# DATA PROTECTION POLICY

This policy is prescribed by The Good Shepherd Trust and all reference to 'the Trust' includes all Trust schools, the central team and subsidiary organisations.

| | | | |
|---|---|---|---|
| Date adopted: | 10/05/2023 | Last reviewed: | 01/05/2023 |
| Review cycle: | Every 2 years or earlier | Is this policy statutory? | Yes |
| Approval: | Risk and Audit Committee | Author: | Data Protection Officer |
| Next Review Date: | 05/2025 | | |

**Revision record**

Minor revisions should be recorded here when the policy is amended in light of changes to legislation or to correct errors. Significant changes or at the point of review should be recorded below and approved at the level indicated above.

| Revision No. | Review Date | Revised by | Approved date | Comments |
|---|---|---|---|---|
| 1 | 1 March 2020 | L Mason | 18/03/20 | • Amended wording to simplify terminology.<br>• Added that a school is considered as an establishment for collective consultation purposes.<br>• Salary safeguarding period changes.<br>• Added potential to extend a redundancy trial period. |
| 2 | 1 October 2021 | L Mason | 13/10/22 | • Accommodation of changes to UK GDPR after exit from EEA |
| 3 | 1 December 2022 | P Coates | | • No significant changes<br>• Inclusion of the responsibility of employees to undergo Data Protection Training. |
| | | | | |

## 1. Introduction

The UK General Data Protection Regulation (UK GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed, or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, workers and other third parties.

## 2. Legislation and Guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR.

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 our funding agreement and articles of association.

## 3. Related Policies and Documents

CCTV Policy

Mobile Device Policy

Electronic Information and Communication Systems Policy

Privacy Notices

Data Retention Schedule

A copy of these can be obtained from admin@goodshepherdtrust.org.uk

## 4. Definitions

| TERM | DEFINITION |
|---|---|
| **Personal data** | Any information relating to an identified, or identifiable, living individual.<br>This may include the individual's:<br>• Name (including initials)<br>• Identification number<br>• Location data<br>• Online identifier, such as a username<br>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity. |

| TERM | DEFINITION |
|---|---|
| **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<br>• Genetics<br>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes<br>• Health – physical or mental<br>• 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.<br>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. |

## 5. When the Trust Processes Personal Data

### 5.1. Data Protection Principles

The Trust is responsible for and adheres to the principles relating to the processing of personal data as set out in UK GDPR law.

The principles the Trust must adhere to are: -

(1) Personal data must be processed lawfully, fairly and in a transparent manner.

(2) Personal data must be collected only for specified, explicit and legitimate purposes.

(3) Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

(4) Personal data must be accurate and, where necessary, kept up to date.

(5) Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed; and

(6) Personal data must be Processed in a way that ensures it is appropriately secure

Further details on each of the above principles is set out below.

#### 5.1.1. Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner

The Trust only collects, processes and shares personal data fairly and lawfully and for specified purposes. The Trust must have a specified purpose for processing personal data and special category of data as set out in the UK GDPR.

Before the processing starts for the first time, we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues in order to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e., that there is no other reasonable way to achieve that purpose).

##### 5.1.1.1. Personal Data

The Trust may only process a data subject's personal data if one of the following fair processing conditions are met: -

- The data subject has given their consent.
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract.
- To protect the data subject's vital interests.
- To meet our legal compliance obligations (other than a contractual obligation).
- To perform a task in the public interest or in order to carry out official functions as authorised by law; or
- For the purposes of the Trust's legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

##### 5.1.1.2. Special Category Data

The Trust may only process special category data if it is entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met: -

- The data subject has given their explicit consent.
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the Trust in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with a disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay.

- To protect the data subject's vital interests.
- To meet our legal compliance obligations (other than a contractual obligation);
- Where the data has been made public by the data subject.
- To perform a task in the substantial public interest or in order to carry out official functions as authorised by law.
- Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.
- Where it is necessary for reasons of public interest in the area of public health; or
- The processing in necessary for archiving, statistical or research purposes.

The Trust identifies and documents the legal grounds being relied upon for each processing activity.

5.1.1.3. Consent

Where the Trust relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the GDPR.

Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. If explicit consent is required, the Trust will normally seek another legal basis to process that data.

A data subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

The Trust will keep records of consents obtained in order to demonstrate compliance with consent requirements under the GDPR.

### 5.2. Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes

Personal data will not be processed in any matter that is incompatible with the legitimate purposes.

The Trust will not use personal data for new, different or incompatible purposes from that disclosed when the data was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).

### 5.3. Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

The Trust will only process personal data when our obligations and duties require us to. We will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, the Trust shall delete or anonymise the data. Please refer to the Trust's Data Retention Policy for further guidance.

### 5.4. Principle 4: Personal data must be accurate and, where necessary, kept up to date

The Trust will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the Trust.

### 5.5. Principle 5: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed

Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The Trust will ensure that it adheres to legal timeframes for retaining data.

We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.

Please refer to the Trust's Retention Policy for further details about how the Trust retains and removes data.

### 5.6. Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage

In order to assure the protection of all data being processed, the Trust will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as: -

- Encryption;
- Pseudonymisation (this is where the Trust replaces information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure);
- Ensuring authorised access (i.e. that only people who have a need to know the personal data are authorised to access it);
- Adhering to confidentiality principles; and
- Ensuring personal data is accurate and suitable for the process for which it is processed.

The Trust follows procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

The Trust will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

### 5.7. Sharing Personal Data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with law enforcement and government bodies where we are legally required to do so. There may be circumstances where the Trust is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities, for example, the Local Authority, Ofsted or the Department of Health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

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

## 6. Data 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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- 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
- The safeguards provided if the data is being transferred internationally

### 6.1. 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 school 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.

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.

### 6.2. Responding to subject access requests

When responding to requests, we:

- Will ask the individual to provide 2 forms of identification if we need to be satisfied of the individuals 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 (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- Where a request is complex or numerous, we will tell the individual we will comply within a reasonable time period after receipt of the request. We will inform the individual of this within one month and explain why the extension is necessary.

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts
- The cost of obtaining the information exceeds the limit detailed in section 12 of the Freedom of Information Act for Public Authorities.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

### 6.3. Other data protection rights of the individual

In addition to the right to make a subject access request (see above), 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 (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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 DPO. If staff receive such a request, they will immediately forward it to the DPO.

## 7. Direct Marketing

The Trust will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The Trust will promptly respond to any individual objection to direct marketing.

## 8. Employee Obligations

Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the Trust in the course of their employment or engagement. If so, the Trust expects those employees to help meet the Trust's data protection obligations to those individuals. Specifically, they must: -

- Only access the personal data that you have authority to access, and only for authorised purposes.
- Only allow others to access personal data if they have appropriate authorisation.
- Keep personal data secure (for example by complying with rules on access to Trust premises, computer access, password protection and secure file storage and destruction. Please refer to the Trust 's Security Policy for further details about our security processes); and
- Not to remove personal data or devices containing personal data from the Trust premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information; and
- Not to store personal information on local drives.
- Complete all Data Protection training as requested by the Trust.

The Trust will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws.

Further details can be found in the Electronic Information and Communication Systems Policy.

## 9. Biometric Data

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 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.

## 10. CCTV

We use CCTV in various locations around school sites 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. Further details can be found within individual school CCTV policies.

## 11. Photographs and videos

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

For primary schools, we will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

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

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

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

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

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

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

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

## 12. Transparency and Privacy Notices

The Trust will provide detailed, specific information to data subjects. This information will be provided through the Trust's privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. Privacy notices set out information for data subjects about how the Trust uses their data and the Trust's privacy notices are tailored to suit the data subject.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the UK GDPR including the identity of the data protection officer, the Trust's contact details, how and why we will use, process, disclose, protect and retain personal data. This will be provided in our privacy notice.

When personal data is collected indirectly (for example from a third party or publicly available source), we will provide the data subject with the above information as soon as possible after receiving the data. The Trust will also confirm whether that third party has collected and processed data in accordance with the UK GDPR.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as "children" under the UK GDPR.

## 13. Privacy by Design

The Trust adopts a privacy by design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the Trust takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

### 13.1. Audit

The Trust will test our data systems and processes in order to assess compliance. These are done through data audits which take place annually in order to review use of personal data.

## 14. Data Protection Impact Assessments (DPIAs)

In order to achieve a privacy by design approach, the Trust conducts DPIAs for any new technologies or programmes being used by the Trust which could affect the processing of personal data. In any event the Trust carries out DPIAs when required by the GDPR in the following circumstances: -

- For the use of new technologies (programs, systems or processes) or changing technologies.
- For the use of automated processing.
- For large scale processing of special category data; or
- For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

Our DPIAs contain: -

- A description of the processing, its purposes and any legitimate interests used.
- An assessment of the necessity and proportionality of the processing in relation to its purpose.
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

**15. Data Security and Storage**

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.

**16. Disposal of records**

Personal data that is no longer needed will be disposed of securely in line with the Trust's Data 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.

**17. <u>Accountability</u>**

The Trust will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the UK GDPR principles.

The Trust has taken the following steps to ensure and document UK GDPR compliance: -

**17.1. Data Protection Officer (DPO)**

Peter Coates, The Good Shepherd Trust, Larch Avenue, Guildford, Surrey, GU1 1JY

The DPO is responsible for overseeing this data protection policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this policy is not being or has not been followed.

**17.2. Personal Data Breaches**

The UK GDPR requires the Trust to notify any applicable personal data breach to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach.

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for personal data breaches. For the Trust this is the DPO.