THE LEARNING TRUST
NURTURING • AMBITION • EXCELLENCE

TLT Subject Access Request (SAR) Policy

Created:	20 October 2025
Policy leads:	Darran Jones, Trust CEO; Dave Helsby, Director of IT and DPO
Review Period:	Annually
Policy renewal date:	Autumn 2026
Reviewed and approved by the Trustees Resources Panel:	20 November 2025
Date approved by the Board of Trustees:	04 December 2025

1. Purpose

This policy outlines how The Learning Trust will respond to Subject Access Requests (SARs) made under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Data Use and Access Act 2025. It ensures individuals can exercise their right to access personal data that the Trust meets is legal obligations in a fair, transparent and timely manner.

2. Scope

This policy applies to:

- All academies within the Learning Trust;
- All employees, trustees/governors, contractors and volunteers who handle personal data:
- Any personal data held by the Trust, regardless of format (digital, paper, audio or visual).
- In line with the Data Use and Access Act 2025, this policy applies retrospectively to all open SAR cases at the date of adoption by Trustees.

3. Definition of a Subject Access Request (SAR)

A Subject Access Request (SAR) is a request made by a data subject to obtain:

- Confirmation that the Trust is processing their personal data,
- A copy of that data

- Supplementary information about how the data is processed, shared and stored

Requests may be made verbally, in writing or through any reasonable communication channel.

4. Legal Framework and 2025 Updates

Under the Data Use and Access Act 2025:

- The Trust must take **reasonable and proportionate** steps to locate data rather than perform exhaustive searches,
- The one-month response deadline may be paused ("stop-the-clock") while awaiting ID verification or clarification of scope,
- Controllers must have a clear complaint-handling route for data subject rights.

When responding to a Subject Access Request, The Learning Trust will take reasonable and proportionate steps to identify, locate, and retrieve the relevant personal data.

This means the Trust will conduct searches where data is likely to be held and will balance the effort required against the likely benefit to the data subject.

The Trust is not required to conduct exhaustive or impractical searches, but must be able to justify the scope and methods used in each case.

Section 9 contains more clarification on how the Learning Trust will interpret 'reasonable and proportionate'

5. Responsibilities

- Data Protection Officer (DPO): Oversees compliance and advises on complex or sensitive SARs
- Headteachers: Ensure local staff awareness and cooperation
- All staff: must forward any SAR immediately to the DPO
- Trust Board: monitors compliance and ensures adequate resourcing

6. Submitting a Request

Requests should be sent to the DPO at dpo@tltrust.co.uk or to the enquiries email address at any of the Trust's academies.

Any clear request for personal data will be treated as a SAR, whether that exact term is mentioned or not.

The Trust will require proof of identity and will pause the timeframe until sufficient verification is received.

7. Verification of Identity

Before releasing data, the Trust must confirm the identity of the requester

Acceptable ID includes a passport, driving licence or recent utility bill.

Parents requesting on behalf of a child may need the child's consent if the child is judged to have sufficient maturity (age 12+).

8. Timeframe for Response

The Trust will acknowledgement receipt within 5 working days and respond within one calendar month once the request is deemed valid (upon confirmation of ID)

For complex or multiple requests, the deadline may be extended by two additional months.

The "stop-the-clock" provision applies while waiting for ID or clarification.

9. Reasonable and Proportionate Searches (DUAA 2025)

Under the 2025 reforms, the Trust is required to take **reasonable and proportionate** steps to identify, locate and retrieve the requested personal data, when responding to a SAR. This means the Trust must make **genuine and appropriate efforts** to find the requested data **without being required to conduct an exhaustive or disproportionate search**. This means:

- The Trust will make genuine and appropriate efforts to locate data where it is **likely to be held**, based on the information provided
- The Trust is not required to conduct exhaustive searches of all systems, backups or historic data
- The Trust will document what was searched, and why.

Determining Reasonableness and Proportionality

The Trust will consider:

1. The nature and clarity of the request – how specific or broad it is
2. Where relevant data is likely to be stored – e.g. MIS (Sims), HR systems, safeguarding platforms (CPOMS/Edaware) and email accounts of key or relevant staff.
3. Resources and time available – balancing the administrative burden against educational operations

4. The sensitivity and significance of the data eg safeguarding or HR information
5. The likely value of the data to the requester – ie whether extended searches would yield meaningful new information.

Scenario	Reasonable and Proportionate Response
Search Scope	Check all systems where personal data is *likely* to be held, not every conceivable location. For example: MIS (SIMS/Synergy), staff HR files, email accounts of relevant staff, safeguarding systems (CPOMS/MyConcern), and key shared drives. No need to manually open every historic email or archive if there's no reason to believe relevant data is there.
Time spent	The search should take an amount of time consistent with the size of the Trust and the scale of the request. For example, 5–10 hours of admin/DPO time for a single-person SAR in a small MAT is likely reasonable; 100 hours is not. Hundreds of emails are fine, thousands are not.
Systems checked	Focus on current systems and recent archives. Only check backups or legacy systems if you have reason to believe they contain relevant data.
Filtering	Use keyword searches and date ranges (e.g. name, email, pupil ID) to limit scope and remove clearly irrelevant data. Initials of pupils is not a reasonable filter.
Third parties	We are not required to recover data held independently by other organisations (e.g. local authorities, external service providers) unless the Trust controls that data.
Documentation	Keep a note of what was searched, and why. The ICO recognises documentation of your rationale as evidence of "reasonable and proportionate" compliance.
Requests for "all data about my child"	Search pupil MIS, safeguarding systems, SEND records.
Requests covering long historical period	Search current systems and key archives, exclude backup and legacy servers unless known to hold relevant data
Generic request with little detail	Seek clarification to narrow scope before searching and instigate "stop-the-clock" to the timeframe

Both the **ICO (2025)** and the **Data Use and Access Act 2025 Factsheet (Cabinet Office)** confirm that:

"Controllers are not required to undertake an exhaustive search across all possible systems or devices. Searches should be reasonable and proportionate to the nature of the request, taking into account the resources available and the likely relevance of the information."

(ICO Guidance on Subject Access Requests, updated 2025)

10. Format, Provision and Fees

Data will be provided electronically unless requested otherwise. No fee unless the request is excessive or manifestly unfounded.

11. Exemptions and Withholding Information

The Trust may withhold data where exemptions apply, including:

- Data identifying another individual
- Legal professional privilege
- Confidential references
- Management planning information
- Safeguarding

Any redactions or exemptions will be justified and recorded. See appendix 2

12. Record Keeping

All SARs will be logged including date received, acknowledged and completed, including verification steps, search scope and rationale, data released/withheld, any exemptions and complaints and outcomes.

13. Staff Training

Staff who handle or may receive SARs will receive annual training on recognising SARs, the “reasonable and proportionate” approach, secure handling and redaction and escalation to the DPO.

14. Complaints and appeals

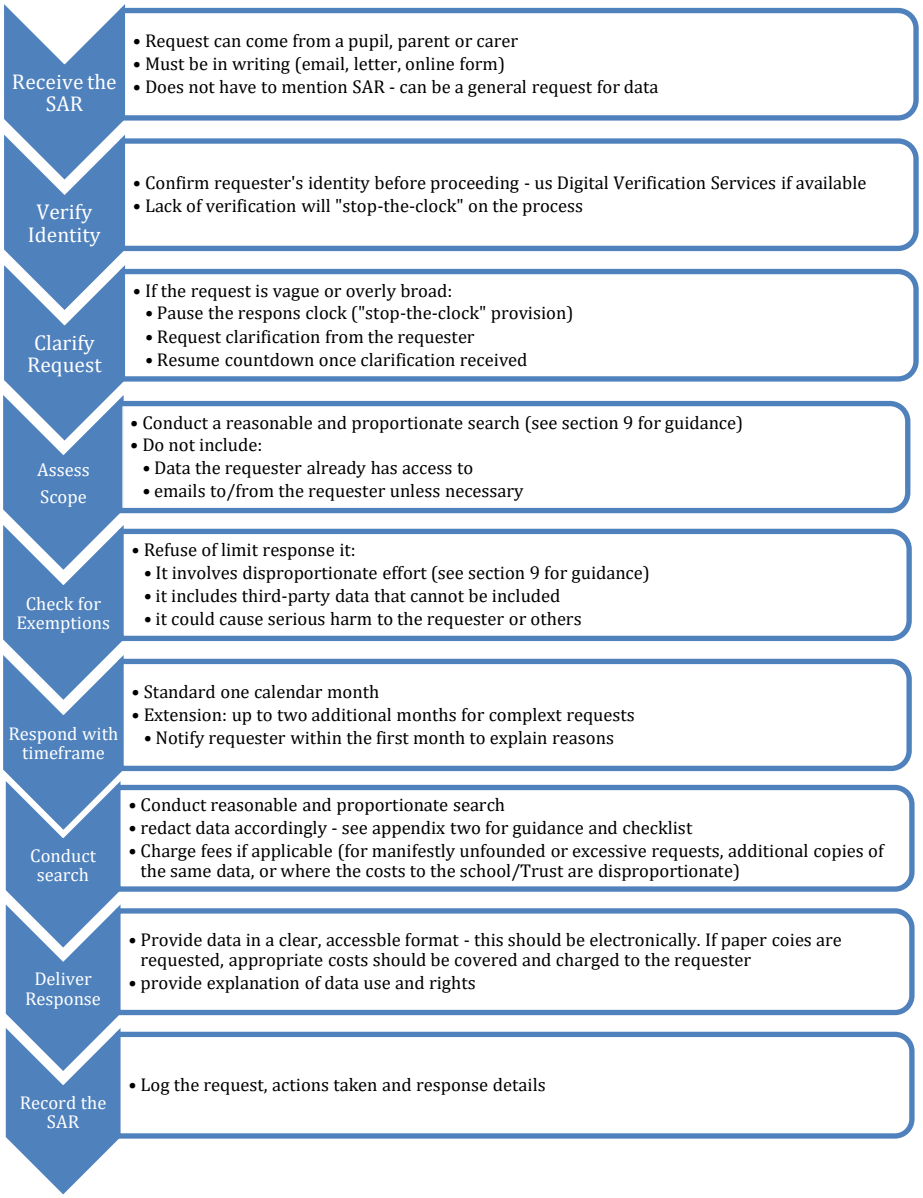
Individuals may complain to the DPO about SAR handling.

If unsatisfied, they may escalate to the Information Commissioner’s Office (ICO) at www.ico.org.uk

15. Review

This policy will be reviewed annually or earlier if there are significant changes to legislation or guidance changes or operational changes.

Appendix 1 - Subject Access Request (SAR) Handling Flow – DUAA 2025



Appendix 2 – Redaction guidelines

1. Protecting the Rights of Other Individuals

If fulfilling a SAR would disclose personal data about another identifiable person, you may redact that information unless:

- The other individual has **consented** to the disclosure, or
- It is **reasonable** to comply without their consent (e.g. minimal impact or public interest)

This is outlined in **Section 7(4)** of the Data Protection Act 2018. [

2. Legal Professional Privilege

Information protected by **legal privilege** (e.g. confidential communications between a lawyer and client) can be withheld. This ensures legal advice remains confidential.

3. Confidential Business Information

If the SAR includes data that reveals **trade secrets** or **commercially sensitive information**, redaction may be justified to protect business interests—especially if disclosure could harm the organisation or its partners.

4. Data Not Relevant to the Requester

Sometimes documents contain the requester's name but are not **about** them. For example:
An email sent to all staff mentioning Sarah in the "To" field but not discussing her specifically does **not** need to be disclosed.

5. National Security or Law Enforcement

Certain exemptions apply where disclosure could:

- Prejudice **national security**
- Interfere with **ongoing investigations**
- Reveal **covert surveillance** or sensitive law enforcement techniques

6. Manifestly Unfounded or Excessive Requests

If a SAR is clearly **unreasonable**, repetitive, or intended to disrupt, the organisation may refuse or limit the response. This must be justified and documented.

7. Internal Management Information

Notes or documents used solely for **internal planning or forecasting** (e.g. succession planning, disciplinary deliberations) may be exempt if they don't directly relate to the individual.

Subject Access Request (SAR) Redaction Checklist

This checklist is designed to support organisations in managing redactions when responding to Subject Access Requests (SARs) under the UK GDPR and Data Protection Act 2018. It includes steps for identifying personal data, assessing exemptions, documenting redaction decisions, and conducting a final review.

1. Identifying Personal Data

- [ ] Review all documents and communications for personal data related to the requester.
- [ ] Confirm the data is about the requester and not merely referencing them.
- [ ] Separate mixed data sets where possible.

2. Assessing Exemptions

- [ ] Check for third-party personal data and assess if redaction is necessary.
- [ ] Consider legal professional privilege (e.g. legal advice, litigation documents).
- [ ] Identify any confidential business information or trade secrets.
- [ ] Review for national security or law enforcement exemptions.
- [ ] Determine if the request is manifestly unfounded or excessive.
- [ ] Exclude internal management forecasting or planning documents if applicable.

3. Documenting Redaction Decisions

- [ ] Record each redaction with justification.
- [ ] Note the type of exemption applied.
- [ ] Maintain a log of redacted items for audit purposes.
- [ ] Ensure decisions are reviewed by a data protection officer or legal advisor.

4. Final Review

- [ ] Verify all redactions are consistent and justified.
- [ ] Confirm the response includes only relevant personal data.
- [ ] Ensure the SAR response is clear, complete, and compliant.
- [ ] Retain a copy of the final redacted documents and checklist.