Data Protection Policy

This policy has been adopted by all **Schools** within The Golden Thread Alliance.

Next Review Date	Summer 2026
Date Approved	Summer 2025

Contents

1. Aims

Our Trust aims to ensure that all personal data collected about colleagues, pupils, parents, carers, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018). This policy also covers the use of Artificial Intelligence (AI) technologies within the Trust and its schools.

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

2. Legislation and Guidance

This policy meets the requirements of the UK GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. The use of AI technologies within the school must comply with UK GDPR and data minimisation principles.

3. 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. This definition includes processing carried out by using AI technologies.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

Our Trust processes personal data relating to parents, carers, pupils, trustees, governors, visitors and others, and therefore is a data controller.

The Trust 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 colleagues** employed by our Trust, and to external organisations or individuals working on our behalf. Colleagues who do not comply with this policy may face disciplinary action. This includes compliance with the policy's provisions regarding the use of AI technologies.

5.1 Board of Trustees

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

5.2 Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. This includes providing advice and recommendation on Trust data protection issues related to AI. The DPO's authorisation is required before personal or sensitive data being processed through open AI tools.

The DPO will also assist in conduction risk assessments through Data Protection Impact Assessments (DPIAs) for AI tools that process personal data before deployment.

They will provide an annual report of their activities directly to the Chief Operating Officer and, where relevant, report to the Chief Operating Officer their advice and recommendations on Trust data protection issues.
The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their SLA.

Our DPO is SchoolPro TLC Limited and is contactable via DPO@SchoolPro.uk

5.3 Chief Operating Officer

The Chief Operating Officer acts as the representative of the data controller on a day-to-day basis.

- Act as the primary point of contact within the Trust for data protection matters, liaising with the DPO, colleagues, and other stakeholders as needed. This included matters related to AI use and data protection.
- Support the DPO in implementing and maintaining the Trust's data protection policies, ensuring compliance with the UK GDPR and Data Protection Act 2018. This included policies and practices concerning AI.
- Coordinate with the DPO to provide guidance and advice to colleagues on data protection best practices, ensuring that all employees understand their responsibilities. This extends to guidance on safe and compliant AI.
- Assist the DPO in conducting regular audits and assessments of the Trust's data protection practices, identifying areas for improvement and implementing necessary changes. This includes auditing the use of AI systems for data protection compliance.
- Work closely with the DPO to ensure that all colleagues receive appropriate data protection training and updates on legislative changes or new best practices. This specifically includes training on data protection risks associated with AI.
- Collaborate with the DPO to manage and respond to data subject access requests, data breaches, or potential breaches, ensuring prompt and effective resolution. This includes incidents involving AI.
- Monitor the Trust's data processing activities and data sharing agreements with third parties, ensuring compliance with data protection legislation and best practices. This includes monitoring data processing and sharing involving AI systems, ensuring vendors comply with policies.
- Support the DPO in maintaining records of the Trust's data processing activities, as required under the UK GDPR and Data Protection Act 2018. This includes records related to AI processing activities.
- Communicate any changes or updates to data protection policies and practices to colleagues, pupils, parents and carers, ensuring ongoing transparency and compliance. This includes updates regarding AI use.
- Promote a culture of data protection within the Trust, working closely with the DPO, senior leaders, Headteachers, and other colleagues to prioritize the protection of personal data. This includes the protection of data when using AI.

Concerns or incidents related to AI misuse, bias or security risks should be reported immediately to the Chief Operating Officer.

5.4 Headteacher

Headteachers are responsible for:

- Take overall responsibility for the school's data protection compliance, working with the DPO, senior leaders, and School Business Manager to implement and enforce policies. This encompasses the use of AI within the school.
- Ensure that data protection is a key consideration in all school activities and decision-making processes. This includes decisions about adopting and using AI tools.
- Communicate the importance of data protection to colleagues, pupils, parents and carers. This includes communicating guidelines and risks related to AI use.
- Report any data breaches, potential breaches, or subject access requests (SARs) to the Chief Operating Officer promptly. This includes incidents involving AI misuse or security risks.
- Address any data protection concerns or breaches, taking decisive action to rectify the situation and prevent future occurrences.
- Ensure that all colleagues receive appropriate data protection training.
- Report all data protection incidents and current actions to the Governing Body or nominated link Governor.

5.5 Senior Leaders

Senior Leaders are responsible for:

- Promote a culture of data protection within the school, ensuring that colleagues understand and adhere to data protection policies. This includes policies on AI.
- Work closely with the DPO to implement and monitor data protection practices. This includes the implementation and monitoring of AI use in compliance with data protection.
- Report any data breaches, potential breaches, or subject access requests (SARs) to the Chief Operating Officer promptly. This includes incidents involving AI misuse or security risks.
- Review data protection concerns or breaches, ensuring that corrective actions are taken promptly. This includes reviewing incident related to AI.
- Ensure that all staff receive appropriate data protection training. This specifically includes training on data protection risks associated with AI.

5.6 School Business Managers

School Business Managers are responsible for:

- Oversee and implement the Trust's data protection policy, ensuring that it aligns with the UK GDPR and Data Protection Act 2018. This includes overseeing policies related to AI use.

- Coordinate with the DPO to ensure colleagues are trained and informed about data protection practices. This includes coordinating ongoing training on data protection risks associated with AI.
- Monitor and evaluate the school's data protection practices, ensuring compliance with relevant legislation. This includes monitoring AI use.
- Collaborate with senior leaders and Headteachers to address any data protection concerns or breaches. This includes concerns or breaches related to AI.
- Coordinate and oversee the processing of subject access requests (SARs).

5.7 Teachers

Teachers are responsible for:

- Ensure that personal data of pupils and colleagues is collected, processed, and stored securely, following the Trust's data protection policy. This includes ensuring that personal or sensitive data is not entered into open AI systems without prior authorisation from the Chief Operating Officer and DPO and that no identifiable information is input into AI systems, unless explicitly approved.
- Use school-approved platforms and tools to communicate with pupils, parents, carers and colleagues to maintain data protection compliance.
- Report any data breaches, potential breaches, or subject access requests (SARs) to the Chief Operating Officer promptly. This includes concerns or incidents related to AI misuse, bias or security risks.
- Complete any required data protection training to maintain awareness of the relevant legislation and best practices. This includes ongoing training on data protection risks associated with AI.

5.8 Associate Teachers/Teaching Assistants

Associates Teachers/Teaching Assistant are responsible for:

- Support teachers in implementing data protection policies by handling student data with care and ensuring secure data storage. This includes adhering to guidelines on the use of AI and ensuring personal data is not mishandled.
- Use school-approved platforms and tools for communication and data sharing.
- Report any data protection concerns, breaches, or subject access requests (SARs) to the Chief Operating Officer promptly. This includes concerns or incidents related to AI misuse, bias or security risks.
- Participate in data protection training as required. This includes training on data protection risks associated with AI.

5.9 Administrators

Administrators are responsible for:

- Maintain the security and confidentiality of pupils, colleagues, and school data by adhering to the school's data protection policies. This includes following guidelines regarding the use of AI and data input.
- Process, store, and share data in accordance with the UK GDPR and Data Protection Act 2018.

- Support the Chief Operating Officer in maintaining data protection compliance by reporting any breaches, potential breaches, or subject access requests (SARs). This includes concerns or incidents related to AI misuse, bias or security risks.
- Support the processing of subject access requests (SARs).
- Attend data protection training as required. This includes training on data protection risks associated with AI.

5.10 All Colleagues

All colleagues are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy. This includes personal data processed using AI tools, ensuring that no identifiable information is input into AI systems unless explicitly approved and that personal or sensitive data is not processed through open AI tools without prior authorisation from the DPO.
- Informing the Trust of any changes to their personal data, such as a change of address
- Contacting the Chief Operating Officer in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure. This includes questions related to AI use.
    - If they have any concerns that this policy is not being followed. This includes concerns regarding AI use.
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way. This applies to the use of AI for processing personal data.
    - 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 European Economic Area. This is relevant when using AI that processes personal data or involves international transfers.
    - If there has been a data breach. This includes breaches involving AI systems or data processed by AI, or AI-generate security threats.
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals. This is particularly relevant when introducing or using new AI tools that process personal data.
    - If they need help with any contracts or sharing personal data with third parties. This includes agreements with AI vendors and data sharing involving AI systems.

6. Data Protection Principles

The UK GDPR is based on data protection principles that our Trust must comply with. Processing personal data using AI technologies must adhere to these principles.

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. AI processing must comply with data minimisation principles.
- 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. This includes implementing appropriate security measures for AI systems.

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

7. Collecting Personal Data

7.1 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 Trust, as a public authority, can perform a **public task,** and carry out its official functions
- The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract
- The data needs to be processed so that the Trust 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 for the **legitimate interests** of the Trust or a third party (provided the individual's rights and freedoms are not overridden)
- Where the above does not apply we shall request clear **consent** from the individual (or their parent/carer when appropriate in the case of a pupil)

For further detail of which lawful basis is used for each category of data, see the relevant privacy notice.

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. This is laid out in more detail in point 7.3.

If we offer online services to pupils, such as classroom apps, we intend to rely on Public Task as a basis for processing, where this is not appropriate we will get parental consent for processing (except for online counselling and preventive services).

When AI tools process personal data we will ensure full compliance with UK GDPR, conduct Data Protection Impact Assessments (DPIAs) and obtain consent where required.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law. This includes information about how AI processes their data, typically provided via our Privacy Notices.

7.2 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.

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

When using AI tools, colleagues must ensure that no identifiable information is input into AI systems unless explicitly approves and that personal or Sensitive data is not processed through open AI tools without prior authorisation from the DPO.

When colleagues no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's record retention schedule.

7.3 Our processing of special categories of personal data and criminal offence data

As part of our statutory functions, we process special category data and criminal offence data in accordance with the requirements of Articles 9 and 10 of the UK General Data Protection Regulation ('UK GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018'). Special category data must not be shared with AI tools without appropriate safeguards. Personal or special category data must not be processed through open AI tools without prior authorisation from the DPO.

Special Category Data

Special category data is defined at Article 9 of the UK GDPR as personal data revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation.

Criminal Conviction Data

Article 10 of the UK GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

Appropriate Policy Document

Some of the Schedule 1 conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data.

This section of our Data Protection Policy document explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018.

In addition, it provides some further information about our processing of special category and criminal offence data where a policy document isn't a specific requirement. The information supplements our privacy notices.

Conditions for processing special category and criminal offence data

We process special categories of personal data under the following UK GDPR Articles:

i. Article 9(2)(a) – explicit consent

In circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.
Examples of our processing include staff dietary requirements and health information we receive from our pupils who require a reasonable adjustment to access our services.

ii. Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the Trust or the data subject in connection with employment, social security or social protection.
Examples of our processing include staff sickness absences.

iii. Article 9(2)(c) – where processing is necessary to protect the vital interests of the data subject or of another natural person.
An example of our processing would be using health information about a pupil or colleague a medical emergency.

iv. Article 9(2)(f) – for the establishment, exercise or defence of legal claims.
Examples of our processing include processing relating to any employment tribunal or other litigation.

v. Article 9(2)(g) - reasons of substantial public interest.
As a Trust, we are a publicly funded body and provide a safeguarding role to young and vulnerable people. Our processing of personal data in this context is for the purposes of substantial public interest and is necessary for the carrying out of our role.
Examples of our processing include the information we seek or receive as part of investigating an allegation.

vi. Article 9(2)(j) – for archiving purposes in the public interest.
The relevant purpose we rely on is Schedule 1 Part 1 paragraph 4 – archiving.
An example of our processing is the transfers we make to the County Archives as set out in our Data Retention Policy.

We process criminal offence data under Article 10 of the UK GDPR

Examples of our processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations.

Processing which requires an Appropriate Policy Document
Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an APD (see Schedule 1 paragraphs 1 and 5).

This section of the policy is the APD for the Trust. It demonstrates that the processing of special category ('SC') and criminal offence ('CO') data based on these specific Schedule 1 conditions is compliant with the requirements of the UK GDPR Article 5 principles. Our retention with respect to this data is documented in our retention schedules.

Description of data processed
We process the special category data about our employees that is necessary to fulfil our obligations as an employer. This includes information about their health and wellbeing, ethnicity, photographs and their membership of any union. Further information about this processing can be found in our staff privacy notice.

We process the special category data about the children in our care and other members of our community that is necessary to fulfil our obligations as a Trust, and for safeguarding and care. This includes information about their health and wellbeing, ethnicity, photographs and other categories of data relevant to the provision of care. Further information about this processing can be found in our pupil privacy notice.

We also maintain a record of our processing activities in accordance with Article 30 of the UK GDPR.

Schedule 1 - Conditions for Processing

Special Category Data (SC)
We process SC data for the following purposes in Part 1 of Schedule 1:

- Paragraph 1(1) employment, social security and social protection.

We process SC data for the following purposes in Part 2 of Schedule 1. All processing is for the first listed purpose and might also be for others dependent on the context:

- Paragraph 6(1) and (2)(a) statutory, etc. purposes
- Paragraph 18(1) – safeguarding of children and of individuals at risk

Criminal Offence Data
We process criminal offence data for the following purposes in parts 1, 2 and 3 of Schedule 1:

- Paragraph 1 – employment, social security and social protection
- Paragraph 6(2)(a) – statutory, etc. purposes
- Paragraph 12(1) – regulatory requirements relating to unlawful acts and dishonesty etc
- Paragraph 18(1) – safeguarding of children and of individuals at risk
- Paragraph 36 – Extension of conditions in part 2 of this Schedule referring to substantial public interest

8. 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, parent or carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we may seek consent, if necessary, before doing this
- Our suppliers or contractors need data to enable us to provide services to our colleagues and pupils – for example, IT and communication companies, education support companies, and those that provide tools for learning. This includes third party AI vendors. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law. AI vendors must demonstrate compliance with the school's security policies before an AI system is adopted and ensure that all AI vendors used by the Trust and its schools comply with UK GDPR.
    - 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. AI systems must be configured to prevent external data sharing, ensuring they do not transmit user

data to third party companies without authorisation. We ensure that no special category data is shared with AI tools without appropriate safeguards.

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 colleagues.

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.

9. Subject Access Requests and Other Rights of Individuals

9.1 Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust 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, email or fax to the DPO.

They should include:

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

If colleagues receive a subject access request, they must immediately forward it to the Chief Operating and Financial Officer.

9.2 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 below the age of 12 are generally not 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 Trust may 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.

9.3 Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary

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

If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Requests will be processed in accordance with the Department for Education guidance 'Dealing with subject access requests (SARs). This guidance also makes reference to "Dealing with information already held by the requestor":

"If a requester already has information previously provided by the school or has access to information, you do not need to resend thus in your response. You will still need to explain that you hold that information and explain why you are not releasing it"

Data protection in schools - Dealing with subject access requests (SARs) - GOV.UK

The UK GDPR does not prevent a data subject making a subject access request via a third party. Requests from third parties are dealt with as follows:

- In these cases, we need to be satisfied that the third party making the request is entitled to act on behalf of the data subject.

- It is the third party's responsibility to provide evidence of this entitlement.
- This might be a written authority to make the request or it might be a more general power of attorney.
- If there is no evidence that the third party is authorised to act on behalf of the data subject, we are not required to respond to the SAR.
- However, if we are able to contact the data subject, we will respond to them directly to confirm whether they wish to make a SAR.

9.4 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 (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time, where consent is the basis 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 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). Where automated decisions making or profiling is used through AI, the school must ensure transparency and accountability, providing clear justifications and safeguard for affected individuals.
- 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 Chief Operating Officer. If colleagues receive such a request, they must immediately forward it to the Chief Operating Officer. Concerns or incidents related to AI misuse or bias should be reported immediately.

It is important to note that the Trust could be reported to the Information Commissioner's Office (ICO) for failing to comply with their statutory responsibilities regarding SARs and other data protection rights of the individual, and penalties (including financial) may apply.

10. 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 records if the child attends a maintained school.

There is no equivalent legal right to access their child's educational record if the child attends an academy or free school in England or an independent school. Our Trust has made the decision to grant equivalent access to the parents and carers of our pupils in line with the ICO's guidance, in order to retain appropriate communication between parents, carers and the Trust.

11. Biometric Recognition Systems

The Golden Thread Alliance does not and has no plans to use automated biometric recognition systems within The Trust or its schools.

12. CCTV

We use CCTV in various locations around the Trust's school sites to ensure it remains safe. We will adhere to the ICO's guidance for the use of surveillance systems including 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 the Chief Operating and Financial Officer. Our CCTV is also available for colleagues within the Staff Intranet Teams channel.

13. Photographs and Videos

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

We will not seek consent from parents or carers for photographs and videos to be taken of their child for educational purposes for use in the classroom and school displays. We will process these images under the legal basis of Public Task.

We will obtain written consent from parents and 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 schools on public area notice boards and in Trust/School magazines, brochures, newsletters, etc.
- Outside of Trust by external agencies such as the Trust photographer, newspapers, campaigns
- Online on our Trust and school's 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 usually accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Child Protection and Safeguarding Policy for more information on our use of photographs and videos.

14. Data Protection by Design and Default

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

- Appointing a suitably 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 data protection impact assessments (DPIAs) where the Trust'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 – see section 14.1). AI tools that process personal data must be risk-assessed through a Data Protection Impact Assessment (DPIA) before deployment.
- Integrating data protection into internal documents including this policy, any related policies and privacy notices. This includes explicitly referencing AI tools in the Data Protection Policy to clarify how AI is used, what safeguards are in place and how compliance with UK GDPR is maintained.
- Regularly training colleagues on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance. This includes ongoing training for colleagues on data protection risks associated with AI.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant. AI systems must be regularly reviewed and audited to ensure compliance with data protection legislation.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our Trust and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices). This includes updating privacy notices to inform colleagues, pupils and parents about how AI processes their data.
    - 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.

14.1 Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment (DPIA) is a process to help us identify and minimise the data protection risks of a project. AI tools that process personal data must be risk assessed through a DPIA before deployment.

We will do a DPIA for processing that is **likely to result in a high risk** to individuals as well as any other major project which requires the processing of personal data.

It is vital that the **DPIA is completed before processing is commenced** to ensure that all risks are identified and mitigated as much as possible.

Our DPIA will:

- describe the nature, scope, context, and purposes of the processing;
- assess necessity, proportionality, and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

To assess the level of risk, we will consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

We will consult our data protection officer (SchoolPro TLC Ltd) and, where appropriate, individuals and relevant experts. We may also need to consult with relevant processors.

If we identify a high risk that we cannot mitigate, we will consult the ICO before starting the processing.

We will implement the measures we identified from the DPIA, and integrate them into our policies, procedures, and practice.

15. Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. Updates to data security measures concerning AI should focus on data access controls, monitoring and risk mitigation.

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 must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must follow the relevant Trust procedures and ensure all records and copies are returned to the Trust
- Passwords that are at least eight characters long containing letters and numbers are used to access Trust computers, laptops and other electronic devices. Colleagues and pupils are reminded to change their passwords at regular intervals. Colleagues must use strong authentication measures (e.g multi factor authentication) when accessing school approved AI systems.
- Encryption software is used to protect all portable devices, such as laptops
- Colleagues, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for Trust-owned equipment (see our Acceptable Use Policy).
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8). This includes ensuring AI vendors comply with the Trust's security policies and that no sensitive data is shared with AI tools without appropriate safeguards.

16 AI System Security Controls

The Trust delegate responsibility to the Third Party IT provider to assess whether AI tools used with the Trust ad school comply with security best practices, including encryption, access control and regular audits.

AI systems must be configured to prevent external data sharing, ensuring they do not transmit user data to third party companies without authorisation.

AI systems must be regularly reviewed and audited to ensure compliance with data protection legislation.

17 Risk Management and AI Monitoring

The Third Party IT Providers must establish monitoring mechanisms to detect AI generated security threats, such as phishing scams, automated misinformation or unauthorised AI interactions.

The Third Party IT Providers must conduct regular penetration testing to evaluate AI-driven cybersecurity risks.

AI vendors must demonstrate compliance with the Trust's security policies before an AI system is adopted.

16. Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. This is with the exception of data that is retained in our Trust archive as described in section 15.

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 Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal Data Breaches

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches. This included monitoring mechanisms to detect AI generated security threats.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

-

It is important to note that the Trust could be reported to the Information Commissioner's Office (ICO) for high risk data breaches and penalties (including financial) may apply.

18. Training

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

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust's processes make it necessary. The Trust will provide ongoing training for colleagues on data protection risks associated with AI.

19. Monitoring Arrangements

This policy will be reviewed and updated **every year** and approved by the Board of Trustees.

20. Links with Other Policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Data Retention Policy
- ICT and Acceptable Use Policy

Appendix One: 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 the Chief Operating Officer. This includes reporting AI misuse, bias or security risks.
- The Chief Operating Officer will investigate the report and determine whether a breach has occurred. This includes breaches involving AI systems, data processed by AI or AI-generated security threats. To decide, the Chief Operating Officer 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 Chief Operating Officer will seek advice from the DPO and alert the Chair of Trustees
- The Chief Operating Officer will make all reasonable efforts to contain and minimise the impact of the breach, assisted by the DPO and relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen based on the Chief Operating Officer's investigation to advise the Chief Operating and further
- The DPO in conjunction with the Chief Operating Officer, will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO 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
    - Identity 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 DPO will notify the ICO.

- The Chief Operating Officer 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 stored in the Breach-Log document in electronic format.
- Where the ICO must be notified, the DPO or Chief Operating Officer will do this via the 'report a breach' page of the ICO website. As required, the report 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 DPO
    - 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 Trust will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when they expect to have further information. The Chief Operating Officer or DPO will submit the remaining information as soon as possible
- The Trust 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 Trust 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 DPO
    - 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 Trust 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 Trust 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 stored in the Breach-Log document in electronic format.

- The DPO and Chief Operating Officer will review what happened and how it can be stopped from happening again. This will happen as soon as reasonably possible

Actions to Minimise the Impact of Data Breaches

An example of the actions we will take to mitigate the impact of a data breach are set out below, focusing especially on a breach involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidently made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Colleagues who receive personal data sent in error must alert the sender and the Chief Operating Officer as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the Third Party IT provider to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of breach might include:

- Details of pupil premium children being published on the Trust and/or school website
- Non-anonymised pupil data or colleague pay information being shared with Governors
- A Trust/school laptop containing non-encrypted sensitive personal data being stolen or hacked.

Appendix Two: Data Breach Investigation Report

Date of Investigation:

Who carried out the investigation:

Findings:

Date of Breach:

Reported to Chief Operating Officer by and date:

Categories of personal data included in the breach: (tick all that apply)

- Data revealing racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union Membership
- Sex life data
- Sexual orientation data
- Gender reassignment data
- Health data
- Basic personal identifiers, eg name, contact details
- Identification data, eg usernames, passwords
- Economic and financial data, eg credit card numbers, bank details
- Official documents, eg driving licenses
- Location data, eg coordinates
- Genetic or biometric data
- Criminal convictions, offences
- Other

How many data subjects affected:

Categories of data subjects affected: (tick all that apply)

- Employees
- Pupils
- Parents and carers
- Third parties

Is the personal data breach likely to result in a high risk to data subject *(a reminder that if this is deemed high risk, we must report this to the ICO within 72 hours)*:

- Yes
- No
- Not known yet

Root Cause Analysis:
Cause of breach: (technical/human error/misuse or failure of AI systems)

Contributing Factors:

Mitigation and Remediation:
We have taken the following measures to mitigate the likely consequences of the data breach and gain control of the data again – This could include measures specific to securing AI systems, halting AI processing or recovering data from AI tools.

- Notify and consult with our Data Protection Officer (SchoolPro TLC)
- Identify and investigate the cause of the data breach including the scope of the data breached

Immediate Actions Taken:

Long Time Measures: (steps to prevent future breaches, This could include revising guidelines for AI use, implementing new AI security controls or providing additional AI specific data protection training.)

Communication Plan: (How and when affected individuals were/will be notified)

- Yes - we have determined it is likely there is a high risk to data subjects so we have communicated this breach to data subjects
- Yes – we have determined that it is unlikely there is a high risk to data subjects, however decided to tell them anyway
- No – but we are planning to because we have determined it is likely there is a high risk to data subjects
- No – we determined the incident did not meet the threshold for communicating it to data subjects

Supporting Documents:

Due to the breach, should colleagues be instructed to undertake some additional data protection training? [Please check when refreshers are due and move forward if necessary]

- Training is up to date but a reminder to colleagues will be issued to take care
- Refresher training is due and will be sent to colleagues to complete
- Training has not yet been completed and colleagues will be asked to complete as soon as possible

Sent to Chief Operating Officer:

[Please send this completed form to kate.george@golden-thread.org to add to the DPO portal for Trust review]