THE ARCHWAY FOUNDATION
DATA PROTECTION POLICY

Version Control			
Version	**Authoriser**	**Date**	**Amendment**
1. Board Approval	Board	Dec 23	
2. Amendment	CEO	28th Feb 2024	Any email attachment to external agencies will be password protected. If email attachments are only for internal use, then links to Lamplight or Sharepoint will be used as they offer a greater level of security.
3. Amendments for KAS Approval	KAS	28th April 2025	Following audit, additional guidance on (1) maintaining accurate records; (2) identifying and responding to individual rights requests; (3) how to respond to a personal data breach, including potential ICO notification; (4) what situations

			would require a DPIA; and (5) working from home. Change to retention period for Friend records from 2 years to 6 years to align with other charities in sector. Email encryption is also added as a method of protecting sensitive emails. Changed reference to Data Officer to Data Controller. Ensured that Friends can object directly to Data Controller rather than through a third party. Changed reference from GDPR Group to Keeping Archway Safe.
4.	KAS	11th September 2025	Removal of Appendix Data Held and reference to separate Privacy Notices made. Reference to DUAA added.

5.	KAS	Oct 2025	Added appendix on "soft opt-in"

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 unless the email is encrypted (emails between Archway staff are automatically encrypted). Any email attachment to external agencies will be password protected. If email attachments are only for internal use, then links to Lamplight or Sharepoint will be used as they offer a greater level of security.

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.

This guidance applies to home, remote and office working. For further guidance, see Appendix C.

4. Privacy Notice

Privacy notices will be provided to individuals under the following categories:

- Friends,
- Staff and Volunteers (including Trustees),
- Donors and Supporters.

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

The Data Protection Act 2018 and UK GDPR place a legal duty on controllers to secure the personal data they process. They also make it a legal requirement for personal data breaches to be reported to the ICO unless they are unlikely to result in a risk to individuals' rights and freedoms.

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.

Deciding on the severity of a personal data breach or an incident and whether it needs reporting

It is the responsibility of the controller to assess and decide whether a breach needs to be reported and to make the report where needed.

When should we report a breach?

If we decide a personal data breach or incident needs reporting, we will report it to the ICO via their reporting form without undue delay, or in any case, within 72 hours (3 days) of becoming “aware”.

We may require a brief period in which to investigate to establish with a reasonable amount of confidence that a personal data breach or incident has occurred. It is at this point we have become "aware" of the personal data breach or incident and our 72 hour period starts. The time of the personal data breach or incident being reported may be different from the actual time of the situation starting. Within that 72 hour window, we can choose when to report. For example, we might spend the first 48 hours investigating the situation and putting in place remedial actions and then report the personal data breach or incident via the ICO form.

Do we need to inform affected individuals about a personal data breach?

It is the responsibility of the controller to assess and decide whether individuals impacted need to be notified about a personal data breach.

Where there is a high risk to an individual’s rights and freedoms, we will contact those who are affected by the personal data breach.

However, unless compelled to do so by the ICO, we do not need to inform individuals of a personal data breach if:

1. Appropriate organisational or technical measures were in place at the time the personal data breach occurred, which made the data unusable or inaccessible. For example, the data or device was encrypted by our IT department before it was stolen.

2. We have taken measures to ensure that any high risk impacts on the individual user are now unlikely to happen. For example, we have corrected the data we hold that was maliciously altered during a cyber attack.

3. Disproportionate effort would be needed to inform individuals of the personal data breach. In which case, a public message on the website or in local newspapers alerting individuals to the personal data breach would suffice, provided there is enough detail to inform them about what has happened. An example of this might be where a personal data breach has occurred, but it is not possible (without disproportionate effort) to identify those affected, so a public message is sent out asking people to contact us if they think they have been affected.

4. Personal data is recovered (returned or securely destroyed) from a "trusted partner organisation." A trusted partner organisation could be the wrong department of our organisation. It could also be an organisation where we have an ongoing relationship, so we know their history and procedures. This could provide us with assurance that they will not read or access the data sent in error and comply with instructions to return it. Even if the data has been accessed, the controller could still possibly trust the recipient not to take any further action with it and to return the data to the controller promptly.

When informing an individual of a personal data breach, we will describe, in clear and plain English, the nature of the personal data breach and at least:

- the name and contact details of our data controller, or other contact point where more information can be obtained
- a description of the likely consequences of the personal data breach
- a description of the measures taken or proposed, to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects.

If possible, we will advise individuals on the steps they can take to protect themselves, and what we are willing to do to help them.

7. Changes to or new systems/processes (DPIA)

Personal Data must be protected, and the Data Protection Legislation requires data protection to be taken into account whenever a new system or process is introduced or where a system or process is changed that involves processing personal data.

Data Protection Impact Assessments (DPIA) must be completed and approved by the Data Protection Lead(s) for any significant changes to how personal data is processed that are likely to result in a high risk to individuals and where any new technologies or systems are used. A DPIA is required, in particular, if:

- installing a new CCTV system
- carrying out automated decision making
- carrying out a project involving large-scale processing of sensitive data

8. Performance Auditing

The Keeping Archway Safe 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

Data Use and Access Act 2025 (DUAA)

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: The Rights of Individuals and Subject Access Requests

Individuals have the following rights regarding data processing, and the data that is recorded about them:

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 Controller.

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.

Full, clear and accurate record keeping is vital to the delivery of safe and effective services. All staff and volunteers have a responsibility to keep full, clear and accurate records for everyone involved with Archway. This is to:

- safeguard continuity of support by providing information to colleagues involved in support;
- ensure Friends receive appropriate support that is in their best interests;
- meet legal requirements or respond to Freedom of Information or Subject Access Requests; and
- evidence your decision-making processes if later queried or investigated

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 Controller.

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 six 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 Controller.

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 Controller.

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.

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 can make an objection through their service coordinator or ask a representative to do so on their behalf. They can also make an objection directly to the Data Controller.

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.

Where a person makes any of the eight requests above, this is called a data Subject Access Request ('SAR'). SARs must be acknowledged promptly and the CEO notified at angelo@archwayfoundation.org.uk.

Archway will make available adequate notices to Friends explaining how the charity uses and processes their information.

A SAR must come from the individual themselves or a person acting on their behalf (also see section on young people). It must be accompanied by sufficient information to enable Archway to verify the identity of the individual and then locate their personal data.

We have one calendar month from the receipt of the request to respond unless the request is complex, and an extension is applied. We will keep a log of all requests, including those made by telephone or in person. We keep records of requests for 3 years from the date of the closure of the SAR, in line with the Records Management Code of Practice.

Confirming identification of the person who has submitted the request is important as it helps to stop organisations from inadvertently disclosing personal data, either accidentally or as the result of deliberate fraudulent action by a third party. Therefore, we must be satisfied that we

know the identity of the requestor before providing any information, including confirming whether or not we hold the information.

If the information provided by the individual in their request is insufficient to confirm their identity, we may need to request information such as:

- proof of identification - for example, driving licence, passport, birth/marriage certificate

- proof of authority - an agent (such as a solicitor) will need to prove they are acting on the person's behalf. For example, this may be through a letter of consent signed by the individual

Appendix B: Data Held

See Privacy Notices for the following:

- Friends
- Supporters, donors and patrons
- Staff and volunteers

These can be found on our website [The Archway Foundation | loneliness charity in Oxford | Oxfordshire, UK]

Appendix C: Soft Opt-In for Direct Electronic Marketing

In limited circumstances, Archway may rely on the "soft opt-in" exemption under Regulation 22(3) of the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR") to send direct electronic marketing communications (including email and SMS) to individuals.

This exemption is applied only where all of the following conditions are met:

- The individual's contact details were obtained in the course of a previous interaction in which the individual expressed an interest in, or engaged with, the organisation's charitable activities (for example, by making a donation, registering for an event, or requesting information).

- The communication relates to the organisation's own charitable purposes, campaigns, events, or fundraising activities, and is similar in nature to the individual's previous engagement.

- At the point of data collection, the individual was provided with a clear and transparent opportunity to refuse or opt out of receiving such communications.

- Each subsequent communication includes a simple and accessible mechanism enabling the individual to withdraw consent or opt out at any time.

The organisation applies the soft opt-in only where it is lawful, appropriate, and consistent with the individual's reasonable expectations. All processing of personal data for direct marketing purposes is carried out in accordance with the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018.

Individuals may opt out of receiving direct marketing communications at any time by using the unsubscribe facility provided in each message or by contacting the organisation directly.

Appendix D: Guidance on keeping safe and secure whilst working from home (from NHS Digital, 2025)

This guide will help you to keep safe and secure whilst working from home. It includes some simple security tips, both online and offline, that will help to ensure our work and data remains effective and secure.

Working remotely brings opportunities for more flexible ways of working, but it also brings new challenges, and one of them is cyber security.

Cyber criminals can exploit the weaknesses in our home and remote networks and encourage us to click links to bad websites that will put malware (malicious software) on our computers.

This means we all have a responsibility to adopt cyber safe remote working practices, and to continue to take the security of Archway data and systems seriously from wherever our place of work is.

Here are some simple security tips, both online and offline, that will help to ensure our work and data remains effective and secure:

Online tips

- be alert to phishing and vishing (telephone equivalent of phishing) scams. Threat actors are well aware that many people work remotely and it presents an opportunity for them to exploit. Seek advice from either the CEO or our Data Protection Trustee for further support if something does not feel right, be it an email, a phone call or a physical approach
- always keep personal information, such as log in details, to yourself
- work offline or connect by tethering to your mobile device, rather than using public Wi-Fi. Connect to Wi-Fi later, once at home on a more secure network
- be suspicious of any emails asking you to check or renew your passwords and login credentials. Try to verify the authenticity of the request through other means, such as calling our IT helpdesk at Wiseserve (Computer Assistance)
- check if emails look trustworthy before you click links or attachments. If it looks suspicious forward it immediately to the CEO and delete it
- change the admin/default password on your home broadband router

- ensure the firmware on your home broadband router is up-to-date
- make sure you are running all the latest versions of software on all your devices
- send links to sensitive documents from either Lamplight or Sharepoint that you send to other colleagues, rather than the attachment itself
- don't use your work email address to register on non-work-related websites
- be aware of fake text messages. Rather than follow the links, always refer back to a trusted website, such as GOV.UK

Offline tips

- always keep all your work devices with you when travelling (never leave work laptops or devices in cars)
- ensure nobody at home, even family members, accesses your devices for personal use, such as internet browsing
- reduce paper-handling to zero. Try not to print documents and work on them in public spaces. They will be vulnerable to theft or misplacement
- use a screen protector to prevent shoulder surfing if you are in public spaces or shared accommodation
- don't write passwords down
- keep your work telephone conversations discreet. Hold them in a private place, if possible
- never leave equipment unattended, anywhere. Lock your workstation when away from it at home. It's good behavioural practice and, if you live in shared accommodation, it's obligatory
- familiarise yourself with our incident reporting processes and report any incidents as soon as you're aware of them
- be cautious with sharing information about your work on social media sites, especially on your personal accounts