

# Alzheimer's Society Information Management Policy

---

Policy and procedure apply to:		Employees: All	Volunteers: All
		Contractors: All	Other: non defined
Version 2.0	Published 27 <sup>th</sup> June 2023	Average Read Time 4 minutes and 0 seconds	

## 1. What you need to know

Alzheimer's Society is committed to processing personal information safely and legally, and in line with individuals' rights. People will only unite with us to create a world without dementia if they see us as a professional organisation who can be trusted to collect, hold, use and manage information appropriately.

We expect all our people to understand and comply with our requirements under data protection legislation, whilst they undertake activities to achieve our charitable aims. We in turn commit to supporting our people to process information appropriately in their role with Alzheimer's Society.

We will do this by providing standards that enable you to manage information correctly. We will also signpost to other relevant procedures/guidelines for more in-depth advice and support. Furthermore, we will provide learning to help reinforce the information in this policy.

Whilst this policy refers to personal information, the standards listed are relevant to all information and must be followed when processing any information, personal or otherwise.

## 2. How we work here

This policy captures the approach to information management that our people must follow. Read the Information Management Standard for full details and advice on putting this into practice.

### We expect you to:

- Read, understand and follow the information management standards outlined in this policy and attached Standard.
- Ask for help if you are not sure how to manage information appropriately.

### Managers:

- Must ensure they are aware of the standards their people should follow. They are responsible for ensuring their people are aware of how they should manage information.

### Suppliers and Contractors:

- Must adhere to the data protection terms and conditions set out in their Society contract, which will be based on our information management policy and standards.

### General information management standards:

It is a legal requirement that, unless an exemption applies, personal information shall be:

- processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary
- accurate and, where necessary, kept up to date
- 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
- processed in a manner that ensures appropriate security of the personal data using appropriate technical or organisational measures
- processed in line with individuals' rights concerning the use of their information

The Society must be able to demonstrate compliance with these principles.

The Society also has a legal obligation to ensure it follows the principles of data protection by design and by default. This means actively ensuring that we consider data protection issues and individuals privacy rights as part of the design and implementation of systems, services, products and business practices and at every stage of the information lifecycle. This cannot be undertaken as a one-off activity, or as an add-on at the end of a project.

It is expected that all processing of information conducted by Alzheimer's Society, or those acting on our behalf, will comply with these principles. If these principles, this policy or connected relevant standards, procedures and guidance cannot be followed, the risk created must be signed off by a senior member of staff (Head of Department as a minimum), recorded in a Risk Action Plan and the Information Governance team made aware.

Where information is lost, mishandled or put at risk, the [Information Governance Incident Reporting Procedure](#) must be followed.

### The Information Lifecycle

To comply with the data protection principles, all personal information must be processed lawfully and securely at all points in its lifecycle. Full details are in the Information Management Standard.

#### Planning:

- Before processing information, make sure you are aware of how the information should be used and managed at all stages of its lifecycle. You should make sure that information is not being processed where there is no legal or legitimate need for it to be processed, and you may need to complete a Data Privacy Impact Assessment. This is explained throughout the rest of this policy and in the guidance.

#### Collecting information:

- Information must only be collected where there is a clear lawful basis to do so. If there is no lawful justification, information should not be collected. When you are collecting personal information, you must ensure that at the point of collection individuals are given information on how the Society will use and manage their information (a Privacy Notice).

**Moving information:**

- Once collected, information should be captured or moved so that it is stored in the relevant corporate information system. You must move information securely, whether the information is being transferred internally to members of the Society or to external partners.

**Storing information:**

- You should store information in a safe, appropriate environment. Appropriate access controls, such as password protection, must be in place to ensure access to information is limited to those who need to know the information.

**Use of information:**

- An individual must be informed at the point their information is collected how we will use their information. Information should not be used for purposes that have not been explained, are not compatible with the reason the information was initially collected for, or for purposes the individual would not expect the information to be used.

**Sharing information:**

- Sharing of information, internally or externally, should only happen where there is a 'need to know' the information. If information does not need to be shared, then it should not be.

**Review and disposal of information:**

- Information can only be kept (retained) for as long as the Society still lawfully needs it for the purpose the information was originally obtained.

### 3. What to do if things go wrong

Compliance with data protection is a legal requirement. Failure to meet our legal obligations could have significant financial and reputational consequences, diverting money and attention from people affected by dementia. We expect all our people to comply with this policy and the associated standards, procedures and guidelines. Deliberate failure to comply will be addressed through the Disciplinary Policy or Volunteer Resolving Concerns Guidance.

### 4. Further information

If you have any questions, contact your line or role manager in the first instance. This policy provides an overview of the requirements for our people and then signposts to other documents for further information:

- Read the Information Management Standard for more information on putting this policy into action, additional explanation on the Information Lifecycle and a glossary of terms.
- For more details on how we manage information as an organisation, refer to the Information Governance Framework.

### 5. Supporting documents

Information Management Standard	Information Governance Framework
Incident Reporting Procedure	Procedure for responding to GDPR rights requests
Procurement Policy	Information Security Policy

## 6. Definitions

Definition	Example
<b>Processing</b>	
Any activity in relation to the personal information, such as: collection, recording, storing, organising, amending, retrieval, use, disclosure, analysis, aggregating, erasure or destruction	<ul style="list-style-type: none"> <li>• Receiving a referral from the NHS</li> <li>• Collecting marketing preferences</li> <li>• Inputting a new starter's details into People+</li> <li>• Sharing research findings</li> <li>• Holding information e.g., gift aid declarations</li> <li>• Deleting old records</li> <li>• Publishing a carer story / photo on social media</li> </ul>
<b>Personal information or Personal data</b>	
Any recorded information relating to an identified or identifiable living person.  An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, or to one or more factors specific to that person	<ul style="list-style-type: none"> <li>• Name</li> <li>• Contact details</li> <li>• CRS P00 Number/Supporter PV Key/Payroll No</li> <li>• Supporter's bank details / donation record</li> <li>• Case Study / Photos / videos of individuals</li> <li>• Social Media handle</li> <li>• Notes of telephone conversations</li> <li>• IP address</li> <li>• Biometric data such as fingerprints or DNA</li> </ul>
<b>Data Subject (living individual)</b>	
Individual who is the subject of personal information	<ul style="list-style-type: none"> <li>• A service user</li> <li>• A supporter</li> <li>• You as a volunteer / employee / contractor</li> </ul>
<b>Data Protection Impact Assessment (DPIA)</b>	
A Data Protection Impact Assessment is a process which helps an organisation to identify and reduce the privacy risks that a project/activity poses to individuals. A DPIA is mandatory where the processing of personal data is likely to be high-risk	Activities which would require a DPIA: <ul style="list-style-type: none"> <li>• Fundraising activity which includes profiling</li> <li>• Outsourcing of DBS checks</li> <li>• Brand new, and significant and high-risk changes to existing, Operations services</li> <li>• New computer database</li> </ul>

Data Protection Legislation referenced in this Policy includes the UK General Data Protection Regulation (UK GDPR) as implemented by the Data Protection Act 2018, the Isle of Man Data Protection Act 2018 and Data Protection (Bailiwick of Guernsey) Law 2017.

### Document details

<b>Author/Owner:</b>	Simon Brumfit, Data Protection Officer
<b>Sponsor:</b>	Robert Butler, Director of Finance and Corporate Resources
<b>Next review:</b>	June 2024
<b>First version published</b>	11/01/2017

