**THE ARCHWAY FOUNDATION**
**DATA PROTECTION POLICY**

## 1. Introduction

The Archway Foundation collects and use certain types of information about Service Users (referred to elsewhere in this document as Friends) and other individuals who come into contact with The Archway Foundation in order to carry on our work. Data is held in accordance with Article 5 of the GDPR legislation:

a) It is processed lawfully, fairly and in a transparent manner in relation to individuals;

b) It is collected for specified, explicit and legitimate purposes and will not be further processed in a manner that is incompatible with those purposes

c) It is adequate, relevant and limited to what is necessary for the operation of our services

d) Every reasonable step is taken to ensure the accuracy of data, and that personal data that are inaccurate are erased or rectified without delay when drawn to our attention

e) Data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

and

f) Data is 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.

The CEO of the Archway Foundation is the Data Controller under the Act, which means that s/he determines for what purposes personal information held will be used.

## 2. Legal basis for holding data.

Under the GDPR, there are six lawful bases for holding data. Data is held under three of these:

Legitimate interest: This covers data held for Volunteers, Trustees, Friends and data relating to health and safety in delivering our services.

Contract: This covers data held for staff.

Consent: This covers data held for fund raising and publicity

Special category data requires both a lawful basis and another justification. It includes data which may be considered to be sensitive – for example which could cause embarrassment or distress to the individual or used as a basis of discrimination – and requires an additional justification. Archway Foundation holds certain types of special category data.

Details of categories under which data is held, together with any additional justification required, are given in Appendix B.

**3. Data Privacy and Disclosure**

The Archway Foundation regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

Data is held in encrypted form on an external server. All data is available to all members of the Archway staff team through individual password access to this database. All members for the team have received training in data protection principles.

Data required for service operation on individual Friends is made available to key volunteers through telephone calls or email. For example name and contact details are given to volunteer drivers, volunteers providing telephone support or undertaking individual support roles.

Data protection principles and procedures are included in volunteer training.

Data on individuals considered to be sensitive (possibly taken from referral data or reports from previous sessions), affecting health and safety or the conduct of sessions, whether social groups or individual support, is provided on a need to know basis (eg to volunteers transporting or visiting Friends or telephoning Friends). Because of its greater sensitivity relevant individuals' names will not be used explicitly in any email including this data.

The Archway Foundation may also share data on individuals with other agencies (for example health services) if it decides that the sharing of such data is in the interest of the individual or has a wider Health and Safety interest. Any data supplied for other purposes (for example for fundraising, grant application and reporting etc) will be only of a statistical nature and will not mention individuals.

Where data on individuals is supplied, the individual will normally be made aware of how and with whom their information will be shared. However there are circumstances where the law allows The Archway Foundation to disclose data (including sensitive data) without the data subject's consent (Appendix B).

It is The Archway Foundation's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party. The Archway Foundation will ensure that it has a written contract with any third party processor to ensure compliance with the GDPR.

Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately.

**4. Privacy Notice**

Privacy notices will be provided to individuals under the following categories: Friends, Volunteers (including Trustees), Staff, Donors, Supporters on mailing list.

Privacy notices will include

(i) the data held under each category
(ii) the legal justification under the GDPR and, for legitimate interest data, an explanation of the legitimate interest
(iii) the rights of the individual under the GDPR
(iv) the complaints procedure
(v) details of how to access this data protection policy which will be held online
(vi) record kept of the information held during contact with Archway

For all new contacts a privacy notice will be provided along with a welcome to Archway, by face to face contact, email or post.

**4. Data Collection and processing: rights of individuals**

The Archway Foundation will ensure that the rights of people about whom information is held, are fully upheld. The Archway Foundation will ensure that each Individual/Service User clearly understands why their information is needed, who it will be shared with, and the possible consequences of them refusing the proposed use of the data.

In all cases where data is supplied or modified as a result of a request, it will use all reasonable means to ensure the identity of the person before supplying or modifying data.

In cases where a request has been denied it will also inform the individual of the reason why their request has been denied and of their right to complain to the supervisory authority and to a judicial remedy.

Further information on the rights of the individual are given in Appendix A.

**5. Accountability and Governance**

**Documentation** will be held electronically to comply with the requirements of GDPR. Documentation will include processing activities, covering areas such as processing purposes, data sharing and retention (see Appendix A).

**Contracts** with any company processing data for the Archway Foundation will be in compliance with the GDPR requirements.

**Data protection impact assessment.** Archway does not meet any of the conditions required for a DPIA. Although sensitive data is held, privacy notices will be provided directly to individuals. The possible need for a DPIA will be reviewed each year as a matter of good practice.

**Data Protection Officer.** Archway does not meet the requirements for a data protection officer.

**Codes of conduct and certification**. At this stage Archway does not conform to a particular code of conduct because of the type and scale of processing. . The possible advantages of subscribing to a code of conduct with formal certification will be reviewed each year as a matter of good practice.

**Registration with the ICO.** Archway has Tier 1 registration with the ICO.

**6. Data Breaches**

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include

i. access by an unauthorised third party;

ii. deliberate or accidental action (or inaction) by a controller or processor;

iii. sending personal data to an incorrect recipient;

iv. computing devices containing personal data being lost or stolen;

v. alteration of personal data without permission; and

vi. loss of availability of personal data.

If an individual believes that a data breach has occurred, or has been informed of one, he/she should report it to the Data Controller as soon as possible. If the breach is notifiable, the Data Controller will report to the Information Commissioner's Office according to their procedures. A summary of any data breaches during the year will be made in the annual report to the Board.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, those concerned will be informed directly and without undue delay by their service coordinator or the Data Controller.

Staff and volunteers are aware that deliberate or negligent misapplication of the rules and procedures identified in this policy which leads to a serious data breach may lead to disciplinary action for staff; or action requiring the resignation of a volunteer. However normally any data breach would be considered in the context of improvements to procedures and training and staff and volunteers are encouraged to identify, with the Data Controller, where these might be made.

**7. Performance Auditing**

The GDPR group will

(i) hold an annual audit of any data breaches

(ii) review the policy in line with Archway's policy review procedures

unless there is a serious data breach which leads to a report to the ICO in which case:

(a) the policy must be reviewed and, if necessary updated immediately
(b) The CEO should inform Chair of Trustees immediately)
(c) the breach and the action should be taken to the Trustees at the next Board meeting, and reported at the AGM

In case of any queries or questions in relation to this policy please contact the Data Controller at The Archway Foundation

**Glossary of Terms**

**Data Controller** – The person who (either alone or with others) decides what personal information The Archway Foundation will hold and how it will be held or used.

**Data Protection Act 2018** – The UK legislation that provides a framework for responsible behaviour by those using personal information.

**UK GDPR: General Data Protection Regulations**

**Individual/Service User** – The person whose personal information is being held or processed by The Archway Foundation for example: a client, an employee, or supporter.

**Consent** – is freely given, specific and informed through an explicit agreement

**Processing** – means collecting, amending, handling, storing or disclosing personal information.

**Personal Information** – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees within The Archway Foundation.

**Special Category data**
This replaces and extends the term sensitive data used in earlier data protection legislation. In addition to the sensitive data categories of data about racial or ethnic origin, political affiliations, religion or similar beliefs, trade union membership, physical or mental health, sexuality, criminal record or proceedings, it includes biometric or genetic data.

**Appendix A: Rights of Individuals**

1. The right to be informed. Data Privacy Notices are available to all those on whom Archway holds data, together with a statement of their rights under the GDPR, as given in this section.

2. The right of access. Friends and volunteers should request access to their data through their service coordinator or ask a representative to do so on their behalf. Others should request access through the Data Officer.

If requests to access data by any individual is deemed by Archway to be excessive (in particular because they are repetitive), Archway may refuse to respond, or charge a fee to cover the administrative costs.

*If it believes the request is reasonable, Archway will comply with the request within one month. However Archway does not have to make the change requested as explained above. In this case an explanation will be provided to explain why no action will be taken along with details of complaint procedures.*

3. The right to data correction (rectification). Individuals have the right to correct personal data which is inaccurate or incomplete.

Friends and volunteers should request corrections to their data through their service coordinator in writing (this includes email) or ask a representative to do so on their behalf. Others should request corrections through the Data Officer.

*If it believes the request is reasonable, Archway will comply with the request within one month for simple cases, three months if they are complex. However Archway may refuse your request. In this case an explanation will be provided to explain why no action will be taken along with details of complaint procedures.*

4. The right to erase data. Records are normally erased after two years of the last contact with Archway. There are a number of valid reasons why you might request earlier erasure:

(i) Where the personal data is no longer necessary in relation to the purpose for which it was collected/processed, or an individual you objects to the processing and there is no overriding legitimate interest for continuing it

(ii) For data held under consent, when the individual withdraws consent.

(iii) When the data was unlawfully processed (i.e. otherwise in breach of the GDPR).

(iv) to comply with a legal obligation.

There are also some specific circumstances where the right to erasure does not apply and Archway may refuse the request. Those most relevant to Archway are:

(i) for public health purposes in the public interest;

(ii) the exercise or defense of legal claims.

(iii) to comply with a legal obligation for the performance of a public interest task or exercise of official authority.

Friends and volunteers make a request through their service coordinator or ask a representative to do so on their behalf. Others should do so through the Data Officer.

*If it believes the request is reasonable, Archway will comply with the request within one month for simple cases, three months if they are complex. However Archway may refuse your request. In this case an explanation will be provided to explain why no action will be taken along with details of complaint procedures.*

Note that erasing data held under legitimate interest is likely to mean that Archway can no longer offer services or accept an individual as a volunteer.

5. The right to restrict processing (use of data). Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, personal data may still be held,, but it cannot be processed further.

   The ways in which data is processed are given in Appendix B.

Archway will restrict the processing of personal data in the following circumstances:

(i) Where an individual has contested the accuracy of the personal data, until its accuracy is verified.

(ii) Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual.

(iii) When processing is unlawful but restriction is requested instead of erasure.

(iv) If Archway no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

Friends and volunteers should make a request through their service co-ordinator or ask a representative to do so on their behalf. Others should do so through the Data Officer.

*If it believes the request is reasonable, Archway will comply with the request within one month for simple cases, three months if they are complex. However Archway may refuse your request. In this case an explanation will be provided to explain why no action will be taken along with details of complaint procedures.*

Note that restricting processing for data held under legitimate interest is likely to mean that Archway can no longer offer services or accept an individual as a volunteer.

6. The right to data portability. This is not relevant to the data held by Archway as processing is not carried out automatically.

7. The right to object. You have the right to object under a number of specific categories, including those relevant to the data held by Archway: data being held under legitimate processing or processing for statistical purposes. Archway will stop processing the personal data unless it can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defense of legal claims.

Individuals are informed of their right to object in the privacy notice at the point of first communication.

Friends and volunteers should make an objection through their service coordinator) or ask a representative to do so on their behalf. Others should do so through the Data Officer.

*If it believes the objection is reasonable, Archway will comply with it within one month. However Archway may disagree with the objection. In this case an explanation will be provided to explain why no action will be taken along with details of complaint procedures.*

8. Rights in relation to automated decision making and profiling. Archway does not use automated decision making or profiling techniques.

**Appendix B: Data Held**

**Legal basis for holding data**

Under GDPR legislation there are six reasons for holding data. Reasons relevant to Archway are consent (explicit consent is needed), contractual and legitimate interest.
Friends' Trustee and Volunteer data is covered under the legitimate interest category. Data held on staff is covered under the contractual category other data is held under the consent category.
Legitimate interest data requires special consideration. The ICO guide to GDPR [1] explains this as follows:

***Legitimate interests:*** *the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.*
Further points which hare relevant to Archway in determining whether this category is most appropriate for holding data are:

*i)* *It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.*

*ii)* *There are three elements to the legitimate interest's basis. It helps to think of this as a three-part test. You need to:*
- *identify a legitimate interest;*
- *show that the processing is necessary to achieve it; and*
- *balance it against the individual's interests, rights and freedoms.*

*iii)* *The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.*

*iv)* *The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.*

*v)* *You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interest.*

***Processing of special category (sensitive) data***

If the information is sensitive personal data, at least one of several other conditions must also be met before the processing can comply with the first data protection principle. Those relevant to Archway Foundation are (from GDPR article 9(2),)

*(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes.*

*(c) 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;*

*(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;*

**Friends' Data**

The overriding legitimate interest is the provision of services (social groups, Individual Support) including transport. Data is held for two years following the last contact with the Friend. After that it is deleted from the database. A two year interval is considered appropriate since Friends quite frequently take extended periods away from social groups or other contact, but then take up our services again. We wish to make this as easy as possible for them.

| Data held | Processing | Why is processing of data necessary | Whose interest | Special category data data? | Additional reasons, special category |
|---|---|---|---|---|---|
| Contact details | Provided to staff and key volunteers social group leaders, driver if relevant, Individual Support volunteer if relevant) | To contact Friend and provide service. | Friend's | No | |
| Service details<br><br>(eg Individual Support, social group) | Provided to staff and key volunteers (social group leaders, driver if relevant, Individual Support Volunteer if relevant) | For setting up and maintaining services offered | Friend's | No | |
| Referral details<br><br>*(sensitive data)* | Supplied to key staff (social group organisers) and key volunteers (social group leader or Individual Support Volunteer) | So suitable services and activities can be offered | Friend<br><br>Key volunteers and staff; other Friends at sessions | Yes | GDPR article 9(2): (c), (d) |
| Data on service use and attendance | Monitored by Social Group Leader/ COO to ensure service is being used appropriately. | So new services can be offered if necessary | Friend benefits from appropriate service and follow up. | No | |
| Feedback relating to health/safety issues<br><br>*(sensitive data)* | Any safety issues raised communicated to key staff and volunteers. | Used to protect other Friends and staff, volunteers. Health issues: may be raised with referrer | Supports Friend and protects volunteers, other Friends, staff | Yes | GDPR article 9(2): (c), (d) |
| Data from impact and measurement tools | Statistical analysis. Monitoring benefit to individual. | To develop services | Friends | No | |

**Volunteers' Data (includes Trustees)**

Volunteers' data is held under the category of legitimate interest. It may sometimes include special category data. Data is held for two years following the last contact with the Volunteer. After that it is deleted from the database. A two year interval is considered appropriate since volunteers quite frequently resume volunteering or request references within that time.

| Data held | Processing | Why is processing of data necessary | Whose interest | Sensitive data? | Additional reasons, special category |
|---|---|---|---|---|---|
| Contact details | Provided to staff<br><br>Name provided to Friends in social group or as driver or Individual Support Volunteer | To contact volunteer | Volunteer's | No | |
| Application details (including references) | Provided to volunteer Manager | To assess suitability for Archway<br><br>As record during volunteer's service in case of changes/complaints | Volunteer's | Possibly | GDPR article 9(2): (a), (d) |
| Volunteer record: training attended, queries, complaints | Supplied to key staff (COO, Volunteer Manager, Volunteer Supervisor) | To offer the best volunteering experience To ensure volunteer is meeting Archway's needs | Volunteer<br><br>Friends | Not within meaning of GDPR | |

**Staff's Data**

Staff data is held under the category of contractual. It may sometimes include special category data. Data is held for 6 years following the last date of employment in the event of there being any investigations. After that it is deleted from the database and sharepoint.

| Data held | Processing | Why is processing of data necessary | Whose interest | Sensitive data? | Additional reasons, special category |
|---|---|---|---|---|---|
| Contact details | CEO or other staff members if required | Everyday procedures (especially with WFH) | Staff member, Archway | No | |
| Emergency contact details | CEO in emergency | For member of staff's protection | Staff member | No | |
| Any relevant health data, eg allergies | CEO and other staff as necessary | For member of staff's protection | Staff member | No | |
| Payroll details | Administrator, CEO, Treasurer | To ensure smooth running of payroll | Staff member | No | |
| Application details (including references) | Accessible to CEO only | In case of subsequent need eg tribunal, complaint, reference request | Staff member, CEO | Possibly | GDPR article 9(2): (a), (d) |
| Employment record: training attended, queries, complaints | CEO only | For career development (eg training opportunities), in case of need such as tribunal etc | Staff member, CEO | Not within meaning of GDPR | |

**Patrons' and Donors' data**

Patrons' data is held under the category of consent. Regular donors' data is held under the category of legitimate interest. Data is held for two years following the last donation or last contact with the patron. After that it is deleted from the database. One off donor data where the only evidence of the donation is a letter or email accompanying or giving information about the donation will be kept for 7 years as legally required by accounting regulations.

| Data held | Processing | Why is processing of data necessary | Whose interest | Sensitive data? | Comment |
|---|---|---|---|---|---|
| Contact details | CEO | For writing to donor or patron | Archway, donor, patron | No | |
| Bank details for direct debit/standing order donations | Administrator, CEO | For processing donations | Archway, donor | No | Only for donors |
| Record of donations | CEO | For contacts with donors | Archway | No | Only for donors |
| Record of communications with the donor | CEO | To develop relationships with donors, to thank them | Archway, donor | No | |