

Access to Personal Records

1. Background

This policy has been developed to provide clear guidance about responding to requests from individuals, or someone acting on their behalf, for access to personal data held about them.

2. Objectives

The aim of this policy is to ensure that individuals, and their authorised representatives, where appropriate, have access to the records held about them by ATD in accordance with the UK General Data Protection Regulations 2018 ("UK GDPR"), the Data Protection Act (2018), the Data (Use and Access) Act 2025, and good practice.

3. Scope

This policy applies to all established staff, agency staff and volunteers. It applies to all requests for access to personal data held by ATD, including data about residents, service users, employees, volunteers and donors.

The rights to access under UK GDPR extend only to living individuals. Requests for the records of deceased residents of Nursing Homes may be made under the Access to Health Records Act 1990 (AHRA).

If you have received a request for personal data, please refer to section 4.1.

If you are responding to a request for personal data in accordance with instructions from the Data Protection Officer (DPO) or appointed person, please refer to section 4.3. ATD's appointed person is the Business Support Manager.

This policy applies to Abbeyfield the Dales Limited and its corporate trustee responsibilities for registered providers Charles Edward Sugden Almshouses, and Frank Crossley's Almshouses, also for the non-registered provider The Pawson Cottage Homes, and its subsidiary Abbeyfield Court Limited.

4. Policy

All written and verbal requests for access to personal data (a "Subject Access Request (SAR)") should be forwarded to the DPO or appointed person, without delay.

The DPO or appointed person will log and acknowledge receipt and obtain all necessary supporting documentation and information with assistance from relevant members of staff. They will then take steps to ensure that the request is dealt with within 1 calendar month that is required by UK GDPR.

Section 4.3 onwards set out full details of the procedure to be followed where a SAR has been made.

4.1. Who can make a Subject Access Request?

Access to personal data will normally be given only to the data subject themselves. Any individual about whom ATD holds personal data has the right of access to that information, including residents, service users, employees, volunteers and donors.

An individual is not entitled to know what is recorded about another individual without that individual's consent.

Individuals who wish to do so can apply for access to their personal records through an agent or representative, for example a solicitor.

4.1.1. Proof of Identity

If there are doubts about the identity of the person making the request you can ask for identification that clearly shows the name, date of birth, and current address only of the requestor. For example, passport or photo identification such as a driver's license, national identification number card, or birth or adoption certificate.

Where ATD reasonably requires proof of identity or clarification of the request, the response period will commence once that information has been received.

4.1.2. Requests made on behalf of someone lacking mental capacity

Where an adult lacks capacity within the meaning of the Mental Capacity Act 2005 and has legal capacity i.e. she or he understands the nature of the request, she or he can request access. The UK GDPR makes no special provisions about requests made on behalf of an adult who lacks mental capacity and is incapable of managing their affairs. If a person lacks capacity to manage their affairs, a person acting under a Court of Protection Order, within the terms of a registered Enduring Power of Attorney or as attorneys appointed under a registered Lasting Power of Attorney can request access on their behalf.

4.1.3. Requests through an agent

If a person has capacity and has appointed an agent, that person can make a valid request for access on behalf of the data subject. Agents should provide evidence of their authority and confirm their own identity and relationship to the individual. If satisfied that the data subject has authorised the agent to make the request, the request must be treated as if it had been made by the data subject. This also applies where a person is acting under Power of Attorney.

A person who is profoundly physically disabled may not be able to give written consent for an agent to apply for access on their behalf. Where a person is unable to give written consent, staff should give the individual as much help as possible and will need to make a judgement on whether the individual has given consent for an agent to act on their behalf.

4.1.4. Requests for access to the records of a deceased person

The UK GDPR applies only to information about people who are alive. Personal data about someone who has died should still be kept confidential but may, at the discretion of the DPO or appointed person be disclosed to others who have a sufficient interest or need to know about the matters recorded. The reasons for wishing to have access should be given in writing.

If a deceased resident was living in a nursing home, where records are prepared on behalf of a registered nurse their records are disclosable under the Access to Health Records Act 1990 ("the AHRA") and may be requested by their personal representative(s). A sealed copy of the grant of probate or Letters of Administration should be requested to verify the authority of personal representatives making such a request.

4.2. What information is available for access?

For information held by ATD, personal data essentially means any recorded information held from which a living individual can be identified. It will include a variety of information including names, addresses, telephone numbers, photographs of people and other personal details.

The information may be held electronically on computer, or in hard copy/paper-based filing systems including files, microfiches, card indexes, day books etc. It may include letters, reports, records of direct contact and telephone calls, records of meetings and case conferences and any audio or visual recordings made, for example, telephone and CCTV recordings.

This information may also be held in various different locations, including head office, divisional offices, care homes and houses.

4.2.1. Exemptions

Providing access to and disclosure of certain kinds of personal information held by ATD may be exempt from the provisions of the UK GDPR. The following are examples of where a decision to not disclose may be appropriate:

4.2.1.1. Risk of Serious Harm

Access to personal data relating to an individual's physical or mental health may be refused if granting subject access would be likely to cause serious harm to the physical or mental health of the individual or someone else.

Staff should bear in mind that the fundamental principle is that individuals have the right to see what is recorded about them, and it is for this reason that this exemption is limited to serious harm. Withholding information on this ground is therefore likely to be exceptional and only so much of the information as is likely to cause serious harm or enable the identity of another to be disclosed or deduced should be withheld.

4.2.1.2. Third-Party Information

Information supplied by a third party (e.g. social services, healthcare professionals), or about someone other than the individual concerned, is termed third party information and should not be disclosed without first seeking consent to its disclosure from the relevant third party.

4.2.1.3. Legal Professional Privilege

Personal information is exempt from access if a claim for legal professional privilege could be maintained in legal proceedings. Any legal advice obtained about a data subject should be held in the confidential section of the individual's records.

4.2.1.4. Other

Examples of other exceptions include but are not limited to:

- Management forecasting/planning exemptions
- Negotiations with the data subject
- Crime and taxation exemptions
- Regulatory investigations
- Confidential references.

4.3. Responding to a Subject Access Request

4.3.1. Step 1

When a written or verbal request is received from an individual or their representative, staff should not attempt to deal with it themselves, but should forward it to the DPO or appointed person urgently. A SAR does not need to be given that title, or even contain those words to be valid, nor does a reason need to be given for the request.

If a request is made verbally, the requestor name and contact details should be obtained and sent the DPO or appointed person. A request sent by email or fax is as valid as one sent in hard copy. Requests may also be validly made by means of social media.

Where the person making the request is disabled we may need to make reasonable adjustments, which may include, but is not limited to, responding in braille, large print or audio format.

4.3.2. Step 2

The DPO or appointed person will log the request and write to acknowledge receipt of it. They will also request additional information as may be required to enable ATD to deal with the request. This includes verifying the identity of the data subject and/or their representative and clarifying the request.

In most cases you cannot charge a fee to comply with a SAR. However, where the request is manifestly unfounded or excessive, or further copies of data are requested, you may charge a "reasonable fee" for the administrative costs of complying with the request.

4.3.3. Step 3

On the day of receipt (whether the day after is a working day or not) of all necessary information and supporting documentation (Proof of ID) the 1 calendar month time limit for dealing with the request will start. The timeframe is from the day after you receive the request until the corresponding calendar date in the next month.

The DPO or appointed person will check all available sources of information, determine which staff members should deal with the SAR and collate the data from all sources. If no documentation can be found, the DPO or appointed person will write to the requester advising them of this fact.

In responding to a Subject Access Request, ATD will undertake searches that are reasonable and proportionate having regard to:

- the nature of the request;
- the systems in which personal data is likely to be held;
- the importance of the information requested;
- the resources required to locate the information.

ATD will be able to demonstrate and document the searches undertaken and the reasons why any further searches would be disproportionate.

4.3.4. Establishing the identity of the applicant or their agent

Where the staff member directly involved in arranging access to the records requested does not know the applicant or their agent, proof of identity must be obtained before any personal information is revealed. A birth certificate, passport, driving licence or other clear proof of identity should be checked (either the original or a certified copy) and a copy will be kept on file.

Where an individual will not be present when their agent is being provided with access, they should be advised in advance that their agent will need to produce proof of identity.

If the applicant or their agent fails to provide evidence confirming their identity, then the DPO or appointed person will write to inform them that their request cannot proceed until this is provided.

4.4. Preparing records for access

Having established with the applicant the exact nature of the information being sought, and whether they simply wish access to the record or want a copy of the information, the staff member will need to assemble the appropriate records (from all locations) and ensure that the content is in order. This will involve ensuring that the contents of the record(s) have been checked so that only appropriate information is accessible.

In addition to a copy of personal data, a requestor may also be entitled to know the category of the information, including whether the information is being processed and for what purpose.

Personal information held on an individual's records may include details of another person. If disclosure would allow them to be identified, the DPO or appointed person should make reasonable efforts to obtain the other person's consent before any disclosure is made. The

DPO or appointed person may decide that it is reasonable in all the circumstances to disclose without obtaining such consent or choose to anonymise the record.

To decide what is reasonable – the following factors may be considered:

- Any duty of confidentiality owed to the third party;
- Any steps taken to seek their consent;
- Whether the third party is capable of giving consent;
- Whether consent has been expressly refused;
- Any legal prohibition; and/or
- Whether the applicant is already aware of the identity of the third party and their involvement in the matter.

Sometimes it will be clear that the information can be given without the third party's consent, e.g. where the applicant has given the information about the third party in the first place.

As referred to at paragraph 4.7(b), where information has been supplied by a third party (e.g. social services, healthcare professionals), or about someone other than the individual concerned, is termed third party information and should not be disclosed without first seeking consent to its disclosure from the relevant third party.

When "editing" information so as to not reveal another person's identity or to prevent it being deduced, only the minimum amount of alteration for this purpose should be made e.g. "Mrs Smith reported to us..." should be amended to "X reported to us." Where this kind of editing is required, extreme care should be taken to ensure the original entry cannot still be recognised. This can be achieved by using a black marker and then photocopying the page again.

As far as possible the personal information revealed to the data subject should be that contained in their record at the time the request for access was received. Routine amendments as outlined above are acceptable but the information must not be tampered with to make it more acceptable to the individual. If any comments in the records may be of a nature that could cause concern, it may be worth identifying this to the requestor and provide an explanation or something to lessen the effect it may have on them.

Where a staff member is unclear about whether information should be revealed or withheld, advice should be sought from the DPO or appointed person.

4.5. Access and viewing of records

Having established from the applicant the nature of the information they seek the designated staff member will have ensured that the records are prepared in the following way by:

- Removing material where exemptions apply; and
- Removing names of, and information given by, third parties.

When all the available material has been checked, if a copy is being provided this should be sent to the address given with a covering letter. If access to the actual case file and content is being provided, or if it is felt that actual disclosure needs to be face to face, a date and venue should be arranged with the applicant (or their representative) within the required timescale (see Section 4.2.1 – Step 3 above). The venue should be a suitable one having regard to any special needs the applicant may have.

The staff member should note any claims of inaccuracies in the records and explain how these will be dealt with (see paragraph 4.2.5 below).

A staff member should be present at all times when access is taking place and ensure that the record is not removed or tampered with in any way. Under no circumstances should the individual (or their representative) have unmonitored access to original records.

Where possible, information will be provided electronically using a secure method unless the individual requests otherwise. Where electronic disclosure is not appropriate, information will be provided in paper format or by another accessible method agreed with the individual.

4.6. Taking copies

Under the UK GDPR, individuals are entitled to a hard copy of their records. If viewing only, or if the content is deemed to require face to face contact, for instance if it is likely to be distressing or require explanation, the records should be made available at an ATD property unless another suitable and appropriate alternative is necessary. Photocopying facilities need to be available to supply copies of the record if subsequently requested by the applicant.

4.7. Correction and erasure

If an individual considers that any personal information held on their record is inaccurate (see below) they may request for it both written and verbally, for it to be corrected or erased.

Inaccurate means incorrect or misleading about any matter of fact. An opinion which does not purport to be a statement of fact cannot be challenged on the grounds of inaccuracy. Inaccurate personal information can be erased or corrected whether received from the individual or from a third party. If ATD does not agree to the request to correct or erase any personal information a note should be included on the record that there is not agreement on this matter. Where a staff member is unclear about whether information should be corrected or erased, guidance should be sought from the DPO or appointed person.

4.8. Recording that access has taken place

The designated staff member should ensure that at the end of the access session(s) a written statement, to go on the record, is prepared and agreed with the individual about what has been decided and any further/future actions. A copy should be sent to the DPO or appointed person.

4.9. Access by other organisations

Occasionally requests will be received from external organisation such as Court Welfare officers and other professionals for access to an individual's records. This may be for assessment purposes, or by organisations such as the Police and Department for Works and Pensions as part of an investigation into a criminal offence.

It is important that anyone receiving such a request should contact the DPO or appointed person for advice before making any response to these types of requests.

4.10. Complaints

Individuals who are dissatisfied with the handling of a Subject Access Request may submit a complaint to the Data Protection Officer.

Complaints will be acknowledged within 30 days and investigated without undue delay.

Individuals will be informed of the outcome and their right to complain to the Information Commissioner's Office (ICO) if they remain dissatisfied. A link to ICO guidance is below:

<https://ico.org.uk/for-the-public/getting-copies-of-your-information-subject-access-request/what-to-do-if-you-dont-get-a-response-or-youre-unhappy-with-it/>

4.11. Subject Access Request Register

The DPO/Appointed person will record details of all requests including:

- Date of request and deadline.
- Requestor details & proof of identity where applicable.
- Systems searched and colleagues involved in the gathering of information.
- Outcome and response date.
- Communication and event log.

5. Finance, Value for Money & Social Value

N/A

6. Supported Appendices

Appendix 1: Subject Access Request (SAR) Process Flow

7. Linked Policies

Data Protection (LG013P)

Mental Capacity Act (C015P)

CCTV (LG005P)

8. Legislation/Regulation

UK General Data Protection Regulations (UK GDPR)

Access to Health Records Act 1990

The Data Use and Access Act 2025 (DUAA)

9. Review

Every 3 years, subject to regulatory and legislative changes.

10. Procedure/Guidance

Further guidance on Subject Access Requests can be found on the Information Commissioner's Office (ICO) website at <https://www.ico.org.uk>

Appendix 1: Subject Access Request (SAR) Process Flow

Appendix 1

Subject Access Request (SAR) Process Flow

