# DATA PROTECTION POLICY

## 1 Introduction

Azalea is committed to good practice in the handling of personal data and careful compliance with the requirements of the UK Data Protection Act.

Azalea is committed to good data management, in order to protect people from harm. In the main this means:

- keeping information securely in the right hands and
- holding good quality information

Azalea also ensures that it takes account of the legitimate concerns of individuals about the ways in which their data may be used. In particular, Azalea aims to be open and transparent in the way it uses personal data and, where relevant, to give individuals a choice over what data is held and how it is used.

The most important risks which this policy addresses are:

- Inappropriate disclosure of personal data about staff, individual volunteers or beneficiaries or donors that puts an individual at personal risk or contravenes a duty of confidentiality
- Negligent loss of data that would cause concern to people whose data was lost and would seriously affect Azalea's reputation
- Failure to engage Data Processors on legally compliant terms (Data Processors are external contractors and suppliers of outsourced services).

## 2 Who the policy covers

This policy covers all:

- Azalea staff
- Azalea volunteers (including Trustees)
- Azalea guests/clients.

## 3 Terms and definitions

**Azalea staff/volunteers'** refers to all staff and volunteers who form Azalea's primary team and includes the CEO, staff team, Encompass Frontline Volunteer team and Flint Frontline volunteer team. This also includes Trustees. It excludes those who serve Azalea from a distance e.g., cake makers, prayer support, donors.

**'Guests/clients'** refers to the women (guests) involved in sex trafficking and exploitation who are engaging with Encompass' services, and the men (clients) who

are/have been purchasing sex and are engaging with Flint's services, whether that is a single encounter during outreach, or an ongoing relationship.

**'Sex trafficking'** refers to the experiences of Encompass service users who are trafficked for the purpose of sexual exploitation both locally, nationally and internationally.

**'Human trafficking'** as defined by the Palermo Protocol, the first internationally recognised definition of human trafficking:

*"Trafficking in persons shall mean the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control of another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or removal of organs."*

## 4 Responsibilities

The Board of Trustees of Azalea recognises its overall legal responsibility for Data Protection compliance.

Day to day responsibility for Data Protection is delegated to the Operations Manager as the nominated Data Protection Officer.

The main responsibilities of the Data Protection Officer are:

- Briefing the Board on their and Azalea's Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on Data Protection issues and practices in Azalea
- Ensuring that Data Protection induction and regular training takes place
- Approving unusual or controversial disclosures of personal data
- Approving contracts with Data Processors (external contractors and suppliers of outsourced services)
- Notification (i.e. registration with the Information Commissioner)
- Handling requests from individuals for their personal data

All staff (and volunteers) are responsible for understanding and complying with the procedures that Azalea has adopted in order to ensure Data Protection compliance.

All managers of teams have the following responsibilities:

- Assisting the Data Protection Officer in identifying aspects of their area of work which have Data Protection implications so that guidance can be provided as necessary
- Ensuring that their activities take full account of Data Protection requirements
- Including Data Protection and confidentiality in the induction and training of all staff including Agency or casual staff and volunteers. (And freelance consultants if relevant)

***'Data controller'*** refers to the organisation that decides why and how personal data is to be processed. Azalea is the 'data controller' under the Data Protection Act (1998) and is therefore ultimately responsible for implementation.

However, day to day matters relating to this data protection policy and the handling of subject access requests will be dealt with by the Data Protection Officer.

***'Data subjects'*** refers to the individual whose personal data is being processed.

***'Processing'*** refers to the use made of personal data including:

- obtaining and retrieving
- holding and storing
- making available within or outside the organisation printing, sorting, matching, comparing, destroying

## 4.1 Data management

All data collection and recording systems are designed to ensure that the data collected is adequate, relevant and not excessive for the purpose. Where relevant, staff and volunteers are given training in good data recording practice to ensure that the data they record is appropriate.

Azalea takes reasonable steps ensure that information is kept accurate and up to date by asking data subjects at appropriate intervals to check their key information for accuracy and to notify Azalea if there have been any changes.

Azalea maintains an agreed retention schedule based on legal and practical requirements.

## 4.2 Retention of records

The Data Protection Act states that data should not be kept for longer than is necessary for the purposes for which it is processed.

Therefore Azalea will use following time periods for retaining staff, volunteer and guests/client data.

These guidelines relate to all staff at Azalea who may hold information about individuals.

## 4.3 Staff/team data

| Details | Period |
|---|---|
| Applicants for jobs who are not short-listed for interview. | **6 months** |
| Applicants short-listed for interview that are not successful. | **12 months** |
| Ex-employees. | **10 years** |
| Summary of record of service of ex-employees. | **20 years** |

*****It is important to remember that computer records as well as manual files are included in this protocol*****

### 4.4 Volunteer data

| Details | Period |
|---|---|
| Once an individual has ceased to be any type of volunteer, any data pertaining to them must be kept securely. | **5 years** |
| Where this is hard copy it must be archived in a secure location or, if the information is on computer it must be filed onto a disc and held securely. | **5 years** |
| Summary of data: For the purposes of giving volunteers references. | **3 years** |
| For keeping Volunteers up to date with Azalea. | **5 years** |
| For Safeguarding purposes: all notes / information required. | **10 years** (subject to any further specific safeguarding regulations) |

### 4.5 Guests/client data

'Guests/Client' refers to anyone caught in sexual exploitation or any others who use Azalea's services, whether that is a single encounter during outreach, or an on-going befriending relationship.

| Details | Period |
|---|---|
| Individuals who have used Azalea service on a single encounter /irregular basis. | **10 years** |
| Individuals who have signed up to Azalea related programmes / regular users. | **20 years** |
| For safeguarding purposes: all notes/information required. | **10 years** (subject to any further specific safeguarding regulations) |

Where this is hard copy it must be archived in a secure location or, if the information is on computer it must be filed onto a disc and held securely.

### 4.6 Disposal of data

Azalea will carry out a periodic review to identify all data that has reached its disposal date. All relevant data on individuals must be disposed of sensitively and completely. If the information is hard copy it must be shredded or incinerated. If the information is soft copy (i.e. on a hard drive or computer disk) it must be deleted from the file, disk and the recycle bin of the computer. Remember to check for all copies of the data.

## 5 Confidentiality and security

Azalea recognises that a clear policy on confidentiality of personal data – in particular that of staff and beneficiaries underpins security. It maintains a policy that sets out which staff and volunteers are authorised to access which data and for which purposes. In particular, this clarifies when data may be disclosed outside Azalea and whether such disclosures require the individual's consent. See the separate confidentiality policy.

Azalea maintains a security policy that sets out measures to protect data 'at rest' – including access being restricted only to authorised staff – and measures to protect data 'in transit', whether it is physically removed from a secure environment or transmitted electronically.

All staff, freelance consultants, volunteers and Trustees are required to abide by any security measures designed to protect personal data from loss, misuse or inappropriate disclosure.

## 6 Principles underlying operational procedures

Good Data Protection practice is, wherever relevant, incorporated into everyday operational procedures. These aim to include:

- Transparency, so that all the individuals about whom data is collected are made aware of the uses that Azalea makes of information about them, and in particular to whom it may be disclosed.
- Informed consent, where necessary, especially in the case of donors and clients.
- Good quality data, so that all the data held about individuals is accurate and can be justified as adequate, relevant and not excessive.
- Clear archiving and retention periods.
- Security, proportionate to the risk of information being lost or falling into the wrong hands.

## 7 Specific legal provisions

Azalea makes no charge for subject access.

- The UK Data Protection Act gives rights of access to an individual to the personal data held on them. They can access this data at any time by making a written request to the Operation Manager
- The Operations Manager must be satisfied with the identification of the individual making the request and can ask for information or documentation as proof
- Individuals are entitled to a copy of the information held on them, both on computer, in emails and as part of a relevant filing system within one month of their request being received
- Individuals also have a right to know why their information is being held, who that information is being disclosed to and for what purpose.

Azalea maintains an up-to-date Notification with the Information Commissioner as required by law.

All contracts between Azalea and external data processors are reviewed regularly by the Data Protection Officer for compliance with Data Protection Act requirements.