Good Shepherd Trust

life in all its fullness

Data Protection Policy

EXTERNAL VERSION

Date of Adoption	**January 2016**
Reviewed	**May 2018**
Reviewed	**September 2019**
Reviewed	**June 2020**
Reviewed	**May 2022**
Reviewed	**April 2024**
Date of Next Review	**May 2025**

Data Protection Organisation Information

Data Protection Officer (DPO):	
DPO Contact Email:	**dataprotectionofficer@thegoodshepherdmat.co.uk**
ICO Registration Number:	ZA099650
Report a Data Breach:	
by email: dataprotectionofficer@thegoodshepherdmat.co.uk	
Report a Subject Access Request (SAR) or Freedom of Information Request (FOI):	
businessmanager@thegoodshepherdtrust.co.uk	
For help and guidance:	
• gov.uk: Data Protection in Schools • https://ico.org.uk/ • https://kymallanhub.co.uk/	

Contents

List of Appendices and Additional Documents

Additional Documents

1 Values

In keeping with our Trust values, every member of the Trust family of schools will be valued and encouraged to fulfil their potential. In our Trust we believe:

- Everyone has something to offer
- Trust, honesty, empathy and social responsibility are the Christian values that frame our work
- We are here for the whole person, spiritually, morally, educationally and socially
- In working with transparency and openness

2 Definitions and Terminology

The proprietor is The Good Shepherd Trust Multi Academy Trust.

For the purposes of this Policy and procedures a child, young person, pupil or student is referred to as a 'child' or a 'pupil' and they are normally under 18 years of age.

Wherever the term '**parent**' is used this includes any person with parental authority over the child concerned e.g., carers, legal guardians etc.

Wherever the term '**school**' or '**setting**' is used this refers to our central office and each of our academies and includes any wrap around care provided and delivered by that setting such as After School Clubs and Breakfast Clubs.

The following definitions explain a little more about our approach to personal data:

'Data processors' are third party organisations which process data on our behalf. They make no decisions about how and why they do that; they just do what we ask them to within the terms of our contract.

'Data subjects' are the people about whom we hold data, and they fall into several general "categories of person", for example, our workforce and their next of kin; pupils, their next of kin, and other professionals involved with them; our contractors (cleaners, caterers, health & safety, and other service providers); agency and other partner organisation workers (supply or peripatetic teachers, educational psychologists).

'Personal data' is any manually or digitally recorded information relating to a living person (a data subject) which identifies them e.g., a name, an email address, an identification number, location data, an image, an IP address, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person and may include facts or opinions about them. Some of this category of personal data will require enhanced security measures such as encryption, password protection and stricter electronic as well as manual access controls e.g., a locked filing cabinet. This will be determined based on a risk assessment of the harm that failing to secure the data might cause e.g., bank details due to the risk of potential fraud, contact information due to potential harassment etc.

'Sensitive personal data' or **'special category data'** includes disability status, sexual orientation, sex life, ethnicity, medical information (both physical and mental health), political, philosophical, and religious opinions/beliefs, trade union membership, and details of criminal convictions or allegations. This category of personal data requires enhanced security measures such as encryption, password protection and stricter electronic as well as manual access controls.

'Pseudonymised personal or sensitive personal data' is information that has been de-personalised but key-coded and it can fall within the scope of the UK UK GDPR and this policy depending on how difficult it is to attribute the pseudonym to a particular individual.

'Supervisory Authority' is the body that regulates compliance with the UK GDPR and in the UK this is the ICO.

'Third country' is the designation given to a country where there is no privacy and security of data equivalence agreement and transfers of personal data are restricted unless the data is specially protected, or an exception applies.

The UK is a 'third country' to states in the EU UK GDPR zone (the EU member states plus Norway, Liechtenstein and Iceland) so, the exceptions that apply to the UK are the adequacy decision on transfers under EU UK GDPR and the adequacy decision on transfers under the Law Enforcement Directive on data transfers between the EU and UK.

A 'third country' to the UK, is any state or country worldwide which is not a part of the UK and to which the UK under UK UK GDPR restricts transfers of personal data unless the personal data is specially protected, or an exception applies. The exceptions that apply to some of these 'third countries' are limited and described in the adequacy decisions the UK has made (see Section 10.5 for more information).

Throughout this document the following terminology is used to describe the roles within the Trust.

Role/Term	Alternatives, description and meaning
Members	Members appoint the Directors. Membership is described in the Trust's Articles of Association
Directors	Also 'the Trust board' or 'the board' The Trust Directors are accountable in law for all decisions about member schools and are accountable to the Secretary of State for Education for the performance of each school within the Trust.
LGB	Also 'Local Governing Bodies' or 'LGB Members' The local governing body is a standing committee of the Trust which has delegated powers to oversee the running of its individual school. The LGB may choose to delegate some of these powers to smaller committees or the Headteacher as it deems fit to fulfil its responsibilities. Where the document refers to the LGB this might be through some committees or further delegation but with the understanding that the ultimate responsibility remains with the LGB.
CEO	Chief Executive Officer A significant number of responsibilities under the scheme of delegation lie with the CEO. It is recognised that the CEO may choose to delegate some of their duties to the Chief Finance Officer and School Improvement Consultants and other staff in their team.
Central Team	Refers collectively to the: Business Manager, Finance Support Officers, School Improvement Consultants, Admin Support Officers and Development Officer Any other staff appropriate to the responsibility or task who work from the Trust's central administration office in Penrith rather than being based in a school.
SLT	Senior Leadership Team The Headteacher/Executive Headteacher, Head of School, Deputy Headteacher or other Senior staff member as appropriate to the individual school's senior leadership structure
	'Headteacher' in policies will usually refer to the Headteacher or Executive Headteacher as appropriate for the leadership structure of the school

Associated policies or documents include:

- Overarching Safeguarding Statement
- Child Protection Policy and procedures
- Online Safety Policy and procedures
- Freedom of Information Publication Scheme
- Health and Safety Policy and procedures
- Procedures for Using Pupils' Images
- Behaviour Policy and procedures
- Staff Code of Conduct
- Surveillance Camera Procedures (where applicable)

3 Introduction

This is a Trust wide policy designed to cover all our schools and central operations.

This document is a statement of the aims and principles of the whole Trust for ensuring the appropriate handling of personal and sensitive information. This policy takes due note of the information and guidance published by the Information Commissioners Office (ICO).

It is the responsibility of the Trust's Board of Directors to ensure registration with the ICO is undertaken.

3.1 Aims

This policy sets out how the Trust's family of schools will:

- Comply fully with the requirements of the Data Protection Act 2018.
- Ensure that all processing is appropriately registered / notified and review and update notified entries.
- Ensure that all staff involved with the collection, processing and disclosure of personal data are made aware of their duties and responsibilities within these guidelines.
- Demonstrate compliance with the Data Protection (DP) principles including:
    - implementing appropriate technical and organisational measures
    - maintaining records on processing activities
    - conducting data protection impact assessments
    - undertaking data protection by design and default

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, we must comply with the Data Protection Principles which are set out in the Data Protection Act 2018 (the 2018 Act).

In summary these principles state that personal data shall:

i.	Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
ii.	Be obtained for a specified and lawful pupose and shall not be processed in any manner incompatible with that purpose
iii.	Be adequate, relevant and not excessive for that purpose
iv.	Be accurate and kept up to date
v.	Not be kept for longer than is necessary for that purpose
vi.	Be processed in accordance with the data subject's rights
vii.	Be kept safe from unauthorised access, accidential loss or destruction

All staff who process or use personal information must ensure that they always follow these principles.

The Good Shepherd Trust is committed to protecting and respecting the confidentiality of sensitive information relating to staff, pupils, parents and LGB members, directors and volunteers and any other type of individual it holds personal data about.

As an organisation there is a legitimate need to keep certain information about employees, pupils and other users to allow, for example, monitoring of performance, achievement, and health and safety.

4 The Data Controller and Designated Data Controllers

The Good Shepherd Multi Academy Trust as the corporate body is the Data Controller under the 2018 Act, and therefore the Directors are ultimately responsible for implementation. The CEO (assuming they are also a director) act as the Designated Data Controller for the Trust as a whole.

Day-to-day responsibility for activity in each location is given to two Designated Data Controllers. They are the headteacher and the senior member of the office staff in each school, and the CEO and a member of staff in the central office. They are also responsible for ensuring that all staff and volunteers in their setting are adequately trained and understand their responsibilities regarding data protection, including recognising a Subject Access Request (see section 7 below) and what to do once a request has been received.

The Trust's central team will coordinate a data audit and produce and manage a central data register. It is the responsibility of each location's Designated Data Controllers to review the register on a regular basis and report any changes, including third parties with whom they share the data. This is particularly relevant for such things as changes of applications and platforms providing online learning services.

Where the individual locations enter into agreements with suppliers, with which third party data sharing will take place, then the Designated Data Controllers for that location must ensure that data sharing agreements are in place before they proceed and ensure the central data register has been updated accordingly, with all relevant correspondence and agreements being shared with the central team's designated data controllers.

5 Data Protection Officer Role & Responsibilities:

The Trust will appoint and support the Data Protection Officer (DPO) to take responsibility for its data protection compliance and ensure they have the knowledge, support and authority to carry out their role effectively. The DPO can be contacted by emailing dataprotectionofficer@thegoodshepherdmat.co.uk.

The Trust has an appointed DPO because:

1) Under the Data Protection Regulations, the processing it carried out is to achieve a public task e.g. education
2) Core activities consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale (FSM, grades, IHCPs/ EHCPs).
3) Core activities consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

The role of the DPO is:

- to take responsibility for and monitor, data protection compliance
- be the point of contact with the ICO (and for data subjects and workers within the Trust)
- to lead/advise on (not necessarily carry out) DPIAs
- to take a risk-based approach
- to maintain data protection records

In delivering the DPO role monitoring tasks will include:

- collect information to identify processing activities
- analyse and check compliance of processing activities
- inform, advise & issue recommend to the controller/processor

Any member of staff, parent or other individual who considers that the policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the appropriate Designated Data Controller or the Data Protection Officer.

6 Responsibilities of Staff

All staff who process or use personal information must ensure that they always follow the data protection principles set out above. To ensure this happens this Data Protection Policy has been developed. This policy **does not** form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the Trust's Board of Directors from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

All staff are responsible for ensuring that:

I. Any personal data that they hold is kept securely.
    - All personal data should be kept in a locked filing cabinet, drawer, or safe; or
    - If it is computerised, be encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and
    - Personal data should not be downloaded or kept on a usb memory key or other removable storage media.

II. Personal information is not disclosed either orally or in writing or via web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

III. All data breaches are reported using the process described in section 9 of this policy

IV. All personal data is handled with reference to this policy and the Trust Online Safety Policy.

V. They are fully aware of their responsibilities regarding data protection including attending aware raising sessions/ workshops as required.

Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases.

Regarding their own data all staff are responsible for:

I. Checking that any information that they provide to the Trust in connection with their employment is accurate and up to date.
II. Informing the Trust of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The Trust cannot be held responsible for any errors unless the staff member has informed it of such changes.

7 Rights to Access Information (Subject Access Requests SAR's)

All staff, parents and other individuals are entitled to:

I. Know what information the Trust and it's schools hold and process about them or their child and why.
II. Know how to gain access to it.
III. Know how to keep it up to date.
IV. Know what the Trust is doing to comply with its obligations.

To facilitate this, the Trust has produced 4 types of privacy notices as follows (these can be found in **Appendix A**:

I. Privacy notice – Workforce
II. Privacy notice – Governance roles
III. Privacy notice – Pupils and Families
IV. Privacy notice – primary school pupils* **Can be adapted with the school logo and name**

*The Trust recognises that whilst parents/carers/legal guardians have the legal responsibility for and can agree to the use of their child's personal data for those children younger than 13, it is good practice to engage with and aid the understanding of those pupils in our schools that are younger than 13. To this end the privacy notice for primary school pupils has been designed to be relevant to and understood by younger pupils.

7.1 Receiving a Subject Access Request

Under Article 15 of the UK GDPR all individuals have a right to access certain personal data being kept about them or their child either digitally or in hard copy. Advice and guidance about dealing with subject access requests can be found on gov.uk.

Ideally, any person who wishes to exercise this right should make a request in writing and submit it directly to the Data Protection Officer:

Email: dataprotectionofficer@thegoodshepherdmat.co.uk

Post: Data Protection Officer, 19-24 Friargate, Penrith, Cumbria, CA11 7XR

A form is available to help people complete their request (**Appendix B**) as this can speed up the process by ensuring the right information is provided however there is no requirement to use this form and a SAR can be made in any format. This could be a verbal request, a written request via a letter, text or email, or come through social media. Once an individual has made a request, we cannot ask them to change the format they made the request in.

A request can be made to anyone who works at one of our settings, this could include:

- Teachers
- Support staff
- Volunteers and Local Governing Body members

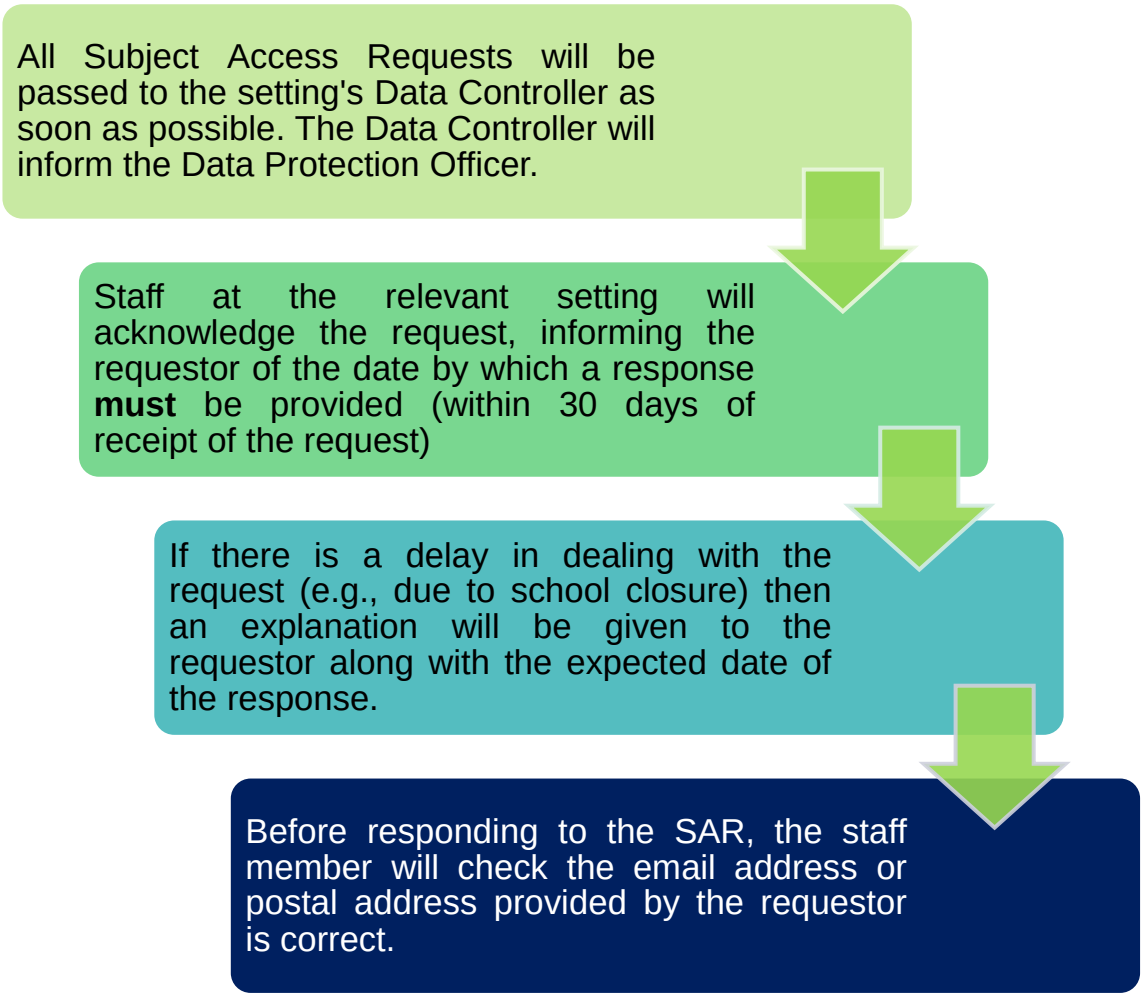
The Designated Data Controllers must ensure that everyone in their setting can recognise a Subject Access Request when it is made or ensure that a clear procedure of reporting to

either the Headteacher or Administrator is in place when anyone is unsure about a request made to them.

The Data Controllers are trained to recognise a SAR and what to do once it is received, even when it does not include the words “subject access”, or refer to the applicable legislation, includes reference to the wrong legislation i.e., often the Freedom of Information Act or is part of a wider issue such as a complaint.

Once a SAR has been received the setting must inform the DPO. SAR’s will be directed to the appropriate Designated Data Controller for the most relevant location to deal with the request depending on who the requestor is, i.e. individual schools for pupil or family information, school volunteers and LGB members and the central Trust for employees, directors and members. The DPO will also notify the Trust business manager of each SAR received.

The process for dealing with any SAR is as follows:



7.2 Information an individual can request

A requestor can ask for any personal data that relates to:

- Themselves
- Someone they have parental responsibility for
- Someone they have permission to act on behalf of

7.3 Clarifying a SAR

Some requests will be non-specific and ask for ‘all the information held’. This could result in a large volume of data and while we cannot ask the requestor to narrow or reduce their request it is possible to seek clarification of what specific information the requestor is looking

for. This might be helpful when the requestor asks for general information because they are not sure what they need.

7.4 Encouraging self-service

If the requestor already has access to the information they want, direct them to this. This may for example include pupil information held on a digital platform such as Class Dojo or similar. Where the requestor can access the information themselves within one calendar month the request does not have to be treated as a SAR.

7.5 When to check the identity of someone submitting a SAR

In most cases when an individual makes a SAR identity verification will be required.

In our settings pupils and their parents or carers are generally well-known to staff. If the Data Controller knows the requestor and is sure of their identity and authority an ID request does not have to be completed. A record of this decision and why it was made must be kept.

If the requestor is asking for their own information and is unknown to the Data Controllers then ID should be provided.

Adults should provide a photo ID plus another form of ID, this could be:

- Their driving license or passport for the photo ID
- A utility bill or council tax bill that confirms their name and address

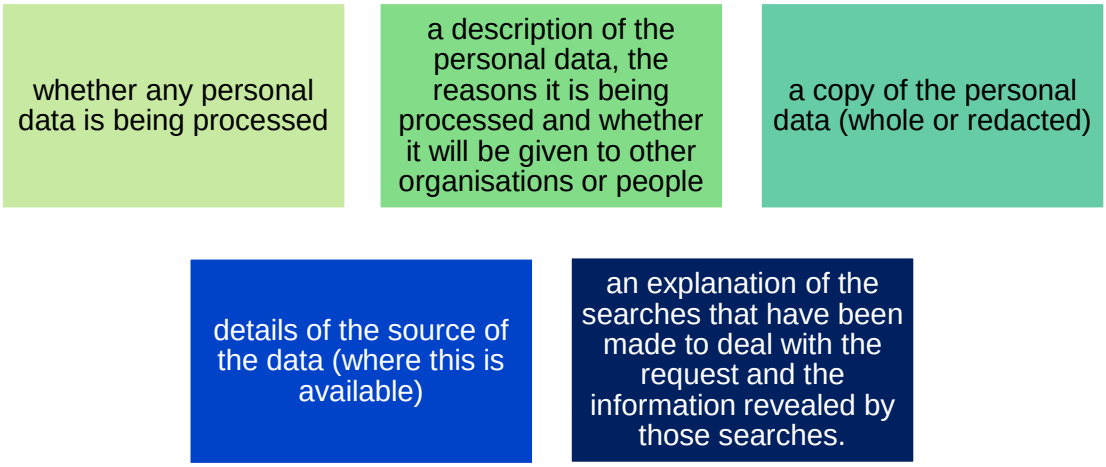
Where requests are being made on behalf of others, such as through solicitors or other third parties, then the authorisation and therefore the right for the third party to access the individual's personal data must be established before the request is dealt with. It is the responsibility of the third party to prove they are entitled to act on behalf of the individual whose data is being requested. They must also provide that individual's ID.

The Data Controllers at each setting are responsible for deciding whether to request ID.

If the requestor cannot provide the standard ID, it is the Data Controller's decision whether alternative identification is appropriate. A record must be kept of this decision-making process.

7.6 Responses to a SAR

In fulfilling the SAR, a statement regarding the personal data held about the requestor will be provided. This will include:



If no personal data is held about the requestor, a response will still be made saying this and, if relevant, why we no longer hold any data. In some cases, there may be grounds for refusing requests for personal data entirely or for providing data that has been redacted, for further information and resources see **section 8** below and **Appendix C**.

7.7 Accessing Pupil's Information

There are two ways of accessing pupil information:

1. Under Data Protection legislation, the UK GDPR grants the right of access to pupils and those with parental responsibility for a pupil
2. Under education regulations, those with parental responsibility have the right to **view** a pupil's education record

7.7.1 Access under UK GDPR

This right of access comes under Article 15 of the UK GDPR.

The right to access information held about a child is the child's right rather than anyone else's, even if:

- They are too young to understand the implications of the right to access
- The right is exercised by those who have parental responsibility for the child
- They have authorised another person to exercise the right on their behalf

This means that, unlike the distinct right of access to the educational record (**7.2.2 below**), the right to make a SAR is the pupil's right alone. Parents are only entitled to access information about their child by making a SAR if the child is unable to act on their own behalf **or** has given their consent.

Before responding to a SAR for information held about a child, the setting's data controller will consider whether the child is mature enough to understand their rights, seeking advice and support from the Trust DPO or Business Manager as necessary. If confident that the child can understand their rights, then a response will be made to the child rather than the parent. What matters is that the child can understand (in broad terms) what it means to make a SAR and how to interpret the information they receive. When considering borderline cases, consideration will be given to:

- the child's level of maturity, where possible and their ability to make decisions like this
- the nature of the personal data
- any court orders relating to parental access or responsibility that may apply
- any duty of confidence owed to the child or young person
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill-treatment
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

It does not follow that, just because a child has capacity to make a SAR, they also have capacity to consent to sharing their personal data with others – as they may still not fully understand the implications of doing so.

In deciding what information to supply in response to a SAR, examples of information which (depending on the circumstances) might be appropriate to withhold include:

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

7.7.2 Access under Education Regulations

Those with parental authority can request to view a child's education record under The Education (Pupil Information) (England) Regulations 2005. Education regulations are not regulated by the ICO, complaints about requests to view an education record will be dealt with through the Good Shepherd Trust's Complaints Policy available from the Trust's website and each school's website and as a paper copy by request at any setting.

Access to education records is a separate right and is not covered by Data Protection legislation. Unlike the right to access under Data Protection legislation, this right does not extend to pupils.

The Education Record
An education record covers information that comes from a teacher or other employee of the Trust, the pupil or a parent, and is processed by or for the Trust's board of directors, the local governing body or teacher. This is likely to cover information such as:

- The records of the pupil's academic achievements
- Correspondence from teachers, other Trust employees and educational psychologists engaged by the Trust's board of directors or the local governing body

It may also include information from the child as well as information from a parent, carer or guardian. Information provided by the parent of another child, or information created by a teacher solely for their own use would not form part of a child's education record.

Making a request under Education Regulations
Those with parental responsibility can apply to the individual setting to view an education record or receive a copy.

The setting **must** comply with a written request within **15 school days**. This does not include school holidays.

Those with parental authority **must** be given access to view the record free of charge.

If a request is made for a copy of the record, this must also be provided within 15 school days but the setting can charge a fee for the copy. The fee must not exceed the cost of supply:

The cost depends on the number of pages provided. For example:

- 1 – 19 pages will cost £1.20
- 29 pages will cost £2
- And so on, up to a maximum of 500+ pages which will cost £50.

If the request is for other information excluding the educational record, then the maximum charge is £10.

There are certain circumstances where an education record may be withheld; for example, where the information might cause serious harm to the physical or mental health of the pupil or another individual. The request for access would also be denied if it would mean releasing examination marks before they are officially announced.

A request to view or receive a copy of the education record, will only disclose the information contained in the record and **must not** disclose any further personal data that my be held by the setting or the wider Trust.

7.8 Managing the SAR Process

In managing the SAR process a record of all requests will be kept including the following information:

- whether ID has been checked, if so, what form it took and if not, why not
- date of receipt of the request
- date of initial response

- details of any time the response was paused and why (e.g., getting identification)
- copies of information provided in response to the SAR, together with copies of any material withheld and an explanation why

More information about Subject Access Requests to help staff deal with them can be found in the ICO guidance and from the DfE.

The Trust may refuse access requests that are manifestly unfounded or excessive. If a request is refused the Trust will explain why and individuals then have the right to complain to the supervisory authority (**Appendix C**).

There is no fee to complete a SAR, however a charge for administration costs associated with the completion of the SAR may be made e.g., printing costs for multiple copies of information.

The Trust aims to comply with requests for access to personal information as quickly as possible.

7.8.1 Timeframes for responding to a SAR

A full SAR response **must** be sent to the requestor within one calendar month starting from the day a SAR is submitted. This timeframe cannot be extended due to school holidays, however if the deadline for a response falls on a weekend or a bank holiday you can respond on the next day. If this deadline will not be met the requestor **must** be informed as soon as possible.

This deadline may be extended if the setting must wait for the requestor to provide identification, evidence of authority or any clarification needed. Therefore, if it takes 3 days for the requestor to provide identification the deadline can be extended by 3 days.

If the request is complex, the response time can be extended by up to a maximum of 2 further calendar months, making the response deadline 3 months in total. The ICO advise that a response should be made as soon as possible within the extended period. The ICO provides guidance on complex requests, it will be up to the Data Protection Officer in consultation with the relevant Designated Data Controller to assess whether a SAR is complex. Retrieving or redacting a lot of information does not necessarily make a SAR complex. If the SAR is being treated as complex the requestor **must** be notified in writing within one calendar month of the original request date.

8 Exempt Information

The Data Protection Act 2018 allows exemptions as to the provision of some information, refer to ICO guidance for more details, therefore all information will be reviewed prior to disclosure.

Third party information provided by someone else such as another employee, child, parent, Police, Local Authority, Health Care professionals or another school will need their consent before it can be disclosed. Likewise, any information which may cause serious harm to the physical, mental or emotional wellbeing of the pupil or any another person should not be disclosed, nor should information that would reveal that the child is at risk of abuse or information relating to court proceedings.

Where redaction has taken place (information blacked out/removed) a full copy of the information provided should be retained to establish, if a complaint is made, what was redacted and why.

Guidance on how to respond when refusing a request for personal information is available in **Appendix C**.

9 Dealing with Data Breaches

9.1 What is a data breach?

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

Personal data breaches can include, but are not limited to:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission; and
- loss of availability of personal data.

9.2 Breach detection, investigation, reporting and monitoring

When a security incident takes place, Trust staff will work quickly to establish whether a personal data breach has occurred. Where there has been breach, prompt steps will be taken to address and contain it.

Every member of staff dealing with personal data has a responsibility to report a data breach that they are either responsible for or become aware of to their setting's Data Controller as soon as possible. Any qualifying breach must be reported to the ICO within 72 hours.

To be effective in data management and ensure a robust breach detection, investigation, reporting and monitoring process a record of **all*** breaches will be kept, documenting:

- the facts relating to the breach,
- its effects
- the remedial action taken and
- the justification process for reporting to the ICO, or not
- the justification process for notifying individuals, or not
- the findings of any follow up investigation
- recommendations to prevent recurrence – e.g. better processes, training or other corrective steps.

A template for recording and reporting breaches from each location can be found in **Appendix D. *Whether they are reported to the ICO or affected individuals or not, see 9.4 below, all breaches will be documented.**

The data controllers in each setting are responsible for maintaining the breach log for their location and reporting breaches to the Data Protection Officer. The Data Protection Officer will then keep an overall log for the whole Trust, combining the data from each setting. It is the Data Protection Officer or their designated deputy who, having established all the facts, will make the decision about reporting to the ICO.

When using third party processors the requirements on breach reporting will be detailed in the contracts between the two parties, including the need for the processor to inform the Good Shepherd Trust without undue delay as soon as it becomes aware of a security breach, with the Trust's DPO then being responsible for notifying the ICO where relevant.

9.3 Assessing the Risk

Before deciding on what steps are necessary, further to immediate containment, an assessment of the risks which may be associated with the breach needs to be undertaken.

This includes an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

Every breach will be assessed on a case-by-case basis, looking at all relevant factors.

Potential adverse effects include emotional distress, or physical and material damage. Some breaches will not lead to risks beyond possible inconvenience, others can significantly affect individuals whose personal data has been compromised. The likelihood and severity of this risk needs to be established.

In assessing the risk, the following questions are considered:

- What type of data is involved?
- How sensitive is it? (ego sensitive due to personal nature (health records) or because of what might happen if it is misused (bank account details))
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data?
- Regardless of what has happened to the data, what could the data tell a third party about the individual?
- How many individuals are affected by the breach of their personal data?
- Who are the individuals whose data has been breached?
- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as loss of public confidence in the Good Shepherd Trust?

The outcome of the data breach risk assessment gives the following severity levels:

Minimal	• No material effect • Usually less than 1000 records • Breach notification required but little damage done
Moderate	• Low long-term impact • Usually, several thousands of records of semi sensitive information • Limited breach notification and financial exposure
Critical	• Legal and regulatory impact • Usually tens of thousands of records of moderate sensitive information involved • Some breach notification and financial loss
Severe	• Significant exposure to business, legal and or regulatory impact • Large amount of sensitive data lost (usually hundreds of thousands to millions of records) • Significant notification process and public image impact
Catastrophic	• Immense long-term impact on organisation and individuals • Large amount of highly sensitive information lost (10M+) • Use of lost information seen • Potentially massive financial impact for the organisation in remediation and related costs • Massive notification process

For further guidance use the ICO self-assessment tool.

9.4 External notification of breaches

9.4.1 Notification of Individuals

Where a breach is likely to result in a "high risk" to the rights and freedoms of individuals, that is it is likely to result in serious and substantial adverse consequences for the individual, Trust staff **must** inform those concerned directly and without undue delay.

Such a "high risk" means the threshold for informing individuals is higher than for notifying the ICO.

This is particularly important if there is a need to mitigate an immediate risk of damage to them i.e. enable individuals to take steps to protect themselves from the effects of a breach.

In contacting individuals, Trust staff will describe the nature of the personal data breach and, at least:

- the name and contact details of your data protection officer or other contact point where more information can be obtained
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects

Where possible, specific guidance and clear advice will be given to the effected individuals on steps they can take to protect themselves and what help Trust staff or contractors can provide. Depending on the circumstances this may include:

- forcing a password reset
- advice on setting strong, unique passwords
- advice on spotting phishing/smishing attempts or fraudulent activity on their accounts.
- Specific advice from the Trust's ICT provider

9.4.2 Notification of the Information Commissioner's Office

When a personal data breach with risk to people's rights and freedoms is identified it **must**, where feasible, be reported to the ICO within 72 hours of identification.

Notifying the ICO of a personal data breach

Where possible please report by calling the reporting helpline: 0303 123 113

When reporting by telephone is not possible (evenings/weekends) please report online

When investigating a breach, relevant Trust staff **must** prioritise and expedite the process urgently. The investigation **must** be given adequate resources to enable reporting to the ICO, if applicable, within the 72-hour deadline.

The external notification to the ICO should include:

- a description of the nature of the personal data breach including, where possible:
  - the categories and approximate number of individuals concerned; and
  - the categories and approximate number of personal data records concerned
- When the breach occurred
- Details of the risk assessment undertaken and its results
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.
- a description of the likely consequences of the personal data breach
- the name and contact details of the Data Protection Officer or other contact point where more information can be obtained

The UK GDPR recognises that it will not always be possible to investigate a breach fully to understand exactly what has happened and what needs to be done to mitigate it within 72 hours. Therefore, reporting can be done in phases if further information is submitted as soon as possible and without undue delay. If such an extension is required this should be explained at the point of the initial notification with a timeframe of when further submission is expected.

10 Data Protection Impact Assessments

The Good Shepherd Trust has a legal obligation to undertake data protection impact assessments (DPIA) before carrying out any processing which is "likely to result in high risk" to individuals' interests. This is a key element of data protection by design and helps organisations like our Trust focus on accountability while using a risk-based approach to compliance.

The ICO template available at **Appendix E** will be used to help get this process right. If a completed DPIA identifies a high risk which we cannot mitigate, we must consult the ICO before proceeding.

A DPIA is a process to systematically analyse processing and help identify and minimise data protection risks. It must:

- describe the processing and the purpose for data processing
- assess necessity and proportionality of what is planned
- identify and assess risks to individuals; and
- identify any measures to mitigate those risks and protect the data.

It does not have to eradicate the risk but should help to minimise risks and consider whether they are justified or not. A DPIA may cover a single processing operation or a group of similar processing operations.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – whether physical, material or non-material - to individuals or to society at large.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. It should look at risk based on the specific nature, scope, context and purposes of the processing. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

In particular, the Trust must do a DPIA if plans to:

- use systematic and extensive profiling with significant effects
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

The ICO also requires a DPIA if new projects:

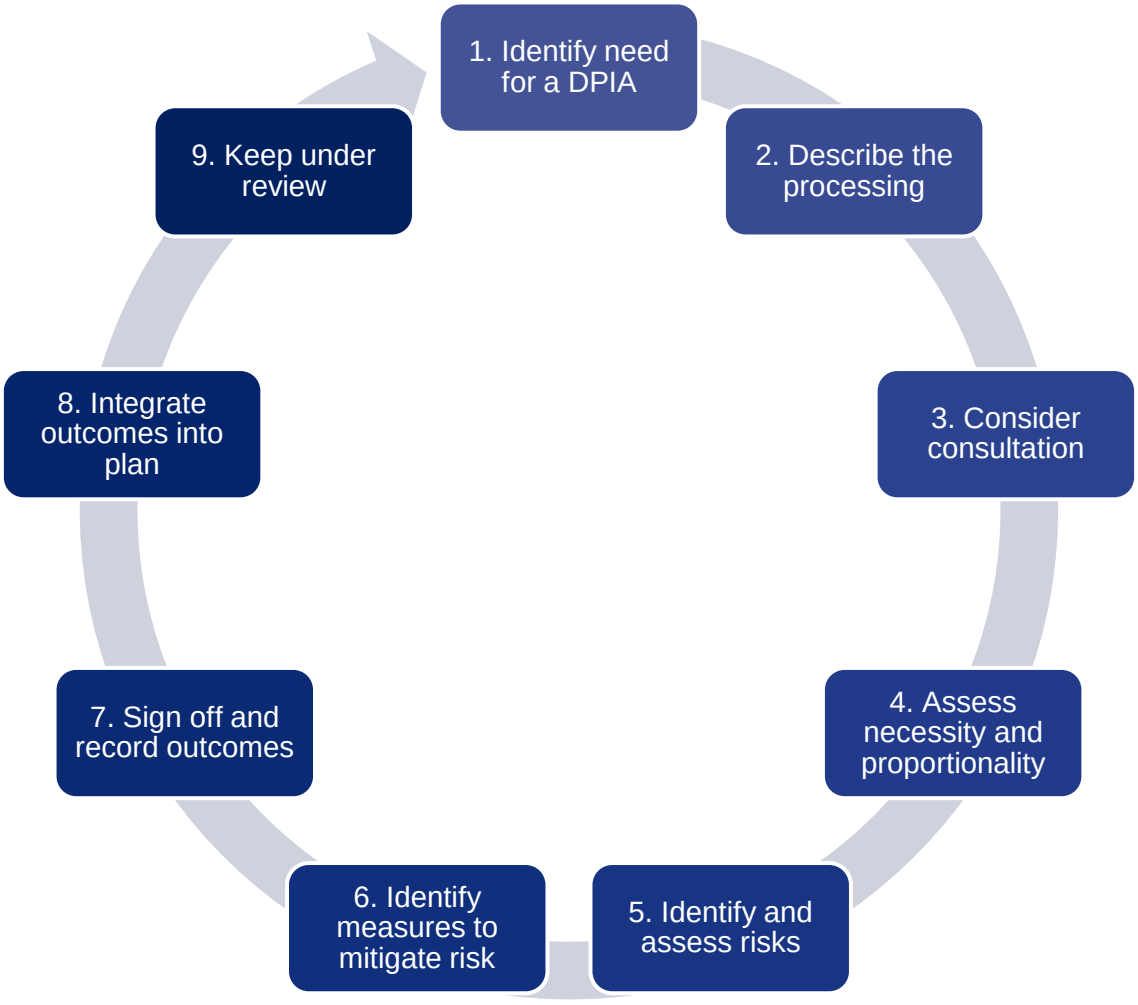
- use new technologies
- use profiling or special category data to decide on access to services
- profile individuals on a large scale
- process biometric data
- process genetic data
- match data or combine datasets from different sources
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')
- track individuals' location or behaviour
- profile children or target services at them; or

- process data that might endanger the individual's physical health or safety in the event of a security breach.

The Trust's board of directors and senior leaders should think carefully about doing a DPIA for any other processing which is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals.

Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of personal data.

A DPIA should begin early in the life of a project, before processing starts, and it should run alongside the planning and development process. It should include these steps:



In undertaking a DPIA the advice of the Trust Data Protection Officer (DPO) must be sought along with consulting individuals, stakeholders and relevant experts as appropriate.

The DPO should be engaged in the following tasks/ decisions:

- whether or not to carry out a DPIA
- what methodology to follow
- whether to carry out the DPIA in-house or outsource it
- what safeguards (incl. technical & organisational measures) to apply to mitigate risks to data subjects' rights & interests
- whether the DPIA has been done correctly and whether its conclusions (to go ahead or not with the processing and what safeguards to apply) are compliant with the UK GDPR

If a DPIA that identifies a high “residual risk” (after mitigating measures have been taken) has been carried out, and further measures to reduce this risk cannot be take then the ICO must be consulted **before** the project starts. Processing **cannot** go ahead until this has happened and a response received.

It’s important to embed DPIAs into the Trust’s processes and ensure the outcome can influence plans. Measures identified within the DPIA process should be integrated into the project delivery. A DPIA is not a one-off exercise and should be seen as an ongoing process, kept under regular review as illustrated above.

10.1 Surveillance Cameras

When it involves surveillance cameras, the government guidance and template, Data protection impact assessments for surveillance cameras (**Additional Document F**) will be used. Kym Allan Health and Safety Consultants also provide model procedures for surveillance cameras if required.

11 Retention of Data

The Trust’s Records Management Policy and Procedures provides more guidance and information on how, when and why data is retained and disposed of. This is based on advice from the Information Records Management Society Toolkit for Schools.

Personal data may only be kept for as long as it is needed, how long this is will depend on the circumstances and the reasons it was obtained. Different categories of data will be retained for different periods of time

List of Appendices and Additional Documents

Appendix A1-4: Privacy Notices

- Workforce
- Governance Roles
- Pupils and Families
- Pupils (primary)

Appendix B: SAR Form
Appendix C: Refusing a request for personal data
Appendix D: Data Breach Log
Appendix E: Data Protection Impact Assessment Template

Additional Documents

Additional Document F: ICO DPIA for Surveillance Cameras
KAHSC Model Surveillance Cameras procedures

All appendices are available on the members' area of the Trust website, the additional documents are available from the ICO and Kym Allan Health and Safety Consultants.

The Pupils and Families Privacy Notice is available from all Trust websites. The Workforce Privacy Notice is available from the Trust's website and via the Trust's payroll app and portal.