SUBJECT ACCESS REQUEST (SAR) POLICY

THIS POLICY APPLIES TO THE HEARTWOOD LEARNING TRUST BOARD, THE CENTRAL TEAM, AND ALL TRUST SCHOOLS/ACADEMIES

This policy has been reviewed in line with The Data (Use and Access) Act 2025 which received Royal Assent on 19th June 2025.

Document Management	
Updated Policy Approved	October 2025
Next Review Date	October 2026
Version	2.2
Approved By	Chief Operating Officer

Contents

Policy Updates

Date	Page	Policy Updates
October 2023	Whole policy	Updated inline with the new Scheme of Delegation
June 2024	3	Statement of Intent - wording updated
June 2024	4	1 - Legal Framework - updated inline with current applicable legislation and Trust policies
June 2024	4	2 - Roles and Responsibilities - section added for clarity of processes involved in SARs reported to the Trust
June 2024	5	4 - Requests for Information - section added for clarity
June 2024	7	8.2 - Point added re: conditions for complying with a SAR from a parent/carer on behalf of a pupil
June 2024	7	9 - section updated to reflect CCTV footage is used for internal monitoring purposes only
June 2024	9	12 - Monitoring and Review - section added inline with other Trust policies
September 2024	6	6.2 - All SARs must be sent to dpo@hlt.academy
September 2024	7	6.3 - Template to respond to SARs with amended to reflect new procedures
September 2024	10	Appendix 1 - Template amended to reflect new procedures
April 2025	3	Introduction added in line with other Trust policies
April 2025	3	Statement of Intent wording updated
April 2025	4	1.3 - Point updated to include Data Retention Schedule
April 2025	4	2 - Roles and Responsibilities section updated
April 2025	6	4.2 - Point added to clarify procedures where a request may not be considered a SAR
April 2025	9	11 - Section added on withholding data/refusing requests
April 2025	10	Appendix removed as an updated version is included within the Trust's SAR procedures
October 2025	4	1.1 - Legal Framework updated
October 2025	7	7.2 - Point added to reflect procedures for responding to SARs
October 2025	Whole policy	References to the Compliance Officer changed to Executive Support Manager

Introduction

Heartwood Learning Trust is an inclusive and collaborative Church of England multi-academy trust serving church, community and alternative provision schools. This policy is guided by our Christian ethos and the visions of our Trust and its schools/academies. We share a clear vision – to create schools where children and young people thrive, as we help them prepare to live life in all its fullness (John 10:10).

For us, a place to thrive means much more than a place simply to be comfortable. Instead, our aim is to develop schools and an educational offer which enable each pupil to flourish academically, practically, emotionally, socially and spiritually.

Statement of Intent

A Subject Access Request (SAR) is a request made by, or on behalf of, an individual for the information which they are entitled to ask for under **Article 15 of the UK GDPR**. Heartwood Learning Trust (HLT) is committed to upholding the rights of individuals to obtain a copy of their personal data and to be transparent about our approach to such requests, as Data Controller.

A subject access request is a written or verbal request for personal information (known as personal data) held about a data subject by an organisation. The **UK General Data Protection Regulation (UK GDPR)** gives individuals the 'Right of Access', entitling the data subject to know what information is held about them. It provides a framework to ensure that personal information is handled properly. However, this right is subject to certain exemptions that are set out in the **UK GDPR**. Any disclosure should be fair, lawful and transparent; information should be limited to what is necessary.

This document sets out the HLT policy for responding to SARs under the **UK GDPR** and the **Data Protection Act (DPA) 2018** and should be read in conjunction with the Trust's **Subject Access Request (SAR) Procedures**.

Frequent verbal enquiries and correspondence that covers information that is provided routinely and can be managed quickly in the normal course of the school/academy's business, e.g. a request by an employee to see their employment contract, are not considered to be SARs and are not considered under this policy.

1. Legal Framework

1.1. This policy has due regard to all relevant **legislation** and and **statutory guidance** including, but not limited to, the following:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act (DPA) 2018
- Freedom of Information Act 2000
- Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- DfE (2023) 'Data Protection in Schools'
- Data (Use and Access) Act 2025

1.2. This policy has due regard to **guidance** including, but not limited to, the following:

- Subject Access Code of Practice

1.3. This policy operates in conjunction with the following **Trust** policies and procedures:

- Data Protection (UK GDPR) Policy and Data Retention Schedule
- Complaints Policy and Procedure
- Freedom of Information (FOI) Policy
- Subject Access Request (SAR) Procedures

2. Roles and Responsibilities

2.1. The **Audit & Risk Committee** on behalf of the **Trust Board** is responsible for:

- Maintaining strategic oversight of the management of risk associated with data protection and personal data under the Trust's control
- Ensuring the Trust remains compliant with applicable data protection legislation regarding their handling of SARs
- Ensuring the Trust respects the rights of individuals to obtain copies of their personal information

2.2. The **Data Protection Officer (DPO)** is responsible for:

- Approval of this policy on an annual basis
- Oversight of all GDPR related practices across the Trust
- Liaising with the **Information Commissioner's Office (ICO)** and seeking legal advice, where required
- Ensuring employees responsible for handling SARs receive suitable training

2.3. The **Principal** is responsible for:

- Ensuring that all staff understand how to recognise a SAR
- Cascading the Trust's **Subject Access Request (SAR) Policy** to all staff
- Ensuring all staff are aware of the school/academy's **GDPR Representative** and how they can be contacted with any queries

2.4. The **Director of Safeguarding** is responsible for:

- Providing advice and guidance to the **Designated Safeguarding Lead (DSL)**, nominated **GDPR Representative** and **Executive Support Manager**, where required to support during SARs

- Reviewing SARs to confirm the data subject(s) are not considered to be at risk of harm should the Trust disclose the requested information

2.5. The **Executive Support Manager (ESM)** is responsible for:

- Proving final validation of redactions and making required suggestions prior to information being disclosed externally
- Ensuring the policy is reviewed and updated
- Providing a main point of contact for SARs received by the Trust and ensuing the requestor is liaised with to confirm receipt of a SAR and to securely release the requested information upon completion
- Ensuring there is an auditable trail/register of all SARs reported across the Trust and assigning a reference to each SAR to ensure this information is tracked appropriately
- Ensuring that deadlines for SARs to the nominated **GDPR Representative**
- Ensuring regular contact with nominated **GDPR Representatives** and school/academy staff to ensure their awareness of the work required and expected timescales for completion
- Liaising with the **ICO** or seeking legal advice on behalf of the schools/academies where required

2.6. The **Designated Safeguarding Lead (DSL)** is responsible for:

- Advising the nominated **GDPR Representative** of any possible safeguarding concerns when dealing with SARs
- Liaising with the Trust's **Director of Safeguarding** where required for complex cases

2.7. The nominated **GDPR Representative** is responsible for:

- Updating the **DPO** via the designated **DPO** email throughout the lifecycle of the SAR
- Liaising with appropriate school/academy staff to collate information requested in any SARs
- Redacting any information requested and ensuring this is reviewed by the **ESM** prior to its release

2.8. **All Staff** are responsible for:

- Adhering to this policy and the Trust's **Subject Access Request (SAR) Procedures** regarding all requests received for access to personal data
- Being able to recognise a SAR and identify who their **GDPR Representative** is
- Providing information to support the completion of SARs, where required and within their remit or area of responsibility and expertise
- Ensuring the wellbeing of pupils, and where applicable, their families, is taken into account when handling SARs

3. Subject Access Requests under UK GDPR

3.1. The **UK GDPR** works in two ways. Firstly, it states that anyone who processes personal data must comply with six principles, which make sure that personal data is:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and where necessary, kept up to date

- Kept in a format which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed
- Processed in a manner that ensures appropriate security of the personal data

3.2. Secondly, it provides individuals with important rights, including the right of access. Individuals have the right to find out details of what personal data is being held about them, by both electronic means (e.g. on a computer or other device) and as paper records intended to form part of a manual filing system.

3.3. **Personal data** means any information which can be used to identify a natural (living) person.

3.4. Personal data includes basic information (such as a person's name, address, telephone number, etc) as well as **Special Category data,** which includes more sensitive data such as information relating to personal beliefs, health, gender or biometric information, etc.

4. Requests for Information

4.1. The Trust and its schools/academies control and process large volumes of personal data regarding stakeholders. Everyone is entitled to submit a request for access to the personal data held about them.

4.2. In cases where the Trust is a Data Processor rather than a Data Controller, the Trust will provide a clear explanation of why they are not able to provide the requested information and will signpost the data subject to the appropriate body.

4.3. The Trust will treat any request where it is clear that an individual is asking for their own personal data, and which is outside of the school/academy's normal course of business, as a SAR. The **ESM** will determine whether enquiries that are not formal requests for information should be processed as a SAR on a case-by-case basis.

4.4. The Trust may receive requests for personal data which refer to the **Freedom of Information Act 2000**; these requests will be processed in accordance with this policy and the Trust will notify the requester of the expected timescale for completion of the SAR.

4.5. As a Multi-Academy Trust, our schools/academies are not expected to adhere to the **Education (Pupil Information) (England) Regulations 2005**, which gives parents/carers the right of access to a pupil's educational record within 15 school days. For academy schools, parents/carers have no legal right of access to their child's educational record; this information may be provided at the school/academy's discretion and may be subject to the pupil's consent, depending on their age. If however, a request for an educational record forms part of the information requested in a Subject Access Request, the Trust will treat this as a SAR and will respond to these statutory requests.

5. Procedures

5.1. When a subject access request is received, the Trust will firstly confirm the identity of the data subject (or the individual making the request on their behalf). The Trust may request any information reasonably required to **confirm the identity of the requester**. The Trust will request any verification documentation promptly.

5.2. The timescale for responding to a SAR is **one calendar month** from the date the identity of the requester is verified and the Trust has received clarification on the types of information being requested, where

applicable. The Trust will respond to a SAR to provide the requester with the information or to provide a clear explanation as to why the Trust is unable to provide the information, depending on the circumstances.

5.3. The information will be provided in the **most appropriate format**. The **UK GDPR** contains a number of exemptions to our duty to disclose personal data and we may seek legal advice if we consider that they might apply. An example of an exemption is information covered by legal professional privilege. If we agree that the information is inaccurate, we will correct it and where practicable, destroy the inaccurate information. If we do not agree or feel unable to decide whether the information is inaccurate, we will make a note of the alleged error and keep this on file.

6. Verbal Requests

6.1. If a verbal Subject Access Request (SAR) is received, the Trust will request that the SAR be **confirmed in writing** (via letter or email), and for the subject to provide any other information the Trust may require to verify their identity. The Trust asks that SARs are submitted in writing so that an accurate record can be retained of any information pertaining to the SAR, for audit purposes.

6.2. Requests should be sent to the nominated **GDPR Representative** within the individual Trust academy/school and emailed to dpo@hlt.academy. Contact information is available on the school/academy's website.

7. Deadline for Receipt of Information

7.1. The Trust will respond without undue delay and where possible, within one calendar month of receipt of the request (where suitable ID has been provided for verification). The Trust may, in exceptional circumstances, extend the 'deadline' by up to two calendar months. An extension may be considered appropriate where the initial assessment of the personal data held indicates that the request is complex, or there are numerous requests received from the same individual.

7.2. Once the information has been gathered for the SAR, the data will be shared via an email link from the DPO inbox to a secure Google Drive folder, which will be made available to the data subject (or the parent/carer submitting the request on their behalf) for a period of 48 hours, to enable them to download the personal data to their personal device. Where it is not possible to provide electronic delivery, the requested information will be made available for collection by the data subject (or the parent/carer submitting the request on their behalf).

7.3. There will be no charge for the request unless it is unfounded or excessive, in which case the Trust has the right to charge a reasonable fee based on the administrative costs incurred for providing the information requested. Alternatively, the Trust may refuse to act on the request.

8. Compliance with a SAR

8.1. A Subject Access Request is valid if it is clear that the requestor is asking for their own personal data (or that of a child for whom they are responsible for, with their consent, if required). A SAR only applies to 'personal data'. A definition of personal data is provided in full within the **Data Protection (UK GDPR) Policy**.

8.2. The Trust will release pupil's personal data requested in a SAR to someone with parental responsibility only when the school/academy believes that doing so would not cause distress, detriment or result in a safeguarding concern for the pupil involved. The Trust will permit release of a pupil's personal data when the pupil has provided their authorisation for this to take place or it is evident that this is in the pupil's best interests.

9. Records to be Provided

9.1. The right of access applies to both electronic/automated records and to manual records which enable information about a **particular individual** to be **easily retrieved**.

9.2. Examples of automated records include:

- Computer files - files stored on discs, DVDs, hard disks, back-up files, emails etc.
- Audio/Video* - CCTV footage, webcam images
- Digitalised images - scanned photos, images held on digital cameras

9.3. Examples of manual records include:

- Files - overview information held on employees, parents/carers, pupils
- Index systems - names, addresses, other details

**It should be noted that the Trust utilises CCTV footage for internal monitoring purposes only.*

10. Redacting Information

10.1. Whilst the **UK GDPR** gives individuals the right to access their own personal data, it does not permit access to information relating to, or that which could be used to identify other people. As such, the Trust will not disclose any personal data relating to third parties when fulfilling a subject access request, unless explicit consent has been received.

10.2. All personal data relating to any individuals other than the data subject will be redacted. Redaction software will be used to permanently edit PDF files by removing the required sections and 'sanitising' the document. Where paper files are manually redacted, this will be repeated until the information is no longer visible. Photocopies of manually redacted documents will be provided to the subject (rather than the original redacted papers) as the photocopying process will ensure the redacted information is completely obscured. A copy of the original redacted documents will be retained by the school/academy.

Some basic rules to apply when redacting

10.3. The information disclosed should relate to the data subject making the request and should not include irrelevant/supplementary information.

10.4. Particular care should be taken when redacting to ensure that the personal data of other individuals is not disclosed. Any information which would allow the reader to identify any person(s) (not including the data subject) from the information held should be removed.

10.5. The following general rules should be applied - although there may be specific incidents when they would not:

- Redact all names other than that of the person making the request
- Redact job titles

- Redact email addresses
- Redact addresses
- Redact phone numbers
- Redact references to an individual's gender if that could lead to them being identified
- Redact personal descriptions which may lead to a person being identified (e.g. a description of someone as a brown-haired man is unlikely to identify someone, but a red-haired man with a beard may redact any other narrative data that would lead to an individual being identified)
- Think about the combination of information sets that taken together would lead to an individual being identified
- When taking out personal details from email headers, leave in the date and title line unless the title line conflicts with the above

11. Withholding Data

11.1. There are **exemptions** to disclosure which are generally very specific and tend to apply to particular cases, e.g. confidentiality of police investigations or HR records.

11.2. Should the identity of any third party be ascertainable following redaction, the Trust would then reserve the right to withhold the information held, and refuse to comply with the SAR if doing so would impede the rights of the third party under **UK GDPR** and the **Data Protection Act 2018**. In such instances the Trust will respond to the requester to justify the decision to withhold any information on this basis.

11.3. Exemptions can apply if a request is considered to be **manifestly unfounded** (e.g. a request is made with malicious intent or for personal gain) or **manifestly excessive** (e.g. disproportionate or repetitive). Further clarification on what constitutes an unfounded or excessive SAR can be sought via the **ICO** website. It is quite rare for exemptions to apply more generally and justifiable decisions must be made on a carefully considered, discretionary basis.

11.4. If an exemption applies, it may be possible to refuse to provide some or all of the requested information, depending on the circumstances. Please refer to the **ICO** website for further information and guidance regarding exemptions and where these apply.

12. Information Commissioner's Office (ICO)

12.1. The Trust would encourage anyone who is not satisfied by our actions following a SAR to seek recourse through our internal complaints procedure. For further information, the Trust's **Complaints Policy and Procedure** is available on our website: https://hlt.academy/our-policies.

12.2. Alternatively, or in cases where an individual remains dissatisfied, they have the right to refer the matter to the Information Commissioner for their review. The **ICO** can be contacted via the following means:

Postal Address	Information Commissioner's Office Wycliffe House, Water Lane Wilmslow, Cheshire, SK9 5AF	**Telephone**	01625 545745
		Email	enquiries@ico.gsi.gov.uk
		Website	https://ico.org.uk

13. Monitoring and Review

13.1. The approver of this policy and the next scheduled review date is shown on the cover page of this document.