | **Accurate and where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay; |
| **5.** | **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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of the data subject; |
| **6.** | **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, using appropriate technical or organisational measures; |
| **7.** | Article 5(2) states that the Controller is responsible for and must be able to **demonstrate compliance** with the Data Protection Principles. |
| **8.** | **Respond** to requests by individuals seeking to exercise their data protection rights (for example the right of access) |

8.1. **Lawful Fair and Transparent Data Processing:**

FAST 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 FAST holds their data, and FAST will be able to clearly state purpose or purposes.

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 (FAST)
- 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 necessary so the processing may be fair.

FAST 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, FAST will guarantee collection of the data as justified under one of the other lawful processing conditions i.e. legal obligation, contractual necessity, etc.;
- Where FAST intends to record activity on CCTV or video, a Fair Processing Notice will be posted in full view;
- Processing of the personal data will be carried out only as part of FAST lawful activities, and FAST will safeguard the rights and freedoms of the Data Subject;
- The Data Subjects data will not be disclosed to a third party other than to a party contracted to FAST and operating on its behalf

8.2. **Processed for Specified, Explicit and Legitimate Purposes:**

FAST will obtain data for purposes which are specific, lawful and clearly stated. The purposes for which FAST processes Personal Data will be available to data subjects at the time of collection of their Personal Data

A Data Subject will have the right to question the purpose(s) for which FAST holds their data, and FAST will be able to clearly state purpose or purposes.

FAST will not further process personal data in a manner that is incompatible with those purposes unless:

- the consent of the data subject has been obtained; ***Form F015 Consent to share***
- in order to comply with a legal obligation; or,
- if further processing is for archiving purposes in the public interest or scientific and historical research or statistical purposes, the appropriate safeguards are in place and there is no risk of breaching the privacy of the data subject

8.3. **Adequate, Relevant and Limited Data Processing:**

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

8.4. **Accuracy of Data and Keeping Data up to date:**

FAST will:

- ensure administrative and IT validation processes are in place to conduct regular assessments of data accuracy;
- conduct periodic reviews and audits to ensure relevant data is kept accurate and up-to-date. FAST will conduct audits every six months to ensure accuracy and staff contact details and details on next-of-kin are reviewed and updated every two years; and
- conduct regular assessments in order to establish the need to keep certain personal data;
- amend inaccurate data which has been notified to FAST by the data subject or is revealed as a result of a subject access request.

8.5. **Timely processing:**

FAST have 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, FAST undertakes to destroy, erase or otherwise put this data beyond use. Please refer to *SOP 008 Data Retention and Destruction*, *including Data Loss Notification and Data Retention Periods List*.

8.6. **Secure Processing:**

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

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

Such measures are detailed in *SOP010, ICT Infrastructure*

8.7. **Demonstrate Compliance - Accountability:**

GDPR obliges organisations to demonstrate that their processing activities are compliant with the Data Protection Principles. The principle of accountability seeks to guarantee the enforcement of these principles.

FAST will demonstrate compliance in the following ways:

- by maintaining an inventory of processing categories, Appendix 1 which will include details on personal data collected, held or processed in line with **Article 30** – 'Records of Processing Activities' upon request, these records will be disclosed to the Data Protection Commissioner's Office;
- When FAST is acting as a Data Controller this record schedule will contain the following information:
  - Entry date
  - Record name;
  - Categories of data;
  - Purpose;
  - Categories of data subject;
  - Processor name;
  - Retention period;
  - Security measures;

This information is recorded in Appendix 1

## 9. The Rights of Data Subjects

FAST has implemented SOP 007 Data Subject Access Request procedure, to manage requests in an efficient manner and within the timelines stipulated in GDPR.

As part of day-to-day operations, FAST staff members 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 FAST, such a request gives rise to access rights in favour of the Data Subject. FAST staff are required to ensure that, where necessary, such requests are forwarded to the AFG committee in a timely manner, so that they are processed efficiently as possible.

GDPR sets out the following rights applicable to data subjects. These rights are restricted in certain circumstances as prescribed under Article 23 of the GDPR and the Acts:

- the right to be informed;
- the right of access;
- the right of rectification;
- the right to restrict processing;
- the right to data portability;
- the right to object;
- rights with respect to automated decision-making and profiling;
- the right to withdraw consent; and
- the right to erasure (also known as the "right to be forgotten")
- to know whether a data controller holds any personal data about them;
- to receive a description of the data held about them and, if permissible and practical, a copy of the data;
- to be informed of the reason(s) for which their data is being processed, and from where it was received;
- to be informed whether the information is being disclosed to anyone apart from the original recipient of the data; and if so, the identity of those recipients;
- the right to data portability - Data subjects can ask for their personal data;
- if the data is being applied to form automated decisions about the data subject, to be told what logic the system uses to make those decisions and be permitted to request human intervention;
- the right to rectify incorrect personal data held;
- the right to erase personal data, *(also known as the "right to be forgotten")* - only applicable in certain circumstances and is not an absolute right
- The data subject can request erasure of their personal data if:
    - the personal data is no longer necessary for the purpose the data was originally collected or processed
    - you are relying on consent as the lawful basis for holding the data, and the individual withdraws consent

## 10. Data Subject Access Request Refusals (DSAR)

There are situations where individuals do not have a right to see information relating to them. For instance:

- If the information is kept only for the purpose of statistics or research, and where the results of the statistical work or research are not made available in an identifiable form.

- Requests made for other, non-data protection purposes can be rejected. If the AFG refuses a DSAR on behalf of FAST, the reasons for the rejection must be clearly outlined in writing. Any individual dissatisfied with the outcome of his/her DSAR is entitled to make a request for the outcome to be reviewed.

## 11. Data Breach

FAST has put in place a procedure, *SOP010 Data Breach Notification* along with an incident log and form. This procedure outlines the general principles and actions for successfully managing the response to a data breach as well as fulfilling the obligations of notification to the Data Protection Commissioner and individuals as required under GDPR. FAST treats data breaches very seriously and any staff members who become aware of potential or actual data breaches, must notify a member of the Senior Management Team immediately.

## 12. Training

General Data Protection training will be provided through staff presentations, attendance at Data Protection-specific training events and seminars where appropriate, staff briefings and information notices. The SMT via the AFG is responsible for overseeing such training.

## 13. Records

13.1. Current Employee Personal Data is stored securely on a cloud based software *and* electronically onsite in the organisations network specific drive which has restricted access.

13.2. Current Customer and Supplier Data is stored electronically on site in third party software. It is stored on the organisations network specific drive which has restricted access.

13.3. Participant records are held electronically on cloud based software. The cloud data is held within the EEA and sets a security compliance score. FAST ensures its security rate is no less than 80% - Very Good.

## 14. Publication

This policy shall be published on the organisations' website without any cited procedures or appendices