Subject Access Requests Policy

Policy Number: 02-02

Version Number: 04

Document Owner: Quality

Signed off by: Ozcan Yaren – Data Protection Lead

Date last reviewed:	22/04/2025	
Due date for next review:	22/04/2028	
Policy consultation with:	SMT	
Legal Requirements:	UK General Data Protection Regulation (UK GDPR) Data Protection Act 2018 Health and Social Care Act 2008	
CQC:		
Other:		
Related Policies:	Data Protection Policy and Procedure	Newlon Group CCTV and Surveillance Policy
	Records Management Policy	Newlon Group IT and Email Policy
	Retention and Disposal Policy and Procedure	
Scope: This procedure will be applied irrespective of the race, gender, marital status, disability, sexuality, religious belief or age of the employee concerned. This policy covers all employees including sessional staff and volunteers. All Outward employees, paid or unpaid, are expected to comply fully with this policy and related procedures. Data protection is referred to in the Staff Code of Conduct and breaching this policy could lead to action under Outward's Disciplinary Procedure		
Policy Equality Impact Assessed		

Version number	Amendments	Reviewed by	Date
04	No significant change	OY - EL	22/04/2025

This information can be made available in alternative formats, such as easy read or large print. Please contact 0208 980 7101 or email info@outward.org.uk.

1. Purpose

1.1 To provide staff with guidance on how to recognise and act upon receipt of a subject access request.

2. Definitions

2.1 Subject Access Request: under the Data Protection Act 2018, Individuals have the right to access and receive a copy of their personal data, and other supplementary information. This right is commonly referred to as 'Subject Access Request (SAR)'. Individuals also have the right to be:

- Told whether any personal data is being processed
- Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people
- Given a copy of the personal data and
- Given details of the source of the data (where this is available).

2.2 Personal Data: any form of information relating to a living person from which they could be identified. This includes any comments or opinions about the person.

2.3 Data Subject: the person whom the personal data is about. This is not always the person making the request. For example, a solicitor might make a request on behalf of their client, a person we support. The data subject would be the person we support.

2.4 Data Protection Lead: Quality Manager as the data protection lead is responsible for processing and responding to subject access requests. They can be contacted by emailing Dataprotection@outward.org.uk.

3. Procedures

3.1 Recognising a Request

If a member of staff is contacted by any person (this could be a person we support) or someone acting on their behalf (such as a relative, friend, solicitor, advocate or a legal guardian) asking verbally or in writing, including on social media for access to most or all of their personal data held by or processed by Outward, this is a subject access request.

Even if the person whom the data is about (the data subject) does not refer specifically to a 'subject access request', staff must be able to recognise this immediately and refer to the responsible officer. A verbal request may present like the examples below:

- "Can you tell me what information is in my file?"
- "I want to see what you hold on me."
- "I'd like to know what personal details of mine you have saved."

Giving out routine information to people we support and tenants, such as repairs information, is part of our normal service delivery. It does not qualify as a subject access request under this procedure.

3.2 Receiving a Request

If a request is received from a data subject (the person whom the data is about) or their representative, either verbally, via letter or an email, the member of staff who receives the request must ensure that the request is forwarded to the Data Protection Lead immediately by scanning and/or forwarding it to Dataprotection@outward.org.uk.

3.3 Receiving a Request for Children

Prior to addressing a SAR concerning information pertaining to a child, staff should assess whether the child possesses the maturity to comprehend their rights. If the request originates from a child and there is a reasonable certainty in their ability to grasp their rights, the response typically should be directed towards the child directly. However, in cases where the child grants authorisation, or if it is apparent that it serves the child's best interests, the parent or guardian may be permitted to exercise the child's rights on their behalf. In instances where the child demonstrates competence, they retain the option to empower an individual other than a parent or guardian to initiate a SAR on their behalf.

3.4 Completing a Request

The Data Protection Lead will send a subject access request to all relevant staff. Anyone receiving the form is expected to carry out a full search of all their electronic and paper files for information relating to the data subject and/or their property, and to provide this information to the deadline set by the Data Protection Lead. Where necessary, this could include a search of archived information.

It is important that information is provided fully and in its original format. There may be occasions where potentially sensitive or confidential correspondence or documents appear in the search results.

Any and all information must be provided to the Data Protection Lead, who may redact or remove sensitive or confidential information using the relevant exemptions of the GDPR. Staff must not alter, erase, destroy or conceal any information with the intention of preventing its disclosure.

Subject access provides a right for data subject to see their own personal data, rather than a right to see copies of documents that contain their personal data. Often the easiest way to provide the relevant information is to supply copies of original documents, but we are not obliged to do this. Information and completed forms should be emailed to Dataprotection@outward.org.uk.

3.5 Verifying a Request

The Data Protection Lead will verify the request, and in case of any queries, they may contact the concerned staff member who received the request or consult other staff members who have interacted with the data subject previously. It is crucial that when an individual claims to represent a person we support or a tenant, we must obtain evidence demonstrating their legal authority to act on behalf of that individual for information requests. Ensuring familiarity with the requester's identity (or the person on whose behalf the request is made) is essential. If there is uncertainty, additional information can be requested to authenticate the individual's identity. The countdown for responding to a SAR initiates once the requested information is received, yet it's advisable to promptly solicit identification documents.

3.6 Responding to a Request

The Data Protection Lead will respond to the data subject or their representative to acknowledge receipt of the request and to confirm when they should expect to receive the requested information.

By law we are required to provide the requested information within 30 calendar days. It is therefore important that requests are referred to the Data Protection Lead as soon as possible.

Upon assembling the requested data, the Data Protection Lead will securely deliver it to the data subject or their representative. Even though, compliance with a SAR must be achieved promptly and no later than one month from the request's receipt, if complexity or a high volume of requests exists, an extension of two months is permissible.

Whether a request is complex depends upon the specific circumstances of each case. Examples of factors which may, in some circumstances, add to the complexity of a request. It is required to be able to demonstrate why the request is complex:

- Technical difficulties in retrieving the information – for example if data is electronically archived.
- Applying an exemption that involves large volumes of particularly sensitive information.
- Clarifying potential issues around disclosing information about a child to a legal guardian.
- Any specialist work involved in obtaining the information or communicating it in an intelligible form.
- Clarifying potential confidentiality issues around the disclosure of sensitive medical information to an authorised third party.
- Needing to obtain specialist legal advice.
- Requests that involve a large volume of information may add to the complexity of a request. However, a request is not complex solely because the individual requests a large amount of information.

When an extension has been deemed necessary the Data Protection Lead will let the data subject or their representative know within one month of receiving their request and explain why an extension has been applied.

For cases involving substantial data volume, requesting clarification from the individual regarding the specific information or processing activities can pause the response time. This pause continues until clarification is received, nevertheless any available supplementary information should still be provided within one month.

3.7 Refusal or Failure to Respond to a Request

The General Data Protection Regulations gives individuals the right to see a copy of the information Outward holds about them, and for it to be provided within 30 calendar days, although exemptions may allow refusal of all or part of a SAR based on circumstances. Outward can decline all or part of a SAR with a clear explanation of the reasons for refusal or failure to respond to a request includes their right to complain to ICO or another supervisory authority, and the option to seek legal enforcement if;

- The SAR is manifestly unfounded and/or excessive requests
- The request involves disclosing information about others, and it is not possible to fulfil the request without their consent
- By the Data Protection Act 2018, categories include crime, taxation, legal privilege, public protection, regulatory functions, journalism, research, health, education, and more.

On the other hand, failure to respond to a legitimate request is a breach of the GDPR and can incur a penalty fine as well as it may also be a breach of Outward's Data Protection Policy and Procedure and could lead to action under the Disciplinary Procedure

3.8 Appeal Procedure

If the data subject is not satisfied with the information provided in response to their request, they must put their concerns in writing to Data Protection, Outward, 4 Daneland Walk, London, N17 9FE or email to Dataprotection@outward.org.uk. Additionally, they retain the option to file a complaint with the ICO or another supervisory authority.

4. General Data Protection Regulations Statement

Outward is committed to compliance with the General Data Protection Regulations and the Data Protection Act 2018. It requires all staff and partners to respect confidentiality and data subjects' rights in line with its policies and procedures.

To ensure compliance with the Regulations staff must ensure that any personal information digitally produced or processed as part of these procedures is appropriately filed within an approved relevant filing system with role-based access control.

Whilst processing paper documents, including those from third parties, these documents must be stored in secure lockable cabinets. Records will be kept for as long as they are needed to meet the operational needs of Outward, together with legal and regulatory requirements. Where there is a deviation from this principle, the reasons for this must be recorded.

A detailed breakdown of retention and deletion of records can be found in Outward's Record Management and Retention Policy.

When disposing of documents containing personal data this should be done via confidential waste.

Please refer to Outward's Data Protection Policy and Procedure for more information.