DATA PROTECTION POLICY

Learning Academies Trust

Version: 4.0

Last review date: 11 March 2026

Next review date: 31 March 2027

LEARNING ACADEMIES TRUST

CONTENTS

CHANGES

Policy date	Summary of change	Author	Version	Review date
01/11/2018	Policy has been created	Kay Mabin, CFO	1.0	01/11/2019
19/11/2019	SAR can now be requested verbally (previously had to be in writing) Section 9.1 updated.	Kay Mabin, CFO	2.0	19/06/2020

07/11/2020	Amendment to formatting and policy names referenced throughout.	Luke Pollard, ICT Network Manager	2.1	07/11/2021
04/11/2022	Review of the policy and language used. Provided more in depth detail on UK GDPR principles	Kelly Miller, DPO	3.0	22/11/2023
19/02/2024		Kelly Miller, DPO		28/02/2025
11/03/2026	Updated to comply with the UK GDPR, Data Protection Act 2018, and Data (Use and Access) Act 2025 (DUAA). Corrected all legislative terminology to 'UK GDPR' throughout. Removed EEA transfer references; updated to UK adequacy framework. Added DUAA changes: seventh lawful basis (recognised legitimate interests); SAR reasonable and proportionate search standard; updated unfounded/excessive SAR threshold; children's online services obligation; processor breach notification obligation; standalone Data Protection Complaints section (s.164A DPA 2018 as amended by DUAA); DP complaints signposting requirement. Strengthened CCTV section with lawful basis, retention and access controls. Removed cross-reference to non-existent CCTV Policy. Specified Schedule 1 DPA 2018 conditions (paras 6 and 18). Added 72-hour ICO notification feasibility qualifier. Streamlined Subject Access Requests and Personal Data Breaches sections; full detail moved to Appendix 2 (SAR Policy) and Appendix 3 (Data Breach Policy). Appendix 1 (breach procedure) absorbed into Appendix 3. Added Appendix 4 (Data Breach Incident Report Form — staff use only).	Kelly Miller, DPO	4.0	31/03/2027

1. AIMS

Our Trust aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored, and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018) Data Protection Act 2018 (legislation.gov.uk), and the Data (Use and Access) Act 2025 (DUAA). The DUAA amends but does not replace the UK GDPR and DPA 2018; all three pieces of legislation apply to our processing activities.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. LEGISLATION AND GUIDANCE

This policy meets the requirements of the UK GDPR and the DPA 2018. It also takes account of the Data (Use and Access) Act 2025 (DUAA), which received Royal Assent on 19 June 2025 and amends the UK GDPR and DPA 2018 in a number of respects, including introducing new requirements around data protection complaints handling. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR guidance and resources | ICO and the ICO's Subject access requests (also known as SARs or right of access) | ICO.

Where our schools use CCTV, it reflects the ICO's CCTV and video surveillance | ICO for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

3. DEFINITIONS

Term	Definitions
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity.

Special categories of personal data	Personal data that is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina, and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. THE DATA CONTROLLER

Our schools process personal data relating to parents, pupils, staff, governors, visitors, and others, and is therefore a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. ROLES AND RESPONSIBILITIES

This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action. When referring to staff within this policy we also include directors, trustees, and governors.

5.1 Board of Trustees

The board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.
Our DPO can be contacted at dpo@learningat.uk.

5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing, and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK to countries without UK adequacy status
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - Considering using a new IT platform
    - If they need help with any contracts or sharing personal data with third parties, including drafting sharing agreements

6. DATA PROTECTION PRINCIPLES

The UK GDPR is based on data protection principles that our Trust and its schools must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant, and limited to what is necessary to fulfil the purposes for which it is

processed

- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

The LAT is responsible for demonstrating compliance with the UK GDPR principles.

This policy sets out how the Trust and its schools aim to comply with these principles.

6.1 Lawfulness, fairness, and transparency

We will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the vital interests of the individual, e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

The Data (Use and Access) Act 2025 also introduced a seventh lawful basis known as 'recognised legitimate interests'. This applies to certain specified categories of processing set out in Annex 1 of the UK GDPR as amended (such as safeguarding and network and information security), where a balancing test against individual rights is not required. The Trust will apply this basis where applicable once the relevant provisions are in force.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018. The conditions we rely on for processing this category of information are:

- Schedule 1, Part 1 – Employment, social security and social protection
- Schedule 1, Part 2, paragraph 6 — Statutory and government purposes
- Schedule 1, Part 2, paragraph 18 — Safeguarding of children and individuals at risk
- Other Schedule 1, Part 2 substantial public interest conditions as applicable

All special category data is stored securely and only individuals who require this information as part of their role will have access to this information.

6.2 Purpose limitation

We will only process personal data for specified, explicit, and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary. Staff must only process personal data where it is necessary in order to do their jobs.

6.3 Data minimisation

We will only use information that is relevant and necessary for the intended purpose. We will consider what information is required and not request any additional information.

6.4 Accuracy

We will ensure the information we process is kept up to date and accurate. Any inaccurate information will be amended as soon as possible.

6.5 Storage limitation

We will keep information for no longer than necessary. When staff no longer need the personal data, this must be deleted or anonymised in line with the LAT's Record Management Policy. If staff are unsure, they should speak with the DPO.

6.6 Integrity and Confidentiality (security)

We will ensure there are appropriate IT systems in place to make sure information is stored and processed securely. We have relevant policies and procedures in place to protect against data breaches.

6.7 Accountability

We have relevant measures in place to demonstrate our compliance when handling and processing personal data.

7. SHARING PERSONAL DATA

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we may seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud

- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the UK, or to countries not covered by UK adequacy regulations, we will do so in accordance with UK GDPR Chapter V and applicable UK transfer mechanisms.

8. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

Individuals have the right to make a subject access request (SAR) under Article 15 of the UK GDPR to access personal data held about them. The Trust is committed to handling all SARs promptly, lawfully, and in accordance with the UK GDPR, the Data Protection Act 2018 and the Data (Use and Access) Act 2025.
The following principles apply:

- Any individual — or a person acting on their behalf — may request access to personal data held about them. Requests can be made verbally or in writing to the DPO at dpo@learningat.uk
- The Trust will respond without undue delay and within one calendar month of receipt of the request. This period runs from the date of receipt of the request, not from the receipt of any supporting information.
- In responding to SARs, the Trust will conduct a reasonable and proportionate search of its records in line with the standard introduced by the Data (Use and Access) Act 2025.
- Where a request is complex or numerous, the response period may be extended by a further two months. The individual will be informed within one month of the extension and the reasons for it.
- Where a request is unfounded or excessive, the Trust may refuse to act or charge a reasonable fee. The individual will be told why and informed of their right to complain to the ICO.
- Full details of how the Trust handles SARs — including children's SARs, identity verification, exemptions, and the provision of data — are set out in Appendix 2 (Subject Access Request Policy).

In addition to the right to make a subject access request, individuals also have the following rights under UK GDPR: the right to rectification; erasure; restriction of processing; data portability; to object to processing; and not to be subject to solely automated decision-making. Individuals should contact the DPO at dpo@learningat.uk to exercise any of these rights. Individuals also have the right to make a data protection complaint to the Trust — see the Data Protection Complaints section of this policy.

9. PARENTAL REQUESTS TO SEE THE EDUCATIONAL RECORD

Parents, or those with parental responsibility, can access their child's educational record. These requests should be made through a Subject Access Request. Please see section 8.

10. CCTV

We use CCTV in various schools within the Trust to ensure they remain safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV. The lawful basis for CCTV processing is Article 6(1)(e) UK GDPR (public task) and, where images capture special category data, Article 9(2)(g) (substantial public interest). Each school within the Trust that uses CCTV maintains a record of its CCTV processing activity within the Trust's Records Management Policy.

CCTV footage is retained for no longer than 31 days unless it is required in connection with an ongoing investigation, complaint, or legal proceedings, in which case it will be retained until the matter is resolved. Access to CCTV footage is restricted to those with a legitimate need, such as the Headteacher, designated members of the leadership team, or the DPO. Footage will not be shared with third parties unless there is a legal obligation or clear lawful basis to do so. Individuals have the right to request access to footage in which they appear; such requests should be directed to the Headteacher of the relevant school and will be handled as a subject access request in accordance with section 8 of this policy. Any enquiries about the CCTV system should be directed to the Headteacher of the individual school.

13. PHOTOGRAPHS AND VIDEOS

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing, and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school magazines, brochures and newsletters.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will not distribute it further and if reasonably possible delete the photograph or video.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

14. DATA PROTECTION BY DESIGN AND DEFAULT

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably experienced DPO, and ensuring they have the necessary

resources to fulfil their duties and maintain their expert knowledge

- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies, and any other data protection matters; we will also keep a record of attendance
- Considering the needs and best interests of children in all data processing decisions relating to online services that children are likely to use, in line with obligations introduced by the Data (Use and Access) Act 2025
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. DATA SECURITY AND STORAGE OF RECORDS

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Portable electronic devices, such as laptops and hard drives that contain personal data are kept under password protection when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.
- On the rare occasion where personal information needs to be taken off site, staff must ensure this data is kept secure. Staff must minimise the risk by not taking paperwork offsite where possible.
- Passwords that are at least 12 characters long are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded

to change their passwords at regular intervals.

- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff, pupils or governors who access personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 7).

16. DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law. All disposal decisions will be taken in accordance with the LAT's Records Management Policy and Retention Schedule.

17. PERSONAL DATA BREACHES

The Trust takes the security of personal data seriously and will make all reasonable endeavours to prevent personal data breaches. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data — as defined in Article 4(12) UK GDPR.
The following principles apply:

- All staff must report any actual or suspected breach immediately to the DPO at dpo@learningat.uk, completing the Data Breach Incident Report Form (Appendix 4).
- The DPO will investigate, assess the risk, and determine whether the breach requires reporting to the ICO. Where reporting is required, the DPO will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the breach (Article 33 UK GDPR).
- Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the Trust will also notify those individuals directly without undue delay (Article 34 UK GDPR).
- All breaches — whether or not reported to the ICO — will be recorded in the Trust's breach register, with a record of the facts, effects, and action taken (Article 33(5) UK GDPR).
- Full details of the Trust's breach identification, reporting, and response procedure are set out in Appendix 3 (Data Breach Policy). The Data Breach Incident Report Form for staff use is at Appendix 4.

18. TRAINING

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19. MONITORING ARRANGEMENTS

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed and shared with the full governing board.

20. LINKS WITH OTHER POLICIES

This data protection policy is linked to our:

- Freedom of Information Policy
- Records Management Policy
- Appendix 2: Subject Access Request Policy
- Appendix 3: Data Breach Policy

21. DATA PROTECTION COMPLAINTS

The Data (Use and Access) Act 2025 (DUAA) introduced a new requirement, under section 164A of the Data Protection Act 2018, for data controllers to have a formal process for handling data protection complaints. This requirement comes into force on 19 June 2026. The following process is specific to complaints about the way in which Learning Academies Trust or its schools handle personal data. It is a standalone process and is separate from the Trust's general complaints procedure, which does not apply to data protection complaints.

What is a data protection complaint?

A data protection complaint is a complaint made by an individual (data subject) who believes that the Trust or one of its schools has handled their personal data in a way that infringes the UK GDPR or Part 3 of the Data Protection Act 2018. Examples may include concerns about how personal data has been collected, used, shared, stored, or disclosed, or a belief that a subject access request has not been handled correctly.

Not all correspondence that mentions personal data will constitute a data protection complaint. A general service complaint, a subject access request, or a grievance raised by a member of staff that happens to involve personal data is not, in itself, a data protection complaint for the purposes of this process.

How to make a data protection complaint

Data protection complaints should be submitted to the DPO in the first instance. Complaints can be made by email to dpo@learningat.uk . Complainants should set out clearly the nature of their concern, the personal data involved, and the outcome they are seeking.

How we will handle your complaint

We will acknowledge receipt of your complaint within 30 days of receiving it. We will then investigate the complaint without undue delay, making reasonable enquiries as necessary, and will keep you informed of progress. We aim to provide a full outcome within three months of receipt, unless the complaint is particularly complex, in which case we will write to you to explain the reason for any delay.

Our response will set out our findings and any steps we have taken or intend to take as a result of the complaint. Where we conclude that no breach has occurred, we will explain our reasoning. All responses will be written in plain and accessible language.

A record of all data protection complaints received, and the steps taken in response, will be maintained by the DPO. These records will be stored securely and will be made available to the ICO if required.

Escalation to the ICO

If you are not satisfied with the outcome of your complaint, or if you feel your complaint has not been dealt with adequately, you have the right to escalate the matter to the Information Commissioner's Office (ICO). The ICO is the UK's independent supervisory authority for data protection. We ask that you exhaust the internal process set out above before approaching the ICO, as this gives us the opportunity to address your concerns directly. The ICO can be contacted at www.ico.org.uk, by telephone on 0303 123 1113, or by post at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

In line with the requirements of the Data (Use and Access) Act 2025, this data protection complaints process will be clearly signposted in the Trust's and schools' privacy notices and made accessible via school websites. Individuals who are unsure whether their concern falls within this process should contact the DPO at dpo@learningat.uk for guidance.

22. APPENDIX 2: SUBJECT ACCESS REQUEST POLICY

1. Overview

Under Article 15 of the UK General Data Protection Regulation (UK GDPR), individuals have the right to access personal data held about them. This right is known as a Subject Access Request (SAR). The Trust has a legal obligation to respond to all valid SARs in accordance with the UK GDPR, the Data Protection Act 2018 (DPA 2018), and the Data (Use and Access) Act 2025 (DUAA). In responding to SARs, the Trust will conduct a reasonable and proportionate search of its records, in line with the standard introduced by the DUAA.

Individuals are entitled to receive:

- Confirmation of whether their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or the criteria used to determine this
- The source of the data, if not the individual themselves
- Whether any automated decision-making is applied to their data, and the significance and consequences of this

It is equally important that in processing SARs, data belonging to third parties (including other children), data that could cause serious harm, or data covered by legal professional privilege is not inadvertently disclosed. Exemptions will be applied strictly in accordance with Schedule 2 of the DPA 2018 and Article 23 UK GDPR.

The Data (Use and Access) Act 2025 introduced a revised standard for responding to subject access requests, requiring the Trust to conduct a reasonable and proportionate search of its records rather than an exhaustive one. This means the Trust is not obliged to search every possible system or location where data may theoretically exist, but must take reasonable and proportionate steps to locate the information requested, having regard to the nature of the request and the likely locations of relevant data

2. Children and Subject Access Requests

Personal data about a child belongs to that child, not to their parents or carers. Children below the age of 12 are generally not regarded as being mature enough to understand their rights and the implications of a SAR. Most requests from parents or carers of pupils below that age may therefore be granted without the express permission of the pupil. This is not an absolute rule; a child's ability to understand their rights will always be assessed on a case-by-case basis.

Where a child has sufficient capacity and maturity, they are entitled to the same rights of subject access as an adult. A parent or carer who wishes to make a SAR on behalf of a child with capacity should be informed that the Trust will respond directly to the child if the child makes a SAR in their own right.

Where a SAR is made by a person with parental responsibility who does not have primary care responsibility, the person with primary care responsibility may be notified that a request has been

made. The Trust will respond in accordance with the UK GDPR. If the person with primary care responsibility seeks to limit the response, further legal advice may be sought.

The right to request access to a child's personal data is not absolute and must be balanced with the child's own rights. Particular care will be given to the child's right to privacy in relation to personal opinions or emotional content. Where disclosure would compromise the rights and freedoms of the child, certain content will be withheld, consistent with Section 45 of the DPA 2018.

3. Recognising a SAR

All staff are responsible for recognising SARs, whether or not they are expressly described as such. A SAR may be embedded within a complaint, a general enquiry, or a request for copies of records. All staff must immediately forward any request they believe may be a SAR to the Data Protection Officer.

Examples of SARs include: a parent requesting all records relating to their child; an employee asking for copies of their HR file; or an individual requesting all correspondence mentioning their name.

4. Responding to SARs

The Trust is committed to verifying the identity of the person making a SAR where there is reasonable doubt about their identity. Identity verification is a proportionate measure and will not be used as a blanket barrier to processing requests.

Where identity verification is sought, the Trust may request:

- Two forms of identification, such as a valid photo ID and a recent utility bill (within three months) and/or change of name documents
- Where the request is made on behalf of a child, confirmation of the relationship — for example a birth certificate, adoption or fostering records
- The Trust may also contact the individual by telephone to verify the request was made, ordinarily within 24 hours of receipt, where this is proportionate to do so

If the requester does not provide identity information when asked, the Trust will not process the request further until it has sufficient confidence in the requester's identity. Where this occurs the individual will be informed.

5. Processing SARs

SARs will be responded to within one calendar month of receipt of the request. If a request is complex, numerous, or requires a particularly extensive search, this period may be extended by a further two months. The individual will be notified within one month of the extension and the reasons for it.

If the information requested contains data relating to a third party, that data will be redacted before disclosure unless consent has been obtained from the third party or it is reasonable to provide the information without consent.

Information the Trust will not disclose in response to a SAR includes:

- Information that may cause serious harm to the physical or mental health of the pupil or another individual

- Information that would reveal that a child is at risk of abuse, where disclosure would not be in the child's best interests
- Information contained in adoption or parental order records
- Information given to a court in proceedings concerning the child

Any information previously held may have already been disposed of in accordance with the Trust's Records Management Policy. Where this is the case, the individual will be informed.

Responses will be provided free of charge. Where requests are unfounded or excessive — for example where they are repetitive or requests further copies of the same information — the Trust may apply a reasonable administrative charge or refuse to comply. Any refusal will be explained in writing, and the individual will be informed of their right to complain to the ICO.

6. Exemptions from SARs
Two categories of exemption may apply to personal data processed by the Trust:

Category A — Qualified exemptions (harm/prejudice test applies):

Exemption or Data Type	
Health data	Disclosure may be restricted if it would cause serious harm.
Social work data	Exemptions apply if disclosure may cause serious harm to physical or mental health.
Educational records	Third-party content may be redacted with justification.
Child abuse data	Exempt if disclosure would prejudice investigation or cause harm.
Risk of serious harm (safeguarding)	Applies to disclosures affecting health or safety of the data subject or others.
Crime and taxation	Exempt where disclosure would prejudice law enforcement functions.
Third-party data	May be withheld under Article 15(4) UK GDPR if it affects others' rights.

Category B — Absolute exemptions (automatic, no harm test required):

Exemption or Data Type	
Legal professional privilege	Do not disclose legally privileged advice or documents.
Confidential references given by the	Absolute exemption — do not disclose references

Trust	written by the Trust.

All exemption decisions will be made on a case-by-case basis and documented.

7. Providing Data

Data that can lawfully be shared will be provided either in hard copy or electronically, according to the individual's preference as stated in their request.

Where data is provided in hard copy, the individual will be required to collect it in person and confirm their identity at the point of collection, using the same identification provided with the original request.

Where data is provided electronically, it will be sent via a password-protected secure link. The password will be communicated separately from the data.

8. Declining Requests

Where the DPO considers that a SAR does not satisfy the criteria for disclosure, the Trust may decline the request in the best interests of the individual or in accordance with applicable exemptions.

The individual will be notified in writing within the one-month response period, with an explanation of why the request has been declined and details of their right to complain to the Information Commissioner's Office (ICO). If the individual remains dissatisfied, they may complain to the Trust using the Data Protection Complaints process set out in the main policy, or contact the ICO directly at www.ico.org.uk or on 0303 123 1113.

23. APPENDIX 3: DATA BREACH POLICY

1. Overview and Scope

This policy sets out the Trust's approach to detecting, assessing, managing, and reporting personal data breaches, in accordance with Articles 33 and 34 of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), and the Data (Use and Access) Act 2025 (DUAA).

This policy applies to all staff employed by Learning Academies Trust (LAT), including governors, volunteers, and work experience students, and to all contractors, third-party companies, and agencies who process personal data where the LAT is the data controller or has an interest in the personal data affected.

2. Definitions

Term	
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (Article 4(12) UK GDPR).
DPO	Data Protection Officer — the appointed person responsible for overseeing data protection compliance and managing breach response.
Data controller	The legal person, public authority, or body that determines the purposes and means of processing personal data.
Data processor	A person or body that processes personal data on behalf of the data controller.
Data subject	An identified or identifiable natural person to whom personal data relates.
Supervisory authority	The Information Commissioner's Office (ICO).

3. Types of Personal Data Breach

A personal data breach occurs when personal data has been lost, destroyed, corrupted, or disclosed without authorisation, or where access to it has been prevented and this has a negative effect on individuals.

Breaches fall into three categories:

Type	Category	Examples
Confidentiality breach	Unauthorised or accidental disclosure or access	Sending personal data to the wrong recipient; unauthorised access to records

	to personal data	
Integrity breach	Unauthorised or accidental alteration of personal data	Data input errors; unauthorised modification of records
Availability breach	Unauthorised or accidental loss of access to or destruction of personal data	Ransomware; accidental deletion; hardware failure

Common breach scenarios include: malware or hacking; physical theft or loss of devices; unescorted visitors in secure areas; non-secure disposal of hardware or paperwork; unauthorised disclosure; data input errors; and inappropriate sharing of personal data.

4. Responsibilities

The Trust takes stringent steps to prevent personal data breaches and reviews its processes annually. All staff are responsible for:

- Taking precautionary measures and being vigilant when handling personal data
- Adhering to the Trust's data protection policies and procedures
- Participating in regular data protection training
- Reporting any actual or suspected breach immediately — without undue delay — to the DPO, regardless of whether the breach was caused by themselves or identified from another source

Any data processor engaged by the Trust who becomes aware of a personal data breach must notify the Trust's DPO without undue delay, in accordance with Article 33(2) UK GDPR. Staff should not report a breach directly to the ICO or to affected data subjects without first consulting the DPO.

5. Identifying and Reporting a Breach

Although procedures are in place to prevent breaches, some will occur. On finding or causing a breach, or a potential breach, the staff member or data processor must:

- Notify the DPO immediately by email to dpo@learningat.uk
- Complete the Data Breach Incident Report Form (Appendix 4) with as much detail as possible, including: the date of the incident; the date it was discovered; the type of data affected and to whom it belongs; who has been affected and how many individuals; and a full description of the breach
- Take any immediate steps available to contain the breach, pending DPO instruction

The DPO will then investigate the breach, carry out a risk assessment, and advise on further containment steps.

6. Assessing the Risk and Deciding Whether to Report

The DPO will assess the severity of the breach and its likely impact on individuals. The statutory test

for whether a breach must be reported to the ICO is whether it is likely to result in a risk to the rights and freedoms of natural persons (Article 33(1) UK GDPR). The test for notifying individuals directly is the higher threshold of high risk to their rights and freedoms (Article 34(1) UK GDPR).
In assessing the risk, the DPO will consider whether the breach is likely to result in:

- Loss of control over personal data
- Discrimination, identity theft or fraud
- Financial loss or damage to reputation
- Physical, material, or non-material damage to individuals
- Particular risk to vulnerable individuals, including children

Where the breach is assessed as low risk and unlikely to affect the rights and freedoms of individuals, no report to the ICO is required. A record must still be made of the breach and the reasons for the decision not to report.

7. Reporting to the ICO

Where a breach must be reported, the DPO will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it, via the report a breach tool on the ICO website at ico.org.uk. If all required information is not available within 72 hours, the DPO will submit an initial report explaining the delay and provide further information as soon as it becomes available, in accordance with Article 33(4) UK GDPR.

The report to the ICO will include, as far as is known:

- A description of the nature of the breach, including the categories and approximate number of individuals and records affected
- The name and contact details of the DPO
- A description of the likely consequences of the breach
- A description of the measures taken or proposed to address the breach and mitigate its effects

8. Notifying Individuals

Where the breach is likely to result in a high risk to the rights and freedoms of the affected individuals, the DPO will notify those individuals directly, without undue delay, in accordance with Article 34 UK GDPR. The notification will describe:

- The name and contact details of the DPO
- The likely consequences of the breach
- The steps taken or proposed to address the breach and mitigate its effects

If notifying individuals directly would involve disproportionate effort, the Trust may instead make a public communication or similar measure, subject to ICO guidance.

9. Containment Actions

The Trust will take proportionate action to contain and minimise the impact of any breach. The

following specific actions will be taken where relevant:

Where special category data is accidentally disclosed by email to unauthorised individuals:

- The sender must attempt to recall the email immediately
- Staff who receive personal data in error must alert the sender and the DPO without delay
- If recall is not possible, contact will be made with the unauthorised recipients, explain the error, and request deletion and non-disclosure
- Written confirmation from all recipients will be obtained that they have complied
- The DPO or ICT department will carry out an internet search to check the data has not been published; if it has, the publisher will be contacted and asked to remove it

Where personal data is accidentally published on the school website:

- The individual responsible must remove the data from the website immediately
- The DPO must be alerted without delay
- If the individual is unable to remove the data themselves, the LAT IT department must be contacted immediately

Where non-anonymised personal data is shared with governors in error:

- The DPO must be alerted immediately
- All governors must be contacted, asked to delete any files, and informed the data was sent in error
- The DPO will obtain written confirmation from all governors that they have complied

10. Recording Breaches

All breaches must be documented by the DPO, irrespective of whether they are reported to the ICO, in accordance with Article 33(5) UK GDPR. The breach register will record:

- The facts and cause of the breach
- The effects and likely consequences
- The action taken to contain the breach and prevent recurrence
- Whether the breach was reported to the ICO and/or notified to individuals, and the reasons for the decision

Records will be stored securely and made available to the ICO on request.

11. Review and Follow-up

Following any breach, the DPO, CEO, and Headteacher will meet as soon as reasonably practicable to review what happened and what steps can be taken to prevent recurrence. The Trust's processes and procedures will be reviewed annually. This policy may be amended from time to

time in accordance with updates to the UK GDPR, DPA 2018, and DUAA.

If an individual believes their personal data has been mishandled in connection with a breach, they may use the Trust's Data Protection Complaints process set out in the main policy, or contact the ICO directly.

24. APPENDIX 4: DATA BREACH INCIDENT REPORT FORM

For internal staff use only. This form must be completed and submitted to the DPO at dpo@learningat.uk as soon as possible after a breach is identified. The form is for reporting purposes within Learning Academies Trust and is not for completion by parents, pupils, or members of the public.

The full version of this form, including the DPO's risk assessment section (Section 2), is maintained as a separate working document by the DPO and is available from dpo@learningat.uk.

Section 1 — To be completed by the member of staff reporting the breach:

Section 1

Date of Report:	Date of Incident:
Date made aware of Incident	Reason for delay, if applicable:
Reported by:	Reported to: DPO
What type of data has been breached and to whom does it belong?	
Who has potentially been affected by this breach and how many?	
Please give a description with as much detail as possible of the breach:	
The risk assessment and investigation into this breach may be compromised if there is a failure to report a true and accurate account of the breach. This may lead to further investigation. By signing this you are confirming the details that have been given are accurate to the best of your knowledge and you should update this report at the earliest opportunity should further details emerge.	
Name: Signed: Date:	

Section 2 of the form will be completed by the DPO. The DPO will assess: whether the breach has affected confidentiality, integrity, or availability of personal data; containment steps taken; risk to the rights and freedoms of individuals (including vulnerability of those affected); whether ICO notification is required; whether individual notification is required; and the final outcome and rationale. A full record will be maintained in the Trust's breach register.