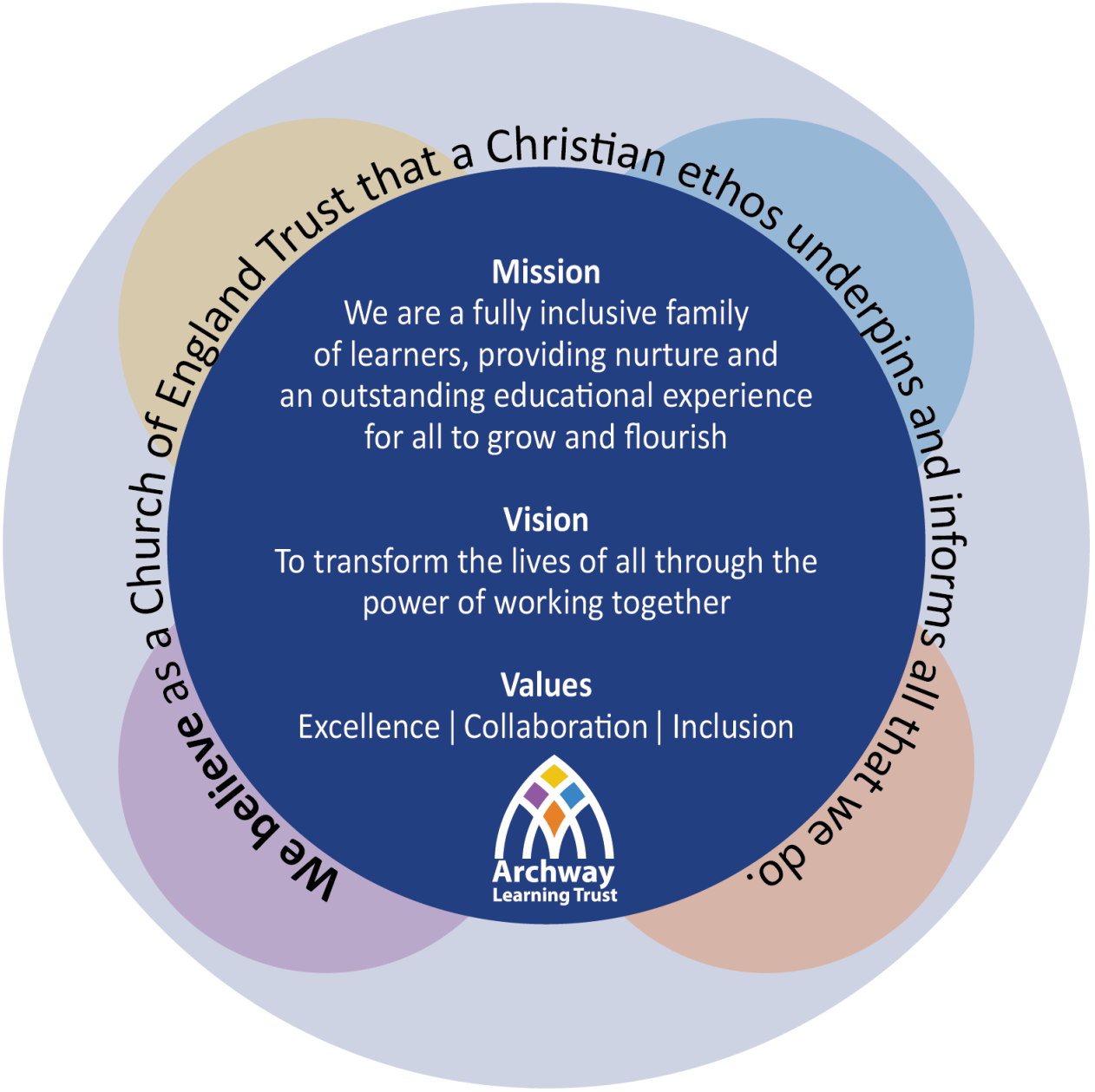
Archway Learning Trust

Data Protection Policy

Approved:	**November 2023**
Review date:	**November 2026**
Responsible Officer:	**Chief Corporate Services Officer**

Trust Ethos, Mission, Vision and Values

The Trust believes in the transformational power of education for each individual and that this is enhanced through collaborative working between the academies.



Working together, transforming lives

Contents

Para	
1	Policy Statement
2	Scope and Principles
3	Data Protection Officer
4	Conditions of Processing
5	Individual Rights
6	Security of Personal Data
7	Data Breaches
8	International Data Transfers
9	Individual Responsibilities
10	Training
11	Data Protection Impact Assessments

Where the word 'Trust' is used in this document it refers to Archway Learning Trust.

Where the word 'Advisory Board' is used it refers to the Academy Advisory Board (AAB) of an individual academy within the Trust.

The term 'Trust Executive Leadership Team' (ELT) comprises, the Chief Executive Officer, Chief Operating Officer, Chief People Officer, Chief Finance Officer, Chief Corporate Services Officer, Directory of Primary Education, Director of Secondary Education and Directory of Technology & Insights.

Where the word 'users' is used it refers to staff, future staff issued with ICT access and/or hardware, AAB members, volunteers and regular visitors.

Where the phrase 'Senior Leader' is used, this refers to the ELT, Principals, Headteachers or Business Service Directors within the Trust.

Where the phrase 'Principal' is used, this also refers to Headteachers.

Related Policies and Procedures

- Biometric Policy
- Freedom of Information Policy
- Charging Policy
- Health, Safety and Security Policy
- ICT Acceptable Use Policy
- Code of Conduct
- Safeguarding Policy
- Social Media Policy
- Privacy Notices
- Publication Scheme
- Records Management – Retention & Destruction Policy

1. Policy Statement

1.1. This policy applies to all personal data, statutory records and organisational records held by Archway Learning Trust. It encompasses paper records, data held on computers and associated equipment either owned by the Trust or on personal devices, including CCTV and biometric identifiers, used by or on behalf of the Trust.

1.2. The Trust is committed to being open and transparent about how it collects and uses the personal data of staff, students, parents and visitors and to fulfilling its obligations defined in law.

1.3. The obligations outlined in this policy apply to all those who have access, or have had access to personal data irrespective of whether they are employees, Trustees, AAB members, employees of associated organisations with whom we share personal data as well as temporary, agency staff.

2. Scope and Principles

2.1.1. The Trust processes personal data in accordance with the principles of data protection defined in Article 5(1) of the UK GDPR 2016:

2.1.2. The Trust processes personal data **lawfully, fairly** and in a **transparent manner** via the use of Privacy Notices and communications with data subjects.

2.1.3. The Trust processes personal data only for **specified, explicit** and **legitimate** purposes.

2.1.4. The Trust processes personal data only where it is **adequate, relevant** and **limited to that necessary** for the purpose of processing.

2.1.5. The Trust maintains accurate records and takes **all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay**. The Trust will promptly update its records when it becomes aware of individual's personal information having changed or where found to be inaccurate. In circumstances where the accuracy of held information is disputed, the Trust will take all reasonable steps to establish accurate records and update these records as necessary.

2.1.6. The Trust **keeps personal data only for the period necessary** for processing.

2.1.7. The Trust adopts appropriate measures to make sure that personal data is **secure** and protected against unauthorised or unlawful processing, accidental loss, destruction or damage.

2.1.8. The Trust maintains **accountability** for its compliance with data protection law and regulatory guidance as per Article 5(2).

2.2. The Trust will inform individuals of the reasons for processing their personal data, how it uses such data and the lawful basis for processing via privacy notices.

2.3. Special Category information (including but not limited to; information relating to race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sexual orientation or biometric data for purposes of identifying a natural person) is given special protection, and additional safeguards apply if this information is to be collected or used.

2.4. Personal data gathered for staff and students is routinely held in the individual's personal file and on MIS systems. The Trust retains a record of its processing activities for staff and students in accordance with the requirements of the UK General Data Protection Regulation (UK GDPR).

2.5. The Trust may hold personal information in relation to other individuals who have contact with the academies, such as volunteers and guests. Such information shall be held in accordance with the GDPR principles and shall not be kept longer than necessary.

3. Data Protection Officer

3.1. We are required to appoint a Data Protection Officer ("DPO") for Archway Learning Trust. Our DPO can be contacted at: DPO@archwaytrust.co.uk.

3.2. The DPO is the central contact for queries relevant to data protection and is responsible for compliance with data protection law as well as this policy. For queries about the application of this policy or if concerned that the policy has not been followed, such queries should be referred in the first instance to the DPO.

3.3. The Trust's network of local, academy-based Data Protection Leads (DPL's) work closely with the DPO and individual academy queries should first be raised with the local DPL.

4. Conditions of processing

4.1. The Trust processes personal, special category data and criminal data, where necessary for various reasons as defined in Article 6, 9 and 10 of the UK GDPR 2016, the processing of all such data must be lawful with one or more of the below lawful bases being applied:

4.1.1. The individual consents to the processing of their personal data and that consent is explicit, unambiguous and freely given by the data subject.

4.1.2. Processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of working towards entering into a contract with the individual, at their request.

4.1.3. Processing is necessary to comply with a legal obligation e.g. the Education Act 2011 or laws relevant to safeguarding.

4.1.4. Processing is necessary to protect the vital interests of an individual which may apply in medical emergencies where the data subject is unable to consent to the processing due to the emergency. We expect this will only occur in very specific and limited circumstances; in such circumstances staff should consult with the DPO in advance, though there may be emergency situations where this does not occur.

4.1.5. Processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the Trust.

4.1.6. Processing is necessary for a legitimate interest of the Trust or that of a third party, except where this interest is overridden by the rights and freedoms of individual concerned.

4.2. When special category data is processed, an additional legal justification applies as per Article 9 UK GDPR. Due to the increased risk of processing special category data the Trust will generally process such data reliant on the following lawful basis:

4.2.1. Where processing is necessary for employment law purposes, such as relating to sickness absence or to conduct investigations for disciplinary procedures.

4.2.2. Where processing is necessary for reasons of substantial public interest, such as in support of equality of opportunity and treatment.

4.2.3. Where processing is necessary for health or social care purposes, such as support for pupils and staff with medical conditions or disabilities.

4.2.4. Where none of the above apply then we will seek explicit, opt in consent for the data subject to process special category data.

4.3. Consent collection is required when pupils or our workforce join the Trust. Third parties such as parents or visitors on site may also be required to complete a consent form where appropriate.

4.4. For all pupils under the age of 13 years old we will seek consent from an individual with parental responsibility for that pupil.

4.5. We will generally seek consent directly from a pupil where they have reached the age of 13. In some circumstances however, such as in the case of biometric data processing it is acknowledged that such processing requires consent from individuals aged 18 or above and therefore the Trust will seek consent from an individual with parental responsibility.

4.6. There are requirements when collecting a valid consent form. Where consent is required for the processing of personal data, the Trust will fulfil its obligation to be transparent by:

4.6.1. Informing data subjects of the proposed data processing via a privacy statement.

4.6.2. Seeking "opt in" consent. The Trust will not ask for data subjects to opt out, nor will it provide pre-filled tick boxes.

4.6.3. Inform data subjects on how they can withdraw consent and who to contact.

4.6.4. Consent must be freely given and as such the Trust will endeavour to separate consent from other terms and conditions and will not generally be a precondition of signing up to a service or to receive goods.

4.7. Consent records must be retained, including how and when consent was collected. Evidence of consent will be held securely for the period necessary to process personal data and to manage data subject rights requests.

5. Individual Rights

5.1. Individuals have a number of rights related to how their personal data is processed as defined in Articles 13 to 23 of the GDPR:

5.1.1. **Subject Access Requests (SAR)** – Data subjects have the right to access personal data we hold about them. Where an individual makes a request for access it will be considered and responded to in accordance with Article 15 UK GDPR.

5.1.2. The Trust will usually deal with a SAR free of charge however a fee may be imposed if a request is considered to be manifestly unfounded or excessive. Alternatively, we may refuse to respond if considered to be manifestly unfounded or malicious in intent. In such cases the Trust will inform the requestor why this decision has been reached.

5.1.3. A fee may be imposed in response to requests for copies of information already provided. In these circumstances a reasonable fee may be imposed based on administrative costs in providing copies of information.

5.1.4. Individuals have a number of other rights under the GDPR and can request that the Trust:

- Rectify inaccurate personal data having assessed and satisfied itself that held information requires updating or amendment to ensure accuracy, this is known as a request for **Rectification** as per Article 16;
- Erase personal data which is no longer necessary for the purpose it was originally collected for, known as a request for **Erasure** as per Article 17;
- Limit the processing of personal data, generally for a specific, limited period of time in cases where the accuracy of data or lawfulness of processing is contested, this is known as a request to **Restrict processing** as per Article 18;
- Seek personal data in a machine readable format for the purpose of transmitting information to another organisation, this is known as a **Data Portability** request as per Article 20;
- Object to the processing of personal data in certain circumstances such as where processing is done in the public interest, for a legitimate interest of the Trust or in cases of direct marketing, this is known as a request to **Object to processing** as per Article 21;
- Object to data processing by solely automated means; this right applies in cases where automation results in data processing or profiling without any human intervention. This is captured under **Rights related to Automated Decision Making and Profiling** as per Article 22. Such processing is extremely rate and consent will be sought where such processing is being considered;
- The **Right to be Informed** is also defined under Articles 13 – 14 and provides that data subjects are provided clear, concise information about how we process their personal data and which is covered via use of Privacy Notices.

5.1.5. We will aim to process "live" Data Subject Rights requests (DSR) within one calendar month. A DSR however will only become live from the date that the following tasks have been completed:

- All necessary identification has been verified, for both the requestor and/or data subject(s);
- Authorisation of the requestor to manage the data subject rights of the data subject has been confirmed;
- Payment of any required fee.

5.1.6. In cases where a requestor's identity or authorisation to make a request is in doubt, the deadline for processing such requests will not begin until the required evidence has been obtained, and where a third party is involved, the written authorisation from the data subject has been confirmed (see below in relation to sharing information with third parties).

5.1.7. The one month period afforded for DSRs may be extended by a further two calendar months where such requests are complex or volumous in nature. What constitutes a complex request will depend on the particular nature of the request and requestors will be notified about any extensions prior to the initial deadline.

6. Security of personal data

6.1. The Trust will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. It will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

6.2. The Trust will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this policy and their duties under the UK GDPR. The Trust will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

6.3. For especially sensitive data such as CCTV imagery or biometric identifiers processed by the Trust, it will take appropriate steps to assess and implement appropriate security standards and procedures necessary to ensure the protection and security of these sensitive, criminal or biometric datasets at all times.

6.4. For more information on how the Trust processes biometric data of students and staff, please refer to the ALT Biometric Information Policy. Alternatively please contact the Trust via the contact information provided in Section 3.

7. Data breaches

7.1. If the Trust discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner's Office (ICO) within 72 hours of discovery. The Trust will record all data breaches regardless of their effect.

7.2. If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

8. International Data transfers

8.1. If the Trust discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner's Office (ICO) within 72 hours of discovery. The Trust will record all data breaches regardless of their effect. The Trust will not normally transfer personal data to countries outside the European Economic Area (EEA).

8.2. Personal data may be transferred to countries outside the EEA on rare occasions. Any such data transfers shall be made to the data host on the basis of a legally binding contract or data processors will provide assurance beforehand that their processing adheres to the UK GDPR.

9. Individual responsibilities

9.1. Individuals are responsible for helping the Trust keep their personal data up to date. Individuals should let the Trust or individual academy within the Trust know if data provided changes.

9.2. Individuals may have access to the personal data of other individuals in the course of their employment or contract with the trust. Where this is the case the Trust relies on individuals to help meet its data protection obligations to staff and students. Individuals who have access to personal data are required:

9.2.1. to access only data that they have authority to access and only for authorised purposes;

9.2.2. not to disclose data except to individuals or artificial intelligence (whether inside or outside the Trust) who have appropriate authorisation;

9.2.3. not to remove personal data or devices containing or that can be used to access personal data, from the Trust's premises without adopting appropriate security measures (such as encryption, password protection and secure travel document bag) to secure the data and the device;

9.2.4. not to store personal data on local drives or on personal devices that are used for work purposes.

10. Training

10.1. The Trust will provide guidance to all individuals about their data protection responsibilities. Data handlers will be provided with training as part of their induction and every two years thereafter as a minimum.

11. Data Protection Impact Assessments

11.1. The Trust takes data protection seriously and will consider, comply with the requirements of Data Protection law in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

11.2. In certain circumstances the law requires us to carry out detailed assessments of proposed processing. This includes where we intend to use new technologies which might pose a high risk to the rights of data subjects because of the types of data we will be processing or the way that we intend to do so.

11.3. The Trust will complete an assessment of any such proposed processing and has a template document which ensures that all relevant matters are considered. The DPO or an appropriate Data Protection lead should always be consulted as to whether a data protection impact assessment is required prior to procurement of a new service or technology involving the processing of personal data.