Arthur Terry Learning Partnership

Together we are stronger

ATLP
Data Protection Policy

Author/Contact:	Katie Astbury Email: katie.astbury@atlp.org.uk	
Document Reference:	ATLP Data Protection / GDPR Policy	
Version	02	
Status	FINAL	
Updated	December 2022 July 2020	
Related Policies	• CCTV Policy • Protection of Biometric Information Policy • Freedom of Information Policy • ATLP GDPR Pupil Privacy Notice • E-safety policy	
Updates/ Key changes	• Removal of reference to EU • Addition of Biometrics policy as a related policy • Updated DPO • Changed governors to advocates • Updated consent for SARs for children over the age of 12 • Updated data retention guidelines	
Review Date/Frequency	Review January 2025	
Approved/Ratified By	ATLP Trust Board	30 Jan 2023

Contents

1. Aims

The Arthur Terry Learning Partnership aims to ensure that all personal data collected about staff, pupils, parents, advocates, trustees, members, visitors and other individuals is collected, stored and processed in accordance with the legal obligations under the GDPR. During our activities as an academy trust, we will collect, store and process personal data about our pupils, workforce, parents and others. This makes us a data controller in relation to that personal data.

This policy is in place to ensure all staff, trustees and advocates are aware of their responsibilities and outlines how each school complies with the following core principles of the GDPR.
Organisational methods for keeping data secure are imperative, and the Arthur Terry Learning Partnership (ATLP) believes that it is good practice to keep clear practical policies, backed up by written procedures.

We are committed to the protection of all **personal data** and **special category personal data.**

2. Legal Framework

This policy meets the requirements of the:

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

This policy is based on guidance published by the Information Commissioners Office (ICO) on the Guide to the UK General Data Protection Regulation (UK GDPR) | ICO

This policy will be implemented in conjunction with the following other school policies:

- CCTV Policy
- Protection of Biometric Information Policy
- Freedom of Information Policy
- ATLP GDPR Pupil Privacy Notice
- E-safety policy

3. Definitions

For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g., an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g., key coded.

Sensitive personal data is referred to in the GDPR as 'special categories of personal data,' which are broadly the same as those in the Data Protection Act (DPA) 2018. These specifically include the processing of genetic data, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, biometric data, sex life or sexual orientation and data concerning health matters – physical or mental.

Processing is anything related 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 is 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 is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. 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. The DPO will report to the highest level of management at the school, which is the Chief Executive Officer for the ATLP.

The DPO will provide an annual report of their activities directly to the Board of Trustees and, where relevant, report to the board their advice and recommendations on data protection issues.

The DPO will be an existing employee that has been appointed to the role, provided that their duties are compatible and do not lead to a conflict of interests.

DPO for ATLP is **Katie Astbury** and is contactable via **DPO@atlp.org.uk**

The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.

The DPO will operate independently and will not be dismissed or penalised for performing their task. Sufficient resources will be provided to enable them to meet their GDPR obligations.

The DPO is also the first point of contact for individuals across the trust and will:

- Inform and advise schools and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor each school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

5. Roles and Responsibilities

This policy applies to all staff employed within the partnership and to external organisations or individuals working on our behalf.

The Board of Trustees has overall responsibility for ensuring that our schools comply with all relevant data protection obligations.

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

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing each individual school of any changes to their personal data, such as change of address
- Contacting the DPO in the following circumstances:
    - Any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - Any concerns that this policy is not being followed
    - If they are unsure whether or not, 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
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data Protection Principles

In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those 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; every reasonable step must be taken to ensure that personal data that is inaccurate, to the purposes for which they are processed, are erased, or rectified without delay.
- Kept for no longer than is necessary for the purposes of which it is obtained.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

7. Collecting Personal Data

Lawfulness, fairness and transparency

The legal basis for processing data will be identified and documented prior to data being processed.

Processing relates to personal data manifestly made public by the data subject

Under GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained (i.e. the individual or their parent or carer when appropriate in the case of a student has freely given clear consent)
- Processing is necessary for:
  1. Compliance with a legal obligation.
  2. The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
  3. For the performance of a contract with the data subject or to take steps to enter a contract.
  4. Protecting the vital interests of a data subject or another person.
  5. For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

For special categories of personal data, we will also meet one of the special category conditions for processing under the data protection law:

- The individual (or their parent or carer) has given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims
- The data needs to be processed for reasons of substantial public interest as defined in legislation
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Reasons of substantial public interest which is proportionate to the aim pursued and which contains appropriate safeguards.
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes.

8. Consent

- Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.
- Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.
- Where consent is given, a record will be kept documenting how and when consent was given.
- The ATLP ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.
- Existing consents will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the Data Protection Act (DPA) will not be reobtained.
- Consent can be withdrawn by the individual at any time.
- Where a child is under the age of 16 **(or younger if the law provides it (up to the age of 13)** the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

9. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations 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 will 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 UK data protection law
    - Establish a contract with the supplier or contractor 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

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

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

We may also share personal data under the Keeping Children Safe in Education requirements to ensure that safeguarding is always paramount.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

10. Rights of Individuals

The right to be informed

The privacy notice supplied to individuals regarding the processing of their personal data will be written in clear, plain language, which is concise, transparent, easily accessible and free of charge.

If services are offered directly to a child, the school will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.
- The existence of the data subject's rights, including the right to:
    - Withdraw consent at any time.
    - Lodge a complaint with a supervisory authority.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the categories of personal data that each school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data is disclosed.
- If the data used to communicate with the individual, at the latest, when the first communication takes place.

The right of access

Individuals have the right to obtain confirmation that their data is being processed.

Individuals have the right to submit a **Subject Access Request (SAR)** to gain access to their personal data in order to verify the lawfulness of the processing.

Each school will verify the identity of the person making the request before any information is supplied.

Where a child is **over the age of 12 (Year 9 and above)** and competent and mature to understand their rights, the SAR must be requested by the child. The child may authorise someone else, other than a parent or guardian, to make a SAR on their behalf.

A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within **one month** of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, each school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

If a large quantity of information is being processed about an individual, each school will ask the individual to specify the information the request is in relation to.

Requests for an educational record

The Education (Pupil Information) (England) Regulations 2005, states that the pupil record must be provided to parents within 15 school days of a request where the pupil is enrolled in a maintained school. This provision does not apply to Academies, independent schools.

The right to rectification

1. Individuals are entitled to have any inaccurate or incomplete personal data rectified.
2. Where the personal data in question has been disclosed to third parties, each school will inform them of the rectification where possible.
3. Where appropriate, each school will inform the individual about the third parties that the data has been disclosed to.
4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.
5. Where no action is being taken in response to a request for rectification, each school will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

Each school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and then later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, each school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

The right to restrict processing

Individuals have the right to block or suppress each school's processing of personal data.

If processing is restricted, each school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

Each school will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school/DPO has verified the accuracy of the data
- Where an individual has objected to the processing and the school/DPO is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful, and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data, but the individual requires the data to establish, exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, each school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

Each school will inform individuals when a restriction on processing has been lifted.

The right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form.

Each school will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual.

Each school is not required to adopt or maintain processing systems which are technically compatible with other organisations.

If the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.

Each school will respond to any requests for portability within one month.

Where the request is complex, or several requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, each school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to object

Each school will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her situation.
- Each school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate

compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- Each school will stop processing personal data for direct marketing purposes as soon as an objection is received.
- Each school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes: the individual must have grounds relating to their situation in order to exercise their right to object.

11. Privacy by design and Privacy impact assessments

The Arthur Terry Learning Partnership will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities.

A DPIA will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow each school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Arthur Terry Learning Partnership's reputation which might otherwise occur.

A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA will be used for more than one project, where necessary.

High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV.

The Arthur Terry Learning Partnership will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, each school will offer a method for individuals to object online.

Where a DPIA indicates high risk data processing, the DPO will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

12. Personal data breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

The Headteacher in each school will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training, are aware of their school's GDPR contact and the requirement to report all breaches to the GDPR contact and/or DPO directly.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

All reportable breaches will be reported to the Information Commissioners Office (ICO) within 72 hours of the school/DPO becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the ICO, will be assessed on a case-by-case basis.

If a breach is likely to result in a high risk to the rights and freedoms of an individual, the school/DPO will notify those concerned directly.

A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the ICO.

If a breach is sufficiently serious, impacted individuals will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at each school, which facilitate decision-making in relation to whether the ICO or the impacted individuals need to be notified.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

13. Data Security and data retention

- Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.
- Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
- Memory sticks will not be used to hold personal or sensitive information.
- All electronic devices are password-protected to protect the information on the device in case of theft.
- Where possible, each school enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g., keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.
- Before sharing data, all staff members will ensure:
    - They are allowed to share it.
    - That adequate security is in place to protect it.
    - Who will receive the data has been outlined in a privacy notice.
- Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of each school containing sensitive information are always supervised.
- The physical security of each school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
- The Arthur Terry Learning Partnership takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.
- The Arthur Terry Learning Partnership is responsible for continuity and recovery measures are in place to ensure the security of protected data.

Data retention & Pupil Records

All schools are under a duty to maintain a pupil record for each pupil.

The pupil / educational record should be seen as the core record charting the individual pupils progress through the education system, and should accompany them throughout their school career.

Pupil records may be held in paper form or electronically.

Retention – Transferring school
Responsibility for maintaining the pupil record passes to the next school. Schools may wish to retain the information about the pupil for a short period to allow for any queries or report to be completed.

Retention – Last known school
The last known or final school is responsible for retaining the Pupil Record. The school is the final or last known school if:

- A secondary phase and the pupil left at 16 years old or for post-16 or independent education, or;
- It is a school at any point and the pupil left for elective home education, they are missing from education or have left the UK.

The pupil record should be retained as a whole for 25 years from the date of birth of the pupil, after which time, if no longer required, it can be deleted or destroyed. SEN and other support service records can be retained for a longer period of 31 years.

Pupil records will contain personal and confidential information and so must be destroyed securely. Electronic copies must be securely deleted, and hard copies disposed of as confidential waste.

14. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system, for example, pupils use fingerprints to receive dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. Each school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the academy will delete any relevant data already captured.

Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

For further information please refer to the ATLP Protection of Biometric Data Policy.

15. Publication of information

Each school within The Arthur Terry Learning Partnership publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Minutes of meetings

- Annual reports
- Financial information

Classes of information specified in the publication scheme are made available quickly and easily on request.

Schools will not publish any personal information, including photos, on its website without the permission of the affected individual.

When uploading information to school websites, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

16. CCTV

We use CCTV in various locations around some school sites to ensure it remains safe, secure and to protect our reputation. 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, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Each school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

For further information on the processing, retention and security of CCTV data, please refer to the ATLP CCTV policy.

17. Photographs and videos

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

Primary schools:

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.

Any photographs and videos taken by parents/carers at any of our events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Secondary schools:

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at any of our events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other

pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where our schools take photographs and videos, uses may include:

- Within each individual school notice boards and in each individual school newsletters,
- Outside of each individual school by external agencies such as the trust photographer, newspapers, campaigns
- Online on any individual school website or social media pages

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

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.

18. Training

All staff and governance members are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development (CPD), where changes to legislation, guidance or any of the partnership processes make it necessary.

19. DBS data

- All data provided by The Disclosure and Barring Service (DBS) will be handled in line with data protection legislation; this includes electronic communication.
- Data provided by the DBS will never be duplicated.
- Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

20. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed annually and approved by the Board of Trustees.

21. Changes to this policy

We may change this policy at any time. Where appropriate, we will notify **data subjects** of those changes.

This policy is reviewed every year by the DPO.

The next scheduled review date for this policy is December 2024.

Annex

Definitions

Term	Definition
Biometric Data	is information about a person's physical or behavioural characteristics or features that can be used to identify them and is obtained or recorded for the purposes of a biometric recognition system and can include fingerprints, hand shapes, features of the eye or information about a person's voice or handwriting
Biometric Recognition System	is a system that operates automatically (electronically) and: • Obtains or records information about a person's physical or behavioural characteristics or features; and • Compares or otherwise processes that information with stored information in order to establish or verify the identity of the person or otherwise determine whether they are recognised by the system
Data	is information, which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Data Controllers	are the people who or organisations which determine the purposes for which, and the way, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes
Data Users	are those of our workforce (including Governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions

Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or Biometric Data
Workforce	Includes, any individual employed by Trust such as staff and those who volunteer in any capacity including Trustees/ Members/advocates/ parent helpers