

Subject Access Request and Request for Information Policy

October 2026

1. Introduction

This policy explains how Realise Training Group and its subsidiaries (“the Company”) recognise and respond to subject access requests and other requests for personal information. It supports compliance with the UK General Data Protection Regulation, the Data Protection Act 2018 and the Data (Use and Access) Act 2025.

A person is entitled to their personal data and the supplementary information required by data protection law. A subject access request does not automatically entitle a person to every document that mentions them, and exemptions or the rights of other people may limit disclosure.

1.1 Purpose and objectives

- recognise verbal, written and social-media requests for access to personal data;
- respond without undue delay and within the statutory period;
- carry out reasonable and proportionate searches and document the search strategy;
- verify identity proportionately, protect third-party information and apply exemptions case by case;
- provide information securely, clearly and accessibly;
- maintain evidence of decisions, disclosures, complaints and outcomes.

1.2 Scope

This policy applies to all employees, contractors and officers of the Company and to requests concerning learners, applicants, employees, customers, business contacts and other living individuals. It covers personal data held electronically or in hard copy, including email, collaboration systems, learning and case-management systems, HR records, call recordings, photographs and CCTV where held by the Company as controller.

This policy does not form part of any individual’s contract of employment or terms and conditions. The Company may amend it from time to time.

1.3 Responsibilities

Role	Responsibilities
All staff	Recognise requests, preserve relevant records and forward them immediately to IT or the Data Protection Officer (DPO).
Managers	Ensure staff understand this policy, support searches and return complete results by internal deadlines.
IT / Information Security	Log and coordinate requests, support searches, security and disclosure, maintain evidence and monitor timescales.
DPO or authorised privacy lead	Advise on scope, exemptions, third-party data, complaints, refusals and extensions; approve higher-risk responses.
Information owners	Search identified systems, explain context and confirm completeness of the search assigned to them.

2. Recognising a subject access request

A subject access request is a request by or on behalf of a living individual for access to their personal data. It does not need to use the words “subject access request”, cite legislation, use a form or be made in writing. Requests may be verbal or submitted through any Company channel.

- A third party may act where appropriate authority is demonstrated.
- A parent or representative does not automatically have access to another person’s data. Capacity, authority and the rights of the individual must be considered.
- Requests that are actually complaints, erasure requests, freedom of information requests or routine service enquiries must be routed appropriately while preserving any data-rights element.

3. Statutory time limit, clarification and extensions

The Company must respond without undue delay and, in any event, within one calendar month. The due date must be calculated and recorded when the request is logged. Internal target dates are operational controls only and do not replace the statutory deadline.

- Where the Company reasonably requires clarification to identify the information requested, it may ask for clarification and record any lawful pause in the response period.
- Where reasonable doubts exist about identity, proportionate additional information may be requested. The request for evidence and receipt date must be recorded.
- The response period may be extended by up to two further months where necessary because of complexity or the number of requests. The requester must be told within the initial one-month period and given reasons.
- Requests must not be delayed merely because the requester does not use the Company form.

4. Subject access process

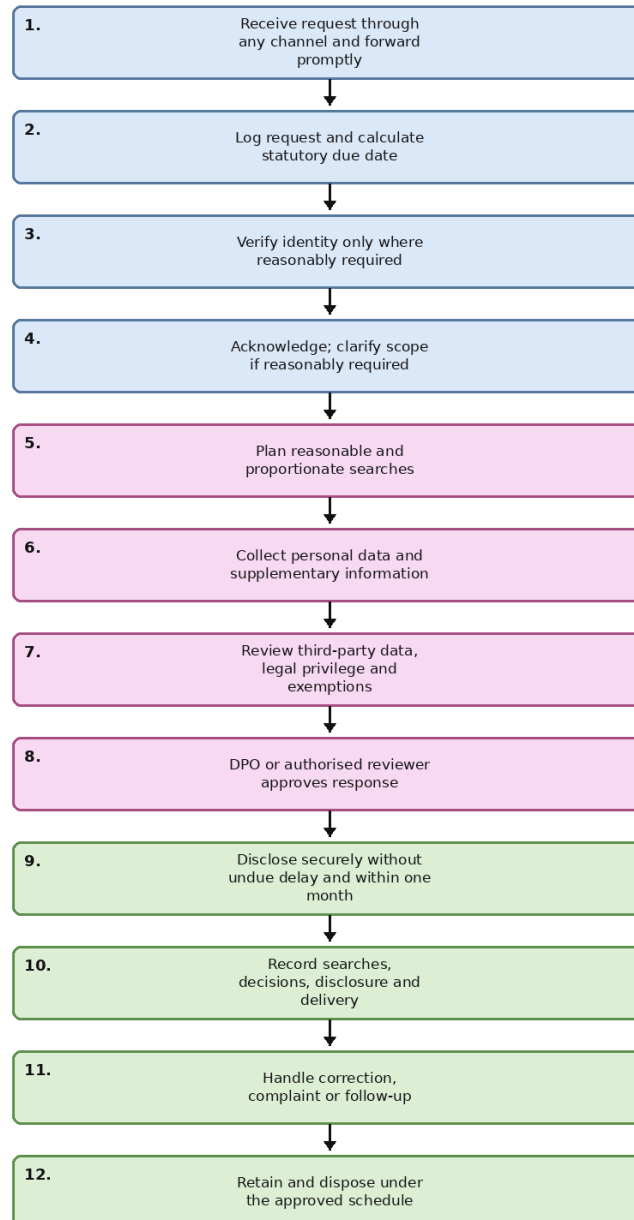


Figure 1. subject access request process

4.1 Stage 1: receipt, logging and verification

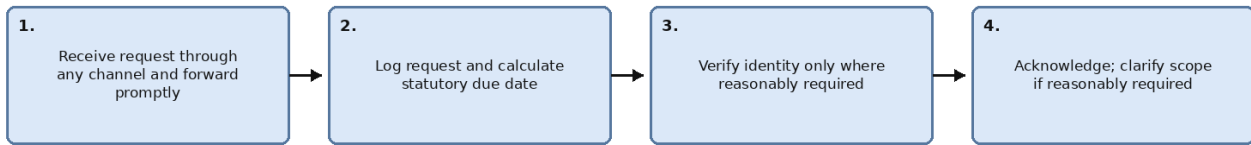


Figure 2. Receipt and verification stage

Step 1: Receive and route the request

Forward the request immediately to IT or the DPO. Preserve the original wording, channel, date and any attachments. Do not ask the requester to resubmit solely on a particular form.

Step 2: Log and triage

Record the request, requester, date received, scope, responsible coordinator, statutory due date, current stage, communications and any special accessibility needs. Identify whether the Company is controller, joint controller or processor for the relevant processing.

Step 3: Verify identity and authority proportionately

Request only the evidence reasonably necessary in the circumstances. Consider the existing relationship, account authentication, sensitivity of the data and risk of unauthorised disclosure. Do not apply a blanket requirement for two original identity documents. Verify third-party authority and the delivery address or channel. Minimise and securely dispose of verification material in accordance with the retention schedule.

Step 4: Acknowledge and clarify where needed

Acknowledge receipt promptly. Confirm the general scope and due date. If the request is broad or unclear, offer assistance and ask only for clarification reasonably required to identify the information. Record when clarification was requested and received.

4.2 Stage 2: search, review and approval

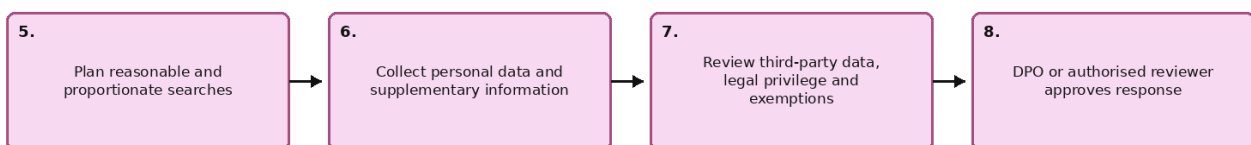


Figure 3. Search, review and approval stage

Step 5: Plan reasonable and proportionate searches

Create a documented search plan based on the wording of the request and where relevant personal data is reasonably likely to be held. The plan may cover e-portfolio and case-management systems, HR systems, email, Teams or collaboration content, SharePoint, signed documents, call recordings, CCTV and retained paper records, as applicable.

Record custodians, systems, date ranges, search terms, limitations and outcomes. Relevant records must be preserved while the request is active.

Step 6: Collect personal data and supplementary information

Collate the requester's personal data, not merely whole documents. Prepare the supplementary information required by law, including purposes, categories, recipients, retention, rights, source information where applicable, relevant transfer safeguards and required information about automated decision-making.

Step 7: Review third-party information and exemptions

The starting point is disclosure of the requester's personal data. Consider third-party rights, confidentiality, legal professional privilege, management information, negotiations, crime and taxation, regulatory functions, education or social-work information, health information and other applicable restrictions case by case. Do not treat document ownership or another organisation's involvement as an automatic reason for removal. Record the legal basis, reasoning, decision-maker and extent of each withholding or redaction.

Step 8: Quality assurance and authorisation

An authorised reviewer must verify identity and authority, search completeness, redactions, exemptions, supplementary information, delivery method and response wording. Material exemptions, refusals and high-risk third-party decisions must be referred to the DPO or authorised privacy lead.

4.3 Stage 3: secure disclosure and completion

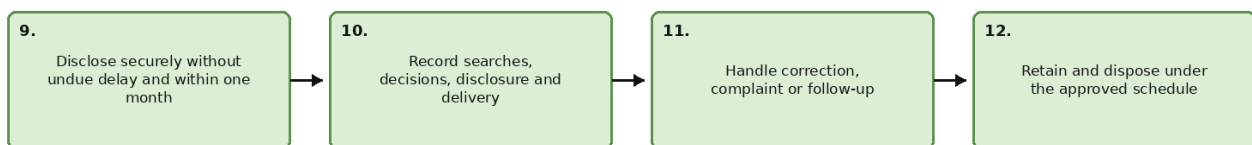


Figure 4. Disclosure and completion stage

Step 9: Disclose securely

Provide the response in a concise, transparent, intelligible and easily accessible form, using clear language. Use the requester's preferred electronic means where appropriate, or another approved secure method. Verify the destination before release and use proportionate encryption, access controls or tracked delivery. Avoid unnecessary portable media.

Step 10: Update the register

Record the response date, information categories supplied, searches performed, exemptions and third-party decisions, reviewer, delivery method, proof of delivery and any delay or extension.

Step 11: Explain outcomes and complaint routes

The response must explain any material withholding or refusal to the extent permitted, and provide the Company's data-protection complaint route and the right to complain to the Information Commissioner's Office. Any complaint must be acknowledged and handled under the Company's data-protection complaints procedure within the applicable legal timescales.

Step 12: Retain and dispose

Retain the request file, response, disclosure copy, search evidence and decision log for the period set by the approved retention schedule. The previous 12-month period may be retained only if confirmed in that schedule and justified by accountability and limitation risks. Dispose of records securely when the period expires and do not keep additional identity evidence longer than necessary.

5. Exemptions, restrictions and refusals

Exemptions and restrictions must not be applied as a blanket rule. The decision must be necessary, proportionate, documented and limited to the information affected. The Company must disclose the remainder where possible.

Topic	Required approach
Information about other people	Consider consent where appropriate and whether it is reasonable to disclose without consent, taking account of all relevant circumstances.
Legal professional privilege	Withhold only material covered by the applicable privilege exemption.
Management information and negotiations	Apply only where the relevant statutory conditions and prejudice tests are met.
Crime, taxation and regulatory functions	Apply only where disclosure would prejudice the protected purpose and the statutory conditions are met.
Education, health and social-work information	Escalate because specific restrictions and consultation requirements may apply.
Manifestly unfounded or excessive requests	The Company bears the burden of proof. Obtain DPO approval, document the evidence, and explain the decision, complaint route and ICO right.
Fees	Normally no fee. A reasonable fee may be considered only where the law permits, with DPO approval and documented calculation.

6. Other information requests

6.1 Court orders and legal proceedings

Refer court orders, litigation requests and legal process promptly to the DPO and appropriate legal or senior authority. Verify authenticity, scope, deadlines and restrictions. Preserve relevant evidence and disclose only what the order or lawful process requires through an approved secure channel.

6.2 Police and other statutory requests

A request from the police or another authority does not automatically require or permit disclosure. Obtain a written request or other reliable record where practicable, verify the requester and authority, identify the purpose and legal gateway, assess necessity and proportionality, disclose the minimum required information, use a secure channel and retain the decision record. Emergency requests must still be documented and reviewed afterwards.

6.3 Safeguarding and information-sharing agreements

Safeguarding disclosures and requests governed by a valid information-sharing agreement must follow the relevant safeguarding process and agreement. Confirm that the request falls within the documented purpose, parties, data types and security controls. Escalate deviations or uncertainty to the DPO, safeguarding lead or IT as appropriate.

6.4 CCTV and recordings

CCTV, images and recordings may contain personal data about several people. Preserve relevant footage promptly, verify the request, assess third-party rights, use redaction or masking where reasonably possible, and disclose through an approved secure method. Portable media is not mandatory and may be used only where approved and appropriately protected.

6.5 Ad-hoc disclosures

Do not assume consent is always the correct legal basis. Identify and document the lawful basis, purpose, necessity, proportionality, recipient, data minimisation and security. Use an information-sharing agreement for regular or systematic sharing where appropriate.

7. Other individual rights

Requests for rectification, erasure, restriction, portability, objection, withdrawal of consent and rights relating to automated decision-making must be logged and referred to the DPO or authorised privacy lead. Each right has conditions and exceptions and must be assessed on its facts.

- Rectification: investigate accuracy and correct or complete inaccurate personal data without undue delay. Record disputes and notify relevant recipients where required.
- Erasure: the right is not absolute. Assess the lawful basis, continued necessity, legal obligations, establishment or defence of legal claims and other applicable exceptions.
- Restriction and objection: record the request promptly and apply interim restrictions where legally required while the assessment is completed.
- Portability: applies only in defined circumstances and requires provision in a structured, commonly used and machine-readable format.
- Automated decision-making: provide required information and safeguards where significant solely automated decisions are used.

8. Governance, training and assurance

- Maintain a central information-request register and evidence of identity checks, searches, decisions, disclosures, delays, extensions and complaints.
- Train all staff to recognise requests; provide role-specific training for coordinators, reviewers and system owners.
- Test completed cases periodically for timeliness, search quality, redaction accuracy, security and completeness of supplementary information.
- Report material trends, overdue cases, incidents and corrective actions to appropriate governance forums.
- Treat misdirected or unauthorised disclosure as a potential personal data breach and follow the Company's incident process immediately.

9. Contacts

Function	Contact
IT / Information Security	iso@realisetraining.com
Data Protection Officer	dpo@realisetraining.com

10. Policy Review

Version Control Number	Realise-08-PD-106
Version	V5
Last Review Date	01/10/2026
Next Review Date	01/20/2027
Policy Owner	Patrick Richter IT Manager
Signed by Managing Director	 Gregg Scott Realise Training Group Managing Director

Appendix A - Change log

Section	Issue identified	Amendment
Legal framework	Policy referred to the DPA 2018 as “GDPR” and did not reflect the Data (Use and Access) Act 2025.	Corrected the framework and updated subject-access process requirements.
Time limits	Used an average 30-day concept and fixed 28-day workflow.	Replaced with one calendar month, lawful clarification handling and two-month extension rules.
Identity checks	Required two original identity documents as a default.	Introduced risk-based, reasonable and proportionate verification.
Scope of access	Stated that a person can obtain all information held about them.	Clarified access to personal data plus required supplementary information.
Searches	No express reasonable and proportionate search standard or search record.	Added documented search planning, custodians, systems, terms, limitations and outcomes.
Exemptions	Used numbered summaries that risked conflating different legal regimes and suggested 73 exemptions.	Replaced with applicable categories, case-by-case tests, approval and decision records.
Other controllers	Treated ownership by another organisation as automatic removal.	Reframed around controller/processor status and lawful handling.
Police and ad-hoc sharing	Suggested broad ability to disclose and over-relied on consent.	Added lawful-gateway, necessity, proportionality, minimisation and audit requirements.
CCTV	Required memory-stick disclosure.	Replaced with approved secure methods and proportionate third-party protection.
Other rights	Suggested automatic correction or deletion.	Added conditions, exceptions and DPO assessment for each right.
Complaints	No complete statutory data-protection complaint route.	Added internal complaint handling and ICO escalation.
Images	Original diagrams contained superseded fixed-day deadlines.	Retained and redrawn the three-stage visual process with corrected statutory wording.
Template	Source formatting and header image did not follow the governing template.	Applied the Group template, required typography and fully bordered tables; excluded the header image.