# The Thomas Adams School

## Policy Statement

# Data Protection

Updated August 2019 ☐

Reviewed by Governors ☐

# DATA PROTECTION POLICY

## 1. Statement of Intent

Our school is committed to the highest standards of Information Governance and protection of individual's personal data and privacy.

We are required to keep and process relevant personal data regarding staff, pupils, their parents and guardians, governors, visitors and other individuals.

Our school aims to ensure that all personal data is processed in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

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

All staff involved with the processing of personal data are aware of their duties and responsibilities within these guidelines. Processing may include obtaining, recording, holding, disclosing, destroying or using data. Reference to pupils in this policy includes current, past or prospective pupils.

This policy will outline how our school will comply with its legal obligations under the General Data Protection Regulation:

## 2. Legislation and Guidance

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

## 3. Definitions

| Term | Definition |
|---|---|
| Personal data | Data relating to a living individual who can be identified. |
| Special categories of personal data | Personal data which is more sensitive and so needs more protection, including information about an individual's:<br>• Racial or ethnic origin<br>• Political opinions<br>• Religious or philosophical beliefs<br>• Trade union membership |

| | |
|---|---|
| | • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes<br>• Physical or mental health<br>• Sexual orientation<br>• Alleged or committed offences, their proceedings and sentences. |
| Processing | Anything done to personal data, such as collecting, recording, holding, organising, structuring, storing, adapting, altering, retrieving, using, disclosing, disseminating, erasing or destroying.<br>Processing can be automated or manual. |
| Data subject | An individual who is the subject of personal data. |
| 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 school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is 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 and volunteers at our school, and to external organisations or individuals working on our behalf. Data protection is seen as a 'whole school' issue, with specific responsibilities delegated as follows:

**Data Protection Roles & Responsibilities: List of duties**

| | |
|---|---|
| Governors | The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations. |
| Data Protection Officer (DPO) | The DPO is responsible for overseeing the implementation of this policy, monitoring the school's compliance with data protection law, and developing related policies and guidelines where applicable.<br><br>They will provide an annual report of their activities directly to the governors and, where relevant, report their advice and recommendations on school data protection issues.<br><br>The DPO is also the first point of contact for schools, individuals and for the ICO. |
| Headteacher | Acts as the representative of the data controller on a day-to-day basis for the school. |
| Data Protection Manager | Is the key person with specific responsibility for Data Protection within the school and responsible for overseeing the implementation of this policy and monitoring the schools compliance with data protection law:<br><br>• Responsible for all information governance including data protection<br><br>• Reports to the DPO and collaboratively works with the other school's Data Managers to share best practice and advice<br><br>• Ensures that the school is compliant with statutory requirements in relation to personal data and privacy<br><br>• Responsible for the Data Protection policy and associated procedures and embedding these into the administrative systems within school<br><br>• Advises the Headteacher and Senior Leadership Team on all matters of Information Governance<br><br>• Takes appropriate action for Subject Access Requests, Freedom of Information Requests, Individual Rights of data requests and Data Breach incidents<br><br>• Promotes a culture of awareness and commitment to information governance and data protection throughout school, inducting and training staff<br><br>• Is the main point of contact for pupils, staff, governors and parents who have data protection concerns |

| | |
|---|---|
| | • Ensures that all staff are aware of the procedures that need to be followed in the event of a data protection breach and can recognise SARs and FOI requests<br>• Ensures that a data protection incident log is kept up to date. |
| IT department | Responsible for security of school ICT system. |
| All Staff | Help to protect individual's personal data and privacy processing any personal data in accordance with this policy.<br>Inform the school of any changes to their personal data<br>Maintain an awareness of current data protection issues through training and CPD.<br>Contact the Data Protection Manager or DPO in the following circumstances:<br>• With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure<br>• If they have any concerns that this policy is not being followed<br>• If they are unsure whether or not they have a lawful basis to use personal data in a particular way<br>• Deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area<br>• To promptly pass on without delay a SAR/FOI request<br>• If there has been a data breach<br>• If they need help sharing personal data with third parties |
| Parents | Responsible for ensuring information that they provide to the school is accurate and up-to-date and notify us of any changes to information promptly. |

## 6. Key Contact Details

The DPO can be contacted at dpo@thomasadams.net

## 7. Individual's Legal Duties

Everyone in school has a responsibility to ensure that they abide by the principles listed in this policy for handling and processing personal data and making sure that information is securely and appropriately managed. If you are unsure about the action you are taking with regard to personal data you should check with the School Data Protection Manager or DPO to ensure you are complying with the DPA.

Our school takes its duties under the Data Protection Act seriously and any member of staff found to mishandle data or share personal data with unauthorised individuals will be subject to investigation under the school's Disciplinary Policy. Deliberate, malicious or reckless breaking of the DPA will be counted as gross misconduct and could result in dismissal. Under this Act you can also be criminally liable if you knowingly or recklessly disclose personal data.

## 8. Data Protection Principles

The GDPR is based on data protection principles that our school 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 they are 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 appropriate security of personal data.

This policy sets out how the school aims to comply with these principles.

## 9. Collecting Personal Data

### *9.1 Lawfulness, Fairness and Transparency*

We will only process personal data where we have one of 6 '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

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

If we offer online services to pupils, such as classroom apps, we rely on public interest as a basis for processing.

Whenever we first collect personal data directly from individuals, we will provide them with the school's Privacy Notice required by data protection law. Privacy Notices will remain accessible to Individuals.

### *9.2 Limitation, Minimisation and Accuracy*

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to 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.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's Retention Schedule.

## 10. 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 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 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 European Economic Area, we will do so in accordance with data protection law.

## 11. Subject Access Requests and other Rights of Individuals

### *11.1 Subject Access Requests*

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that 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 if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests must be submitted in writing, either by letter to the school or email to dpo@thomasadams.net. A template form is available at https://thomasadams.net/policies-documents. The request should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

We recommend that you submit a Subject Access Request to us electronically, on our template form which is available on the school website, but this is not compulsory.

If staff receive a subject access request they must immediately forward it to the Data Protection Manager or DPO.

### *11.2 Children and Subject Access Requests*

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either

be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

### *11.3 Responding to Subject Access Requests*

The school will comply with requests for access to personal information as quickly as possible and will ensure that requests for access are dealt with within the timescale specified by legislation.

Requests for access made by pupils and parents will be dealt with within 15 school days. The school will process requests from all other data subjects within 40 calendar days. An initial response will be sent to the requestor within 21 days of receiving an access request. The response will confirm the request has been complied with, indicate the intention to comply, or give the reasons for regarding the request as unjustified.

If there is an objection from a data subject to the school processing their personal data, the objection should be made in writing to the Headteacher.

### *11.4 Other Data Protection Rights of the Individual*

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the school office, Data Protection Manager or DPO. A Request Form is available on the school website and at Appendix 2 of this Policy. If staff receive such a request, they must immediately forward it to the school Data Protection Manager or DPO.

## 12. Parental Requests to see the Educational Record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil).

## 13. Biometric Recognition Systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school 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. The 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 school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or 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 school's 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 school will delete any relevant data already captured.

## 14. CCTV

We use CCTV in various locations around the school site 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, 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.

Any enquiries about the CCTV system should be directed to dpo@thomasadams.net

## 15. 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, newsletters, etc.
- 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 delete the photograph or video and not distribute it further.

## 16. 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 qualified 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 privacy 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
- 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.

## 17. Data Security

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.

Staff will ensure that personal and sensitive data is secured in accordance with the provisions of the GDPR and the school's ICT policies or associated procedures.

## 18. Disposal of Records

Personal data that is no longer needed will be disposed of securely in line with our Retention Schedule. 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.

## 19. Personal Data Breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the event of a suspected data breach, we will take action by following our Data Breach Management Procedure and completing a Data Breach Record (Appendix 3). Where necessary we will report the breach to the ICO within 72 hours.

## 20. 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 through meeting updates and internal/external training.

## 21. Monitoring Arrangements

The DPO is responsible for monitoring and updating this policy. This policy will be reviewed every 2 years or updated due to legislation changes and updates as they become relevant.

**Appendix 1**
**The Thomas Adams School**
**Retention Schedule for Pupil Records**

| **Type of Data** | **Retention Period** | **Reason** |
|---|---|---|
| Personal data including: date of birth, address, family contacts, photographs on electronic databases and some paper files. | 7 years from leaving school.<br><br>Computer records will be wiped and paper files shredded. | References and potential litigation. |
| Education progress and achievements, including examination grades on electronic databases and some paper files. | 7 years from leaving school.<br><br>Computer records will be wiped and paper files shredded. | References and potential litigation. |
| Behaviour and exclusion data on electronic databases | 7 years from leaving school.<br><br>Computer records will be wiped. | References and potential litigation. |
| Welfare information including information relating to abuse, child sexual exploitation, radicalisation, etc in paper files. | 7 years from leaving school.<br><br>These records will be shredded. | For potential litigation, welfare concerns and criminal prosecutions. Limitation period for negligence. |
| Health information – on electronic databases and in medical records. | 7 years from leaving school.<br><br>These records will be shredded. | Potential litigation. Limitation period of negligence. |
| Accident Books: records and reports. | Data collected and stored concerning accidents or incidents arising out of or in connection with any school activity is kept until the pupil is aged 21, as the pupil affected by the incident has the legal right to make a claim relating to that incident 3 years after their 18th birthday. | Limitation period of negligence. |

**The Thomas Adams School**
**Retention Schedule for Staff Records**

| Type of Data | Retention Period | Reason |
|---|---|---|
| Personnel files including training records and notes of disciplinary and grievance hearings. | 7 years from the end of employment. | References and potential litigation. |
| Staff application forms/interview notes. | At least 6 months from the date of the interview. | Time limits on litigation. |
| Facts relating to fewer than 20 redundancies. | 3 years from date of redundancy. | Time limits on litigation. |
| Facts relating to 20 + redundancies. | 12 years from date of redundancy. | Limitation Act 1980. |
| Income Tax and National Insurance returns, including correspondence with tax office. | At least 3 years after the end of the financial year to which the records relate. | Income Tax [Employment] Regulations 1993. |
| Statutory Maternity Pay records and calculations. | At least 3 years after the end of the financial year to which the records relate. | Statutory Maternity Pay [General] Regulations 1986. |
| Statutory Sick Pay records and calculations | At least 3 years after the end of the financial year to which the records relate. | Statutory Sick Pay [General] Regulations 1982. |
| Wages and salary records. | 6 years. | Taxes Management Act 1970. |
| Accident books; records and reports of injuries and diseases. | At least 3 years after the date of the last entry. | Social Security (Claims and Payments) Regulations 1979; RIDDOR 1995. |
| Health records. | During employment. | Management of Health and Safety at Work Regulations 1999. |
| Health records where reason for termination of employment is connected with health, including stress-related illness. | 3 years. | Limitation period for personal injury claims. |
| Medical records kept by reason of Control of Substances Hazardous to Health Regulations 1999. | 40 years. | COSHH Regulations 1999. |
| Ionising Radiation Records. | At least 50 years after last entry. | Ionising Radiation's Regulations 1985. |

**Appendix 2**
**The Thomas Adams School**
**Subject Access Request Form**

The following information is required to help the school to respond fully to your request. Please complete the information below and return this form by email to dpo@thomasadams.net or by post to the Data Protection Officer, The Thomas Adams School, Lowe Hill, Wem SY4 5UB. Requests for access made by pupils and parents will be dealt with within 15 school days. The school will process requests from all other data subjects within 40 calendar days.

**Your details**

| | |
|---|---|
| Title: | |
| Forename(s): | |
| Surname: | |
| Telephone number: | |
| Email address: | |

**Information being requested**

Please provide specific details (and any relevant dates) of the information being required and any additional information that may enable us to locate your personal data.

By completing this form, you are making a request under the General Data Protection Regulation (GDPR) for information held about you by the school that you are entitled to receive.

| |
|---|
| |

## Declaration

By signing below, you confirm that you are the Data Subject named in this Subject Access Request Form. You warrant that you are the individual named and will fully indemnify the school for all losses and expenses incurred if you are not. The school cannot accept requests in respect of your personal data from anyone else, including members of your family – see Data Protection Policy extract at the foot of this page.

| | |
|---|---|
| Name: | |
| Signature: | |
| Date: | |

## Extract from The Thomas Adams School's Data Protection Policy Statement

11.2 Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

**Appendix 3**
**The Thomas Adams School**
**Data Breach Record**

| | | | | | |
|---|---|---|---|---|---|
| Date | | | | | |
| Person responsible for dealing with breach | | | | | |
| Which data subject is involved? | | | | | |
| Data type involved | | | | | |
| Reported by | | | | | |
| Phone/email sent to DPO | Y/N | Is this high risk? | Y/N | Report to ICO | Y/N |
| Date reported to data subjects | | | | | |
| Action taken | | | | | |
| Preventative action suggestions – including training | | | | | |
| Notes | | | | | |
| Actions approved by | | | Date: | / / | |