DATA PROTECTION POLICY

(for Schools and the Kindergarten)

This policy will be reviewed annually or in response to changes in legislation		
Created	April 2018	IT Director, Head of HR, Vice Principal
Last Review	August 2022	Compliance Manager
Approved	September 2022	Principals and Headteachers
Next Review	September 2023	Compliance Manager

AIMS

Thomas's London Day Schools aim to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

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

DEFINITIONS

Term	**Definition**
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: Name (including initials) Identification number Location data Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: Racial or ethnic origin Political opinions Religious or philosophical beliefs Trade union membership Genetics Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes Health – physical or mental Sex life or sexual orientation

Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

THE DATA CONTROLLER

Our school processes personal data relating to parents, pupils, staff, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the Information Commissioner's Office (ICO) and will renew this registration annually or as otherwise legally required.

ROLES AND RESPONSIBILITIES

This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf. Members of staff who do not comply with this policy may face disciplinary action.

Principals

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

Compliance Manager

The Compliance Manager is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will work with the Privacy and Compliance Team to provide advice and guidance on all aspects of data protection.

They will provide an annual report of their activities directly to the Principals.

The Compliance Manager can be contacted on compliance@thomas-s.co.uk.

Privacy Leads

Each School has a privacy lead who will deal with any requests or enquiries relating to data protection compliance. They are also the first point of contact for individuals whose data the School processes. .

The IT Director and Head of HR work closely with the Compliance Manager to ensure data protection compliance in their areas of responsibility.

Head

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

All staff

Members of staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the Compliance Manager or Privacy Lead in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether 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.

Pupil and parent responsibilities

All pupils and parents shall:

- Ensure that all personal information they provide to the school is accurate and up-to-date'
- inform the school of any changes to that information, for example, change of address

Pupils may, from time to time, process personal information for example, for an assignment or research. In these circumstances they must notify their teacher and the Compliance Manager, who will provide further information to ensure pupils are complying with data protection legislation.

DATA PROTECTION PRINCIPLES

The UK 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 it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed

- Processed in a way that ensures it is appropriately secure
- The controller will be responsible for and able to demonstrate compliance with the above principles.

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

PROCEDURES

1. COLLECTING PERSONAL DATA

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 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 UK GDPR and Data Protection Act 2018.

Individuals are provided with a copy of the relevant Privacy Policy which details our purposes for processing personal data. These are also available on the school website.

Limitation, minimisation and accuracy

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

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

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

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 policy.

2. 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 UK we will do so in accordance with data protection law.

3. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

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 should be submitted to the Compliance Manager (compliance@thomas-s.co.uk). They should include:

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

If any member of staff receives a subject access request they must immediately forward it to compliance@thomas-s.co.uk. .

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers.

Pupils can make subject access requests for their own personal data provided that, in the reasonable opinion of the school, they have sufficient maturity to understand the request they are making. This is generally considered to be age 13 and above although this will depend on both the child and the personal data requested, including any relevant circumstances at home. Slightly younger children may also be sufficiently mature to have a say in this decision.

Parents can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data.

The pupil's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to subject access requests, we will follow the procedure set out in Appendix 1.

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 (where consent is the lawful reason for processing)
- 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 UK
- 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 P&C Team. If staff receive such a request, they must immediately forward it to the P&C Team.

4. PARENTAL REQUESTS TO SEE THE EDUCATIONAL RECORD

There is no automatic parental right of access to a child's educational record in independent schools, but we are likely to provide information on request. Such a request should be made in writing to the Head of your child's school.

5. BIOMETRIC RECOGNITION SYSTEMS

Where staff members or other adults use the school's biometric system(s), we will 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.

6. CCTV

We use CCTV in various locations around the school site to ensure it remains 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.

Please see the CCTV policy for further information about the CCTV system.

7. PHOTOGRAPHS AND VIDEOS

Information relating to this can be found in our Personal Devices and Photography Policy.

8. 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 Compliance Manager ensuring they have the necessary resources to fulfil their duties and where required we will seek assistance/advice from external advisors
- 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
- Completing data privacy impact assessments (DPIA) where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies. All completed DPIA's will be reviewed and signed off by the Compliance Manager. Completed DPIA's will be held centrally and will be reviewed as and when required. A DPIA form is located at Appendix 2.
- 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 Compliance Manager 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

9. DATA SECURITY AND STORAGE OF RECORDS

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data will not be left anywhere where there is general access
- Where personal information needs to be taken off site, staff sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

10. DISPOSAL OF RECORDS

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

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

11. PERSONAL DATA BREACHES

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 3. When appropriate, we will report the data breach to the ICO within 72 hours.

12. TRAINING

All staff and Principals are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

13. MONITORING ARRANGEMENTS

The Compliance Manager is responsible for monitoring and reviewing this policy and will be reviewed annually.

14. LEGISLATION AND GUIDANCE

This policy meets the requirements of the UK 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.

See also: CCTV Policy, Health & Safety Policy, ICT (Acceptable Use) Policy, Information Security Policy, Online Safety Policy, Personal Devices and Photography Policy, Pupil and Parent Privacy Notice, Safeguarding and Child Protection Policy

Staff Handbook: Staff Privacy Notice, Record Management Policy

Appendices

Appendix 1: Subject Access Request Procedure

Appendix 2: Data Privacy Impact Assessment Form

Appendix 3: Personal Data Breach Procedure

APPENDIX 1: SUBJECT ACCESS REQUEST (SAR) PROCEDURE

An individual can request details of personal data which is being held about them. The following process should be followed when making a Subject Access Request:

- Submit a request detailing the information they wish to see. This should be sent to the Compliance Managerby e-mailing compliance@thomas-s.co.uk
- The request will be reviewed by the Compliance Manager and the individual will be contacted if further information is required (e.g. in order to confirm the identity or authority of the individual or in order to assist in locating the data sought by the individual).
- Once all the information required is received an acknowledgement will be sent to the individual confirming receipt of the request and advising that the information requested will be provided within 1 calendar month of the acknowledgement. In some cases the time period may be extended by a further 2 calendar months where requests are complex or numerous. The individual will be advised if this is the case. Where requests are deemed to be manifestly unfounded or excessive the School has the right to refuse to respond. Where this is the case an individual will be provided with an explanation in writing and informed of their right to complain.
- Where the information requested identifies third parties, information will be redacted to protect the identity of them (unless permission has been expressly given by the third party for their information to be left in-tact).
- There may be occasions where information is exempt from this process (e.g. if it is legally privileged). Each SAR will be assessed by the Compliance Manager when the request is received.
- The Compliance Manager will liaise with the individual in relation to the delivery of the information when it is ready to be sent.
- The information will be provided free of charge, however where requests are deemed to be manifestly unfounded or excessive, or where further copies of the same information is requested the School reserves the right to make a nominal charge for this. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.
- A log of SARs received and actions taken will be maintained by the Compliance Manager.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child
- Is legally privileged

If the request is in relation to the schools CCTV cameras, the CCTV request form should be used which can be located at the end of the CCTV Policy.

APPENDIX 2: DATA PRIVACY IMPACT ASSESSMENT (DPIA) FORM

This form should be completed when a new project is being considered and where changes used are planned to existing practices (e.g. system or process changes with relates to personal information).

DPIA forms should completed in liaison with the Compliance Manager and must be signed off by the IT Director or Compliance Manager. An electronic version is available on MSP.

Date of Assessment:	
Completed by:	
Name of the Process: *This is the name of the process, system or website*	
Purpose of the Process: *Why do you need this?* *What will it be used for?*	
Under what legal basis it the information being processed? *Please select the most appropriate option*	• Consent: the individual has given clear consent for you to process their personal data for a specific purpose • Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract • Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations) • Vital interests: the processing is necessary to protect someone's life • Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law • Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.
Where does the data come from? *Who is providing you with personal information?* *Please select all that apply.*	• Pupil • Parent of Pupil • Staff Member
In which locations does the processing take place? *Where will the personal information be stored and processed? In the UK, the EU or another country? Please specify which country if possible.*	
Who is impacted by the processing? *Whose information will be shared and processed?* *Please select all that apply.*	• Pupil • Parent of Pupil • Staff Member

What is the process for deleting the data? *Please read the Data Processor's Privacy Notice or Data Protection Policies to find this information.*	
Describe the process workflow: *Describe here how the personal information will be shared with the Data Processor, how the information will be used by the Data Processor and how the information be will kept safe by the Data Processor.* *Please read the Data Processor's Privacy Notice or Data Protection Policies to find this information*	
What risks are there to the data subject? *How can the information provided end up in the wrong hands?*	
What measures are currently in place to protect the data subject and their rights? *What security measure have the Data Processor and you put in place to secure this information.* *Please read the Data Processor's Privacy Notice or Data Protection Policies to find this information.*	
What additional measures will be put in place to ensure all risks are covered? *Will any additional measures be put in place for securing this information by the Data Processor or yourself?*	
Is the risk deemed to be *High, Medium or Low?	
Date of next review	

Reviewed and signed off by the Compliance Manager / IT Director	

* If the risk is deemed to be high and the risk cannot be mitigated then the ICO (Information Commissioner Office) must be consulted before the processing commences

APPENDIX 3: PERSONAL DATA BREACH PROCEDURE

This procedure is based on guidance on personal data breaches produced by the ICO.

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify their School Privacy Lead or the Compliance Manager by by e-mailing compliance@thomas-s.co.uk providing as much information as possible. This must then be followed up by completing the electronic Data Breach Form located on MSP (Staff Resources – Forms).

The Compliance Manager and School Privacy Lead will investigate the report, and determine whether a breach has occurred. To decide, they will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

The Compliance Manager and School Privacy Lead will:

- alert the Head and the Principals
- make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
- assess the potential consequences, based on how serious they are, and how likely they are to happen
- work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, they will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the Compliance Manager must notify the ICO.

- The Compliance Manager will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are held and recorded by the Compliance Manager.
- Where the ICO must be notified, the Compliance Manager will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the Compliance Manager will set out:
    - A description of the nature of the personal data breach including, where possible:

        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the Compliance Manager
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the Compliance Manager will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the Compliance Manager expects to have further information. The Compliance Manager will submit the remaining information as soon as possible
- The Compliance Manager will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the Compliance Manager will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the Compliance Manager
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The Compliance Manager will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The Compliance Manager will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be held within the breach log which is a secure document held by the Compliance Manager.

- The Compliance Manager, School Privacy Lead, Head and Principals will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take actions to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.