Alzheimer's Society Information Management Standard

Standard applies to:		Employees: All	Volunteers: All
		Contractors: All	Other: non defined
Version 1.0	Published 28th June 2023	Average Read Time 38 minutes	

Introduction

This document must be read alongside the Information Management Policy, which explains the approach we expect our people to follow with managing data appropriately. This Standard document then gives further information on how to follow the policy in practice.

If this Standard isn't met, it should be reported as an information governance incident. We can all make mistakes, and it's important we know when this Standard isn't met. The Information Governance team keep a log of information incidents to record what steps we've taken to reduce any harm, and to reduce the chance of it happening again.

If someone **deliberately** doesn't follow the Standard for managing information, the Society Disciplinary policy or Volunteer Resolving Concerns guidance may be used.

Roles and Responsibilities

This Standard is relevant to:

- **Volunteers, Trustees and Employees:** Volunteers, Trustees and Employees must follow the requirements stated in this Standard. You are responsible for managing information as described in this standard. If you have any questions, ask your manager.
- **Process Owners:** Owners of local (Directorate / Department /Team level) processes involving information must ensure that the processes required for managing that information in line with the Information Management Policy and Information Management Standard are defined and communicated to all relevant colleagues / volunteers.
- **All Managers**: must ensure they are aware of the standards their team should follow. They are responsible for ensuring all their people (volunteers and employees) know how to classify and handle information correctly and consistently. If you have any questions, ask the Information Governance team (information.governance@alzheimers.org.uk).
- **Suppliers:** must adhere to the information governance terms and conditions set out in the contracts issued by the Society, which should be based on the requirements in this Standard.
- **Information Governance team:** responsible for the Information Management Standard.
- **Head of Compliance & Risk:** responsible for ensuring this Standard reflects current data protection requirements and (through the Information Governance team) providing further advice to teams where needed.

Putting the policy into practice

The Society has a legal obligation to ensure it follows the principle of data protection by design and by default. This means actively ensuring that people's privacy, rights and information are appropriately protected. This cannot be undertaken as a one-off activity, or as an add-on at the end of a project. The Society must make sure it is thought about before and during the processing of information.

To comply with the data protection principles in the Policy, all personal information must be processed lawfully and securely at all points in its lifecycle – see diagram for the stages.

The remainder of the Standard explains the data protection requirements when handling information and at each point of the lifecycle (some requirements span more than one stage) and signposts to other relevant procedures and guidance for more information and advice on how to meet the requirements.

Index

1. Handling Information

Policy: Before you begin processing information, make sure you are aware of how it should be handled in a way that ensures appropriate security of the personal data using appropriate technical or organisational measures

This section of the Standard explains what measures are needed to handle information securely for different types of information – this depends on the level of confidentiality, and how much harm could happen if that information is lost. Harm could include a fine to the Society for not taking care of information about people, or damage to the Society's reputation with the public and other organisations as a trusted organisation.

Where the Society collects, stores and uses information, including personal data, appropriate safeguards must be in place to keep that information safe. These help to ensure confidentiality for service users, supporters, volunteers, employees, and for sensitive Society information. These safeguards are needed to meet Society, legal and contractual requirements.

1.1 Levels of information: classifying depending on confidentiality & risk

The Society uses three information classification levels, and these are based on the information's value to the Society or to individuals if it's personal information.

Each classification level has a standard for how it's used and protected, depending on the nature of the information and the risk if it was seen by the wrong person. By using classification levels, you're clearly telling anyone who sees the information how carefully they need look after it.

The classification levels affect how anyone should store, access, share and dispose of information. Always think about what classification information is before using it.

- **Public** – Information we've designed for the public, or have to make available to the public

  No risk at all for this information being made public. That's what it's meant for.

  For example: leaflets, our public website, press releases, our charity annual report, leaflets, official Society posts on social media.

- **Official** – Organisation and team information, procedures and policies that are useful for all or groups of staff and volunteers to access and are mainly intended for internal use. Other information that is used to help the Society achieve our strategic ambitions and may be shared externally, as long as it does not contain confidential information about people.

  Low risk to the Society or individuals if this sort of information was made public.

  Stop & **Check** before **Sharing** Official information outside the Society

  For example: Arena or Yammer content, our organisation's Policies and Procedures, Emails which do not contain Official-Sensitive information, signed contracts, statistical reports about service users and supporters, limited colleague information such as name, role title and work contact details.*

*Some Policies may be fine to share externally if it is necessary, others may contain sensitive information that should not be shared in that level of detail, so check with the policy owner if you are not sure. For example, the Information Management Policy can be shared as is with NHS Commissioners where the Society is bidding to deliver dementia support services to their area, but the Information Management Standard contains confidential information about security standards and should not be shared externally – check with the Information Governance team for any summary information for use in these circumstances.

- Official-Sensitive – More confidential information that could damage the Society, individuals or other organisations if it was made available to people or organisations that should not have it. This could be personal information about one or more people, or business information that is commercially sensitive. Information about service users and supporters from which they can be identified is likely to always be Official-Sensitive.

  Stop & Check before Sharing Official-Sensitive information inside or outside the Society

  Medium to High risk to the Society or individuals, depending on the information involved, if this type of information was made public or shared with the wrong recipients.

  For example: personal information about service users, supporters and donors, details about colleagues or volunteers beyond role and work contact information, commercial tenders in progress, draft research reports, planned restructures, IT security measures, budget planning, accident reports.

The classification of information may change over time – for example draft new factsheets may be Official and only intended for internal use initially, but when they are finalised and approved for release, they will change to Public.

1.2 Levels of information: how to work with each classification level

- Information level: Public

  Access and sharing – can be publicly available. No need to lock away printed copies.

  Email – can be sent with no extra protection.

  Post – can be sent in standard post.

  Disposal – digital copies can be deleted. Printed copies can go to recycling (or general waste for non-recyclable materials).

- For Information levels Official and Official-Sensitive see the table below for how to handle that information depending upon your activity and classification level:

	OFFICIAL (default level)	OFFICIAL – SENSITIVE
General		
Marking the classification	**Documents - Must** mark the classification in the header or footer of each page. **Emails** - will soon have the functionality to choose a classification label of Public, Official, Official-Sensitive. *Look out for communications about when this change is implemented.*	
Photocopying / Printing	Dispose of unwanted copies securely.	Do not print or copy documents unless absolutely necessary. Use secure print functionality if available. Documents must not be left unattended, and all copies / printing must immediately be collected from the machine.
Transmission by spoken word (including phone calls and voicemail)	Make sure you cannot be overheard by anyone who should not know the information. This includes when working from home - ensure family, flatmates, visitors, children (old enough to understand / potentially repeat the information discussed) cannot overhear conversations. Do not discuss in public areas.	
		When leaving voicemail messages, don't mention any sensitive information. When leaving messages on landlines, don't mention the reason for the call as others with access to the home may hear the message and be unaware of a dementia diagnosis.
Storing		
Electronic record storage location	Store in relevant corporate information system (for example CRS, Progress, People+). Where this is not possible, store in a network folder with restricted access or password-protected file using authorised software (e.g., Sharepoint). Before storing information outside of AS servers, consult with Information Security to ensure appropriate security measures are in place.	
Physical storage of paper records	Take reasonable precautions to restrict access – clear away when leaving unattended or no longer in use.	Store in an approved locked container / cupboard / room; restrict access to authorised people only. Lock away when leaving unattended or no longer in use.
Electronic equipment holding information – temporary storage	Only temporarily store, and transport, personal information on Society authorised devices if there is an agreed business reason to do so. Use Society-authorised encrypted equipment (USB stick, external hard drive) if temporarily storing electronic personal information outside the internal network for the purpose of transferring it to an authorised Society location. Don't leave device unattended; store in similar ways to paper records when not in use.	

<table>
<tr><th colspan="3">Moving / transferring / sharing</th></tr>
<tr><td rowspan="2">Email transfer</td><td colspan="2">Ensure the correct recipient is selected (check Outlook has not auto populated with an incorrect recipient or a personal, not work, email address of a Society colleague).

Only send to an external organisation(s) if there is a genuine business need.

If sending information to multiple recipients who don't know each other and do not need to know each other, use bcc functionality.</td></tr>
<tr><td></td><td>If emailing to a non-Society email address, you must use either:

• Email encryption* - the secure email facility within Outlook (For more information on this, and how to use this facility, please see the Society's Email Security Guidance Microsoft Defender - Best Practices for Users and the How do I open a protected message? Outlook (Microsoft.com)

Or if you experience problems using email encryption, report them to IT ServiceDesk with as much detail as possible including error messages seen by the sender or recipient, and in the meantime use:

• Password Protection - Attach Official-Sensitive information as a password-protected file and the password sent through a different method (for example: SMS, phone call).

If the external recipient cannot open the email / attachments when using encryption or password protection and information still needs to be sent you may use OneDrive for secure data transfer – see Information Security team advice in the link.

*When using Email encryption, follow these tips:

- When in the message that you want to send, select the Options menu within Outlook, then Encrypt, and then select Encrypt Only from the drop-down menu that appears.
- Using this encryption option will also encrypt any attachments to the email.
- Microsoft encryption works with any external email address regardless of provider. For example, with Gmail and Yahoo addresses not just with Outlook address.</td></tr>
<tr><td>Electronic file transfer</td><td colspan="2">Managed centrally, consult Information Security for guidance.</td></tr>
</table>

Moving paper records in person	Place information in an envelope/container, which is not left unattended.	Information must be transported in a bag which can and must be locked and is not left unattended. If transporting large amounts of information, use a Hotbox (contact Facilities).
Postal transfer	Care should be taken that address details are accurate and legible. Provide return address in case of non-delivery. Post information in line with standards stated in activity/process guidelines, if there are guidelines in place.	
		Mark as "Private & Confidential". Where there are no local guidelines on how information should be posted, consider sending by at least Royal Mail 'Signed For' recorded delivery, if the loss of the information would be highly impactful to individuals or to the Society.
Disposal / Deletion / Destruction		
Disposal of paper records	Cross shred (using DIN 3 minimum level shredder) or place in Confidential waste bag/bin. Record in accordance with timeframes stated in the **Retention and Disposal Schedule.** **Ensure you update your region's/directorate's paper records inventory to show when they were destroyed and who by.** If outsourcing to another organisation, ensure a destruction certificate is received / kept.	
Deletion of electronic records	Delete file or record in accordance with the **Retention and Disposal schedule** timescales. When deleting emails, they must be 'double deleted' (in inbox and 'deleted' folder) If you have a recycle bin on your desktop, make sure this is regularly emptied. Delete from encrypted USB memory stick or portable media as soon as transferred into electronic storage area. Return Society issued IT equipment for secure disposal when no longer required.	
Destruction of hard copy electronic records (CDs, disks)	If your office has a contract with Shredding Alliance, then these can be placed directly in the confidential waste bin. If your office does not have a contract with Shredding Alliance for secure information disposal, seek advice from Facilities.	

1.3 Why is Handling Information important?

The classification levels affect how anyone should store, access, share and dispose of information. This helps us meet our legal responsibilities under Data Protection law for secure handling of people's information including colleagues, volunteers, supporters and service users. It also helps us protect other confidential or otherwise sensitive information like tenders, bids, partnerships and finances.

If we don't protect information appropriately, we're at risk of exposing information we shouldn't share. And that could lead to embarrassment, reputational damage, risk to people's privacy including data protection law breaches, as well as fines and other commercial harm.

2. Lawful processing

Policy: Personal information shall be processed lawfully.

This section of the Standard explains the different ways in which personal information can be processed in a lawful way, whether that is at the collecting, using, sharing, storing or other stage of the information lifecycle.

2.1 Lawful processing of personal information – what is an acceptable 'legal basis'?

There are 6 different legal bases under Data Protection law which organisations can rely upon to process personal information and you need to be able to meet at least one of them for your proposed use of information that you intend to collect, use, share, store etc.

Consent: the individual has given clear and valid consent for the Society to collect and use (and share if relevant) their information for a stated purpose (either directly consented to the Society or may have consented to another party such as a GP referring a service user). E.g.,

- Referrals from another organisation into Society services for people affected by dementia
- Information about someone who can give an employment reference for a job applicant
- Marketing consent from an event participant for email marketing
- Referrals by the Society to an external organisation such as Social Services for safeguarding purposes
- Individual requesting copy of information to be sent to a solicitor

To ensure consent is valid, follow the requirements in the **Consent** section of this Standard.

Contract: the collection, use (and sharing if relevant) is **necessary** for a contract the Society has with the individual, or because they have asked us to take specific steps before entering into a contract with them. E.g.,

- Purchasing an item from the Society's Online shop and their information being processed so they can pay for the item and have it delivered
- Where people can enter an event via the Society's allocation of places, rather than direct with the event organiser, our contract / terms with them require us to pass their information to the event company so they can undertake the challenge
- Job applicants giving their information so that an Occupational Health pre-employment assessment can be completed

Legal obligation: the collection, use (and sharing if relevant) is **necessary** for the Society to comply with the law (not including contractual requirements)

- Consultations around workforce planning
- Health & Safety mandatory reporting
- Some safeguarding reporting requirements

Vital interests: the use and sharing if relevant is **necessary** to protect someone's life. The threat must be significant and imminent.

- Providing medical personnel with supporter / service user information in the case of a medical emergency

Legitimate interests: the collection, use (and sharing if relevant) is **necessary** for the Society's legitimate interests or the legitimate interests of someone else, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

- Providing corporate partners with updates on their organisation's fundraising at an individual employee feedback level, so they can match it, with employees having been told that these updates will be given.
- Using people's information to send them marketing / promotional communications or materials in the post
- Using designated contacts' contact information to communicate with them about a referral
- Using peoples' information for analysis and reporting purposes

Public interest: the collection, use (and sharing if relevant) is **necessary** for the Society to perform a task that is in the public interest or being undertaken by the Society on behalf of a Data Controller with official authority (such as a Public Health body).

- Sharing information with a care home during the pandemic about which Society colleagues that would be visiting had received the Covid vaccination

If the information being collected and used is special category personal information (such as health, ethnicity etc.), we will need to ensure a further condition is met. Contact the Information Governance team at information.governance@alzheimers.org.uk for advice.

If we want to share non-personal information, there is no specific legal basis we should meet. However, we should still make sure there is a legitimate business need for the sharing and that what we are sharing is not subject to any confidentiality.

3. Consent

Policy: Personal information shall be processed lawfully.

This section of the Standard explains what makes consent a valid lawful way to use someone's personal data. The **Lawful processing** section of the Standard sets out the different ways in which personal information can be processed in a lawful way and consent is one way. Where the Society uses consent from individuals to collect, use, share their information for a particular reason, there are various criteria that must be met to make the consent valid.

3.1 What do we mean by consent?

Consent is permission for something to happen or agreement to do something. It is more than informing people that something will happen if they don't object.

Consent is mainly used:

- where the use of someone's personal information by the Society for a particular purpose is voluntary; or
- the type of personal information about them is more sensitive (such as health or ethnic origin) and so we need their agreement to use their information for that purpose.

Examples of when the Society should seek the consent of an individual include:

- To use their health information to provide a service
- To record their story and/or image for use in marketing activities
- To send the individual marketing messages electronically

3.2 Why is consent important?

Data Protection law requires organisations to make sure that whenever they use personal information about an individual, the purpose it will be used for is legally allowed. For some activities, getting consent from the person whose information we want to use is the best way to make sure the Society is allowed to go ahead with using their information for that activity.

Where we use consent as the legal reason to use personal information, we need 'valid consent' from the individual, otherwise we can't lawfully use the information for the reason we collected it. If we use someone's personal information for an activity without valid consent (when consent is needed), the Society might have to stop undertaking that activity and could be subject to monetary fines from the data protection regulator.

3.3 What does consent need to be valid?

Consent is valid if it is:

- **Freely given:** the decision to consent must be made by the person themselves*, not influenced by pressure from others. Consent for a specific purpose can't be made a condition of something else. For example, consent to receive fundraising marketing can't be a condition of someone receiving a support service.
- **Informed:** the person must be given information about what the activity involves, and how their information will be used. This also includes what will happen if they don't consent to the activity, so they can make a fully informed decision.

- **Able to be easily withdrawn:** the person must be made aware they can withdraw their consent at any time, and how they can do this. Withdrawing consent must be as easy as giving consent.
- **Specific:** the scope of the use of their information must be made clear to the individual.
- **Unambiguous:** the person must clearly indicate they are giving permission or are happy for something to happen such as signing a form or clicking a submit button online.

We must also be able to **demonstrate** that consent was given. If we can't show that someone consented, and exactly what they agreed to and when, we will be unable to justify our future actions later on. Our use of their personal information for this purpose may then not be lawful.

***Who can give consent** - Valid consent can be obtained from a Legal proxy - someone who the individual has given a Lasting Power of Attorney to, or the court has awarded a Deputyship to (over the person's Health & Welfare or Property & Financial affairs). For example, an Attorney or Deputy for an individual in relation to their health and welfare could give consent for the Society to process that person's health information to deliver a group service to them.

NOTE: If there is no Attorney or Deputy, another individual can't give a GDPR compliant consent for the Society to process someone's personal information, but there may be another lawful way apart from consent that the Society can use – please check your local procedures for further guidance in the first instance, and then contact the Information Governance team if more information is required.

Seeking and recording consent: Consent doesn't always have to be given in writing, we can get consent in other ways, such as verbally. So, we can demonstrate that non-written consent was given, we need to make a written or electronic record. This should include when the consent was given, how, and what we told the individual that the personal information would be used for. This record of consent should be made as soon as possible afterwards.

Reviewing consent: Where consent is gained, it should be reviewed at appropriate intervals to ensure it's still valid for the activities it covers - that the individual is still happy for the activity to happen. This may require you to refresh consent from individuals and this should be included in team procedures. For example, consent for service user stories to be used for marketing or training purposes expires after a certain number of years and consent must be re-obtained for the story to continue to be used.

The information Governance team have produced a Consent Checklist to help you consider whether your proposed consent approach is valid - Save a copy to your local drive to fill it in.

3.4 Other considerations when seeking consent

3.4.1 Mental capacity considerations

For consent to be valid, the person must have capacity to give that consent. Some people are able to communicate a decision (e.g., indicate they agree to something) despite lacking capacity to make that decision. Our people must therefore consider capacity whenever dealing with consent. You should refer to the Mental Capacity Act Policy and Mental Capacity Act Procedure for further information.

3.4.2 What else might personal information collected be used for?

When an individual consents to their information being used, it will be for a specific purpose. If the Society wants to use that information for other reasons, the individual has a legal right to be informed. The Collecting Information section of this Standard sets out what we must tell individuals when we obtain their information.

Where you know a future use of that information will also need consent, consider whether to ask for that additional consent up front or at the time you need it. If the former, ensure the individual understands the separate uses of information they are agreeing to.

3.4.3 What if consent is not given?

If someone lacks capacity to consent, a 'best interests' decision should be made by the most relevant person. You should refer to the Mental Capacity Act Procedure for details. If someone has capacity but refuses to consent to their personal information being used for a particular purpose, this usually means you shouldn't use their information to undertake the activity.

If you still need to process information about the individual without their consent, you may be legally allowed to do so in some circumstances e.g., if the processing is necessary to fulfil safeguarding obligations (see the Society's Safeguarding policies and procedures). Contact the Information Governance team for advice if needed.

3.4.4 Individuals rights once consent has been given

Individuals have the right to withdraw consent, and further use of their information must then be stopped (e.g., a note put on their record to indicate consent has been withdrawn to process their health information in relation to a particular service, their Story / images / video or audio recording no longer used for promotional purposes). We may still have other legal reasons to keep some of their information in our records for a reasonable retention period.

4. Planning

Policy:

Before you begin 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.

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.

This section of the Standard explains what steps you must take when planning to undertake a new activity, or making changes to an existing activity that will alter how information is processed.

You must complete the Data Protection Impact Assessment (DPIA) Screening Questionnaire to see if a full Data Protection Impact Assessment (DPIA) questionnaire is required. It is a legal requirement that a DPIA is conducted on all high-risk activities. For further information about DPIA's see the information governance pages on Arena.

Even if a DPIA is not required, the Society is obliged to ensure privacy risks and people's rights are considered and built into our systems and processes. You should contact the Information Governance team for advice in this planning stage to ensure information is being processed lawfully and in an effective way – contacting the team early in the planning process will also help them plan and prioritise resource if necessary to assist you.

If you are contracting another organisation to process information on the Society's behalf, you must follow the Procurement Policy so that appropriate due diligence is undertaken, especially in relation to the management of personal information. As part of this process, the Procurement team will engage with the Information Governance team to make sure data protection requirements and risks can be considered.

5. Collecting information

Policy: Information must only be collected and used in ways that we are legally allowed to. 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).

This section of the Standard explains **what** we need to let people know about how we will use information collected about them (usually in a 'privacy notice'), **when** we have to provide the relevant privacy notice, and **who** we have to provide it to (as there can be some circumstances where a privacy notice does not have to provided). The Standard also gives examples of the different valid legal reasons for collecting and using personal information.

This includes the immediate purpose it is being collected for and any future purposes it may be used for. This will ensure personal data is processed lawfully, fairly and in a transparent manner. This is particularly important where consent is required to process personal information, as without this step being taken, the consent will not be valid. This will normally be done by linking to one of the Society's existing privacy notices.

Individuals have a right to be provided with information about how their personal information will be used. It is important to be transparent both to meet the legal requirement and to promote the trust and respect between us and our stakeholders.

5.1 Are we legally allowed to collect and use the information for our intended purpose(s)?

Any personal information that we collect or is provided to us by others (people or organisations) can only be collected and then used for purposes that are allowed by privacy laws.

You need to establish that you are allowed to collect and use the information for your planned purpose / activity. See the **Lawful processing** section of this Standard for more details, and for examples of valid lawful conditions that apply to the use of personal information.

Once you have established that the Society is legally allowed to collect and use the personal information for the planned purpose(s), the right of people to be informed about how organisations use their personal information needs to be considered – see the following section:

5.2 Why do we need to tell people how we are using their information?

- People have a legal right under data protection laws and regulation to be informed how organisations will use their personal information.
- People can only make informed choices about whether to provide their information when they understand how it will be used – such as whether to engage with us or not.

5.3 What Privacy Information do we need to tell people?

The table below summarises what information we must, by law, tell people whose personal information we collect and use. This is usually provided within something called a 'Privacy Notice' or Privacy Statement.

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer	✓	✓
Purpose of the processing and the lawful basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable (where we are relying on legitimate interests)	✓	✓
Categories of personal data (e.g., contact, health, financial)		✓
Any recipient or categories of recipients of the personal data (e.g., event organisors, social services, medical assessors)	✓	✓
Details of transfers to other countries and safeguards	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of each of data subject's rights (right of access, erasure, correction, objection)	✓	✓
The right to withdraw consent at any time, where relied upon	✓	✓
The right to lodge a complaint with the Privacy regulator	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences	✓	✓

5.4 When do we need to give people the privacy notice information?

- Directly obtained - If we are collecting personal information directly from an individual, the Privacy notice should be provided either just before they give us their information or at the point that they do so.

- Indirectly obtained - If the personal information is obtained from someone other than the individual the information is about (i.e., from a GP as part of a referral or from another organisation as part of a fundraising event) the privacy notice should be provided within a reasonable period which must not exceed one month from when the data was obtained, and at the latest during the first communication with the individual.

  For example, if we receive a referral from a Memory Clinic, we must tell the person being referred by no later than one month but if we make contact with that individual on day 14 after receiving the referral, we must provide the privacy notice at that point and not wait until a month has passed.

  Similarly, if we buy a marketing list from another organisation for a postal mailing campaign, we must tell the people on the list how we will use their information either within a month of obtaining their data or when we send them the postal mailing if that is in less than the one-month timescale.

- If it is intended that personal information should be disclosed to another organisation, the privacy information must be provided before this happens.

5.5 Who needs to be given the privacy notice information?

Most people whose personal information we collect, and use, have the right to be informed how the Society will use their information and therefore must be given a privacy notice.

This includes the groups below who each have their own version of a Privacy Notice:

- Supporters
- Service users
- Employees
- Volunteers
- Website users

Exemptions

In cases where information we collect is limited, and the purpose we use it for has very little impact on the person, there may be an exemption from providing them with an individual privacy notice.

However, to rely on an exemption a Data Protection Impact Assessment (DPIA) needs to be completed and reviewed by the Information Governance team, and a suitable Privacy Notice published on the Society's external website.

Exemptions have been agreed for:

- Designated Contacts, Relationships and Emergency Contacts for Service Users
- People using Facebook Donate
- Prospects being researched

If you are unsure whether or not your category of people need to have a privacy notice and your local procedures / guidelines and Line Manager cannot answer the question, you should contact the Information Governance team for advice via information.governance@alzheimers.org.uk

5.6 What format does the privacy notice need to be in?

Privacy notice information can be provided online, in a paper format (such as a leaflet), electronically such as via an attachment or link in an email, or verbally (in cases where the privacy notice or statement is small).

Which format is best may depend on how you collect the information – for example:

- if someone asks to join a group service you could email them a copy of the leaflet or a link to it if you collect their email address or post them a leaflet.
- If someone calls the Supporter Service line to request information / resources, they may be read the short Privacy Statement
- if someone completed an online webform (for example to register for an event), it is recommended that a 'layered approach' is taken to providing the fair processing information. Before they submit information to us, it should be briefly explained to them what the information will be used for and a hyperlink to the full privacy notice provided so they can read the full notice if they wish to. An example of a layered privacy notice for a fundraising activity is as below:

  Registration Page

  Fill in your details below to register. We will use your information to send you a fundraising pack and communicate to you fundraising ideas to help you raise money. For more information about how we will use your information – including how we ensure it is managed and used properly and your rights in relation to how your information is used – please see our Supporter Privacy Notice

  If you require help constructing your layered privacy notice statement, please contact the Information Governance team for assistance.

5.7 Which Privacy Notice should be provided?

The Society engages with several different groups of stakeholders and collects and uses different information about them for different purposes. There is no one single privacy notice which explains how the Society uses the information of all its stakeholders. Instead, there are some privacy notices which relate to different groups of stakeholders or specific activities.

Supporter Privacy Notice
Service User Privacy Notice
Employee Privacy Notice
Volunteer Privacy Notice
Website user Privacy Notice

These notices should contain the information we are legally required to provide to people about how the Society uses their personal information. They are available on the Society's external website (via the Legal information link at the bottom of the website homepage) but the relevant notice must still be provided at the point of data collection (with the exception of the notice for Society website users).

Some areas may have other existing Privacy Notices / Statements for certain groups / activities, that have already been reviewed and approved by the Information Governance team. For example, there are marketing consent statements for all teams that send marketing materials to supporters or collect supporter information, and a Privacy Notice for external e-learning participants.

5.8 What to do if an existing privacy notice does not cover how your activity will be using information

There may be occasions, especially for new or specialised activities, where our existing privacy notices do not cover an activity.

If this is the case, first consider if the privacy notice can be updated to cover your activity. This is particularly important if you will be using information within one of our main databases such as CRS, Progress or People+. When telling people about how their information will be used, we need to make sure we cover all purposes the information will be used for. Having multiple privacy notices relating to different activities creates a risk the notices will not accurately or completely describe all the purposes the personal information could be used for.

If it's not appropriate to update an existing privacy notice, you will need to create your own to provide to people before their information is collected. A template to help with this and ensure all necessary information is provided is included in **Appendix A** at the end of the Standard.

If you want an existing privacy notice amended, or want to create your own specific one, you should contact the Information Governance team for advice and assistance in these activities.

5.9 Privacy Notices where Alzheimer's Society is a data processor

It is the responsibility of a data controller to provide information to individuals about how their personal information will be used. For some of our commissioned services though, we are not the data controller but the data processor, collecting and processing information on behalf of the commissioning body.

In these circumstances we should help the data controller meet their legal responsibilities through providing service users with the required information about how their personal information will be used. It needs to be clear to the service users though that the Society is not acting as the data controller for this service, but the commissioning body is.

You should contact the Information Governance team for advice and assistance in these activities.

5.10 Marketing Privacy statements

If you are collecting information to use for electronic marketing purposes, as well as complying with data protection legislation, the processing must also be compliant with Privacy and Electronic Communications Regulations 2003 (PECR).

Marketing does not cover just the selling or provision of goods or services, but all promotion or advertising an organisation does. This includes promoting the aims or ideals of a charity. Any fundraising, campaigning or general promotion of the aims and values of the Society sent electronically to individuals must comply with PECR.

Teams responsible for capturing people's personal information for marketing purposes, who use Progress currently to record those people must follow the Marketing consent guidance. This includes using the prescribed wording in the Marketing Statements to ensure that the information collected can be used for our standard range of marketing purposes with those individuals. These teams must also ensure that the recorded marketing preferences are screened against for future marketing communications.

For teams who intend to send electronic marketing / promotional communications outside of these existing processes (such as one-off email campaigns to individual GPs about the Society's services) must also comply with the PECR requirements and must contact the Information Governance team for advice.

6. Moving information

Policy: 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.

Information should be captured or moved so that it is stored in the relevant corporate information system (e.g., CRS, Progress, People+) or in a corporately available location (e.g., J Drive team folder or Public folder).

This may require you to move information from the location or format it was collected in, into an electronic format (e.g., paper form scanned into CRS, email saved to directorate folder in the J Drive, Great Conversations notes written initially in a notebook and then typed up and uploaded into People+).

You should move information as soon as possible into the correct storage place for that information so it is available to those who need to see it. Once it has been moved, you should strongly consider whether the original copy of the information still needs to be kept. This is because keeping duplicate copies of information can cause confusion and problems, as explained in Section 5. Where it is not needed, you should dispose of the original copy securely (see Section 8).

You must move information securely, whether the information is being transferred internally to members of the Society or to external partners. The standards relating to movement of information within the **Handling Information** section of this Standard must be followed. In order to identify the correct requirements in the Handling Information section you may need to first identify the suitable classification level for the information if this has not already been done.

7. Storing information

Policy: 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.

Guidance on safe storage provided within the **Handling Information** section of the Standard must be followed.

Keeping duplicate copies of the same information should be avoided, as this can lead to:

- Confusion as to which is the main copy,
- Vital changes being missed and the most up to date version of information not being used, especially when held across different formats (i.e., in paper and electronic form),
- Difficulty in finding relevant information when it is needed,
- Some versions of the information not being dealt with properly if rights requests are received, e.g., may not be deleted if they make an erasure request, and
- Increase to storage costs as more records are being kept.

If you plan to store information outside of the Society's IT network, information security due diligence must be completed as part of the Procurement Policy.

When storing electronic information on the Society's network drives, you should follow any published guidance on Arena.

Detailed guidance on paper records can be found in paper record archiving procedure.

8. Using information

Policy: 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.

For example, people expect us to use the information collected as part of a recruitment exercise to make a decision as to their suitability for a role. They do not expect us to use their information for fundraising purposes.

The Society's standard Privacy Notices for certain groups of people (such as supporter, service user, employee, volunteer etc.) should be checked to see if the proposed use of their personal information is already covered.

If not, Data Protection legislation provides some exemptions to this requirement in limited circumstances (for example, for crime prevention/investigation purposes, research, legal purposes). The Information Governance team should be consulted to confirm whether the activity would be covered by an exemption, or whether the activity cannot occur without notifying the data subject.

If there is not an exemption that could be relied upon you may need a bespoke Privacy Notice to be created for the new processing purpose and you must contact the Information Governance team to discuss this – see also the **Collecting Information** section of this Standard, sub-section 5.8.

Before using information for marketing purposes, the Marketing consent guidance must be consulted and followed to ensure compliance with data protection legislation and, where wishing to market via electronic communication channels, PECR.

9. Sharing information

Policy: Sharing of information, either 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.

This Standard explains the Information Sharing Principles to be followed to ensure the minimum necessary information is shared safely and lawfully, along with a flow-map and more detailed information to support decision-making about what information to share, when and with whom – **See Appendix B** at the end of the Standard. The Standard also sets out when Data Sharing Agreements (DSA) should be considered.

There is a separate procedure for responding to GDPR Rights Requests – see **Rights** section of this Standard.

9.1 Information Sharing Principles

When you are making a decision about what information to share with another person or organisation there are some key elements that you must consider. The Information Governance Team has created the following information sharing principles to help colleagues make good decisions about sharing information:

- You must have a **valid reason** to share it AND the recipient must have a **need to know** it
- If the purpose can be achieved with **anonymised** information - do that
- Consider whether you have a **legal basis** to share – do you need Consent before sharing (usually the case for us to share health data externally but there are some exceptions such as Safeguarding referrals)
- If personal information needs to be shared, **minimise** the amount to what's relevant & necessary
- Usually, the person should have **been informed** that their information will be shared for this purpose (either in the full Privacy Notice or in a separate way)

9.2 Who will you share the information with and why do they need it?

It is important that we only share information with those who have a legitimate right and/or need to see it. You need to be happy that the person/organisation you intend to share the information with is who they say they are (if they are requesting the information).

To determine this, consider:

- do you know the requestor and are confident this is them?
- if it is the individual the information is about, have they provided any proof of identity?
- if the requestor is a representative of the individual, do they have a letter of authority or a Lasting Power of Attorney allowing them to represent the individual?
- is there someone you can check with at the organisation if the requestor is not familiar to you?
- does the request come from an official email address linked to the organisation (i.e., not a hotmail or gmail account)?
- was the request on letter-headed notepaper or an official request form? Are the contact details given, correct?

It is important to establish why the person/organisation needs-to- know the information (whether they are requesting it from us, or we are proactively decided to share it with them) Understanding their need can help us to decide whether we are legally allowed to share the information with them and also what information is necessary to share with them.

We should not be providing third parties with information just because they ask for it or because of who they are if they are in a position of authority - information should only be provided for clear and necessary purposes. If an organisation has been unclear as to why they want or need the information, do not be afraid to ask.

9.3 Does 'personal' information need to be shared?

Think about what the information you are considering sharing is needed for. Is personal information needed to answer the question, or could it be anonymised/ depersonalised? For example, if a commissioner needed to know how many attendees there were at a Singing for the Brain session, we could provide the number of attendees rather than the names of the individuals who attended.

9.4 Are we legally allowed to disclose the information?

Unless an exemption applies, information must be disclosed in a way that privacy laws allow. Even if there is a contract between the Society and another organisation, we cannot share personal information with them if no relevant legal basis can be found which allows the sharing.

For examples of valid lawful ways to share the information, see the Lawful processing section of this Standard.

9.5 Selecting / minimising information to share

Personal information should be restricted to only as much as is absolutely necessary for the purpose.

When considering what part of the information we hold to share, ask these questions:

- Does the requestor need to know all of the information they have asked for or is there a reduced amount of data we can share with them to meet their purpose?
- If we are proactively planning to share information, consider what is the minimum amount of information we need to share about an individual to achieve our purpose for sharing?
- Is there any duty of confidentiality attached to the information that might restrict how much we share?

9.6 Informing the individuals' whose information will be shared

Individuals have a right to be informed about how their information will be used and this includes when it will be shared with others including external organisations.

When considering sharing information, particularly with external organisation, ask yourself these questions:

- Does the individual the information relates to know about the request?
- If you are relying on consent to make the sharing lawful, has the individual agreed for this information to be disclosed?

- If they are not aware, and you think there are reasons why they should not be informed and your local procedures don't cover this, please contact the information governance team for advice

9.7 Recording the disclosure

If disclosure of personal information is required, particularly externally, a record of what you need to share, with whom and why should be recorded.

When making a record consider the following:

- If you have **received** a request for information you need to keep a record of the request and your decision – even if you have decided not to share information.
- If you have a business need to **proactively share** information, particularly externally, make a record of what you need to share, with whom and why.
- Ensure that the record of the disclosure is located in the most suitable place depending on what is being disclosed to whom and why e.g., we're making a referral for service user to another organisation, this would be recorded on CRS. If you're sharing an event's participant data with an external event organiser this will be recorded on Progress.

If you are not sure where to record the request, speak to your Line Manage and if advice is still required contact the Information Governance team.

9.8 Disclosing information safely

When disclosing information, it should be shared safely and securely. The right level of security will be determined by the classification of the information which takes into account the nature of the information and the risk of it falling into the wrong hands. – see the **Handling Information** section of this Standard.

When disclosing information, make sure you consider the following:

- The classification of the information you are disclosing – if you are not sure what the classification is, refer to the **Handling Information** section of this Standard.
- Once you have established the classification, follow the transfer guidance given to ensure information is shared safely.

9.9 Data Sharing Agreements (DSAs)

Data Sharing Agreements (DSAs) can sometimes be referred to as Data Sharing Protocols or Information Sharing Agreements. These are not contracts but are documents that detail the agreed sharing of information between organisations and the common rules concerning it.

They are not legally binding contracts and as such are not legally enforceable. However, they can be helpful in supporting a relationship between multiple organisations where information needs to be shared, e.g., when participating in an integrated care pathway.

If you will be entering into an arrangement where personal information will be regularly shared between organisations, particularly where the organisations don't already have a contract

between them all, it may be appropriate to consider a Data Sharing Agreement. In some cases, in Ops a commissioner or local authority might request a DSA or ISA are entered into by the Society.

You can find more information in the Data Sharing Agreement Guidelines.

Information should be transferred in a safe way by following the advice given in the **Handling information** section in this Standard.

10. Review and disposal of information

Policy: Information can only be kept (retained) as long as there is a lawful basis to hold that information.

The retention periods for different types of information are detailed in the Records Retention and Disposal Schedule. This must be followed by all Society volunteers and employees and, if information is being held outside of the Society, by our data processors.

Information should be disposed of in line with the guidance detailed within the **Handling Information** section of this Standard and any other published procedures / local arrangements.

Personal information may also have to be disposed of in response to a valid request from the individual or their legal representative. For further guidance there is a GDPR rights requests Procedure – find out more in the **Rights** section of this Standard.

11. Individuals Rights

Policy: Individuals have a number of legal rights concerning the use of their information. We must make sure that whenever designing or procuring new information systems, or processing information in a new way, these rights are met.

Under GDPR, individuals have a number of rights concerning the use of their information. The Society must make sure whenever designing or procuring new information systems, or processing information in a new way, these rights can be met if a relevant request is received.

These rights are to:

- be informed of how their information will be used
- have inaccurate information rectified
- have (in certain circumstances) their information erased
- object to the processing of their information, particularly in relation to direct marketing and for research and statistical purposes
- request the restriction of the processing of their information
- access information held about them
- have their information provided in a portable format
- know if they are subject to decisions made by automated means (i.e., by a computer alone with no human input)

You should be aware that you may receive a request from an individual relating to these rights. If you do, consult the GDPR rights requests Procedure for advice on next steps to take. It is important that you do this and undertake the stated required action promptly as a number of type types of requests must be completed within a statutory timeframe.

Supporting documents

Information Management Policy
Consent Checklist
Data Sharing Agreement Guidelines
Paper record archiving procedure
Mental Capacity Act Policy
Information governance incident webpage
GDPR rights requests Procedure
Records Retention and Disposal Schedule
Marketing consent guidance
Mental Capacity Act Procedure

Definitions

Some of our terms explained:

Definition	Example
Processed / Processing / Using	
Any activity in relation to the personal information, such as: collection, recording, storing, organising, amending, retrieval, use, disclosure, analysis, aggregating, erasure or destruction	• Receiving a referral from the NHS • Collecting marketing preferences • Inputting a new starter's details into People+ • Sharing research findings • Holding information e.g., gift aid declarations • Deleting old records • Publishing a carer story / photo on social media
Personal information or Personal data	
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	• Name • Contact details • CRS P00 Number/Supporter PV Key/Payroll No • Supporter's bank details / donation record • Case Study / Photos / videos of individuals • Social Media handle • Notes of telephone conversations • IP address • Biometric data such as fingerprints or DNA
Data Controller	
The organisation which, alone or jointly with others, determines the purposes and means of the processing of personal information	Alzheimer's Society is the data controller for most personal information used by Society people. The NHS/Local authority could be for some commissioned services. The Society will be the controller for dementia connect services
Data Subject	
Individual who is the subject of personal information	• A service user • A supporter • You as a volunteer / employee
Privacy Information	
Information which must be provided to the individual in order to enable us to lawfully use their personal information	• Your Personal data Consent forms

Document details

Author/Owner:	Lisa Moore, Information Governance Manager
Next review:	June 2025
First version published	28th June 2023 (previously various documents)

Appendix A: Privacy Notice Template

The template has three parts to it:

Part A

An introduction to the notice and its purpose.
Please use the standard text. The examples of personal information can be altered.

Part B

This contains information about the activity and how the information will be used. It should cover:

- How and why the information is used (including what your legal basis is)
- If information will be shared, with who and why
- How information will be stored and how long it will be retained for.

Be specific about how and why information will be used in your activity.

Part C

This contains the general information which must be provided to all individuals, whatever their relationship with us, concerning how they can apply their rights in relation to their personal information.
Please use the standard text.

Even if the fair processing information is not presented within a single notice, all three parts of the template must be covered in some way.

[Part A] What is personal data?

Your personal data is information that identifies you, such as your date of birth or your address. It can also be information that reveals something about you, for example your contact details. Depending on your relationship with us, we may also hold health information, donation details or other relevant data.

However, you are connected with us, we will respect your privacy and your rights.

[Part B] How and why we use your information

[*Provide specific information on how and why the personal information will be used and reference the legal basis. Here are suggested headers to help you cover all necessary points.]*

- How and why, we use your information
- Sharing your information
- Storing your information
- Where is your information held?

[Part C] How we support your privacy rights

Security and confidentiality

We take care to make sure your information is secure when we use, store, and transmit it. It

is only accessed by people who have been verified and authorised to do so. Every one of us who has access to your personal information is obliged to respect that it is confidential, and we deliver training to make sure this happens.

Your consent

If we are using your data on the basis of your agreement then at any time, you can withdraw your consent and we will stop using it.

Further rights

Please contact us at any time you want to:

- See what information we hold on you
- Request a portable copy of your information
- Ask for corrections to be made
- Ask us to stop using your information in any

way. We'll do our best to respect your wishes.

How to contact us

If you have any questions about how we are using your information, please contact us:

- By phone to Customer Care on 0330 333 0804
- In writing to Customer Care, Alzheimer's Society, XXX
- By email to enquiries@alzheimers.org.uk

You can also use the online form for general enquiries on our website alzheimers.org.uk

For a copy of your personal information, to ask us to correct the information we hold about you or to stop using your information, please contact the Information Governance team:

- In writing to Alzheimer's Society, XXX
- By email to information.governance@alzheimers.org.uk

Complaints

If you are unhappy with how we are processing your information, please contact us using the details outlined above. If you are still unhappy after receiving our response, you can raise your concern with the Information Commissioner's Office.

[*Service Delivery only:* Please note that if you are using our services, and that support is commissioned by a public organisation, then your complaint may also be made available to them so that they can address your complaint and our response. Where this applies, you may also complain directly to the commissioning body.]

Appendix B: Flowchart of considerations to undertake when disclosing Information