Data protection and Freedom of Information Policy

Recommended by Operations Director:	June 2025
Approved by Operations Committee:	June 2025
Ratified by Trustee board:	July 2025
Review Due:	Summer 2026

Contents

1. Policy Statement

We must protect the data and information we hold on any individual and will do so under the guidance of the law.

2. Definitions

Term	Definition
Trust	is Marlow Education Trust, Sir William Borlase's Grammar Trust, West Street, Marlow, SL7 2BR
Department of Education (DfE)	is the government department which deals with education
Local Authority (LA)	is Buckinghamshire County Council
Chair of Trustees	is Sarah Cooper
CEO	is Kevin Ford
Trust	is Marlow Education Trust, Sir William Borlase's Grammar Trust, West Street, Marlow, SL7 2BR
Trusts Data Protection Officer (DPO)	is Satswana Ltd, Suite G12 Ferneberga House, Alexandra Road, Farnborough, GU14 6DQ. admin@satswana.com
Data Protection Act (DPA)	The Data Protection Act 2018 makes a provision about the processing of personal data, which is subject to GDPR, with an amendment in 2023.
Freedom of Information Act (FOI)	The Freedom of Information Act 2000 discloses information held by public authorities or persons providing services for them and amends the Data Protection Act.
UK General Data Protection Regulation (GDPR)	which applies across the European Union (including in the United Kingdom)
Educations Act (EA)	The Education Act 1996 consolidates the Education Act 1944 and certain other educational enactments.
Information Commissioners Office (ICO)	This organisation ensures compliance with the Data Protection Act, Freedom of Information Act, and GDPR and handles formal complaints.
Personal Data	Any information relating to an identified or identifiable living 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.

Term	Definition
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
Serious Harm Test	is a legal threshold used to determine if a statement or action has caused significant negative consequences, particularly in relation to reputation, health, or financial standing. It's a key concept in defamation law, data protection, and child protection, among other areas
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data Subject	The identified or identifiable individual whose personal data is held or processed.
Data Controller	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing personal data.
Data Processor	means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the 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
Electronic Platform	An electronic platform is any means the trust communicates. This could include, but is not limited to, Email, Online Portals, and Social Media platforms.

Term	Definition
Sensitivity Labels	Are labels applied to electronic documents to support data protection within the trust? The following labels are active: ● Highly Confidential – Does not leave the site. ● Confidential – Can leave the site but must be encrypted. ● General – Can leave the site. ● Personal – Discretion of the end user. ● Public – Is available to the public.

3. Aims & Objectives

This policy aims to provide a model set of guidelines to enable staff, parents, and children to understand:

- The law regarding personal data.
- How personal data should be processed, stored, archived, and deleted/destroyed.
- How staff, parents and children can access personal data.

In addition, there is brief guidance at the end of this policy on FOI, which covers other information held by trusts.
The policy's objective is to ensure that the trust acts within the requirements of the DPA when retaining and storing personal data and making it available to individuals, and that responding to enquiries for other information is also legal under the FOI.

4. 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 ICO on the UK GDPR and the DFE on Generative artificial intelligence in education.
It meets the requirements of the following:

- Protection of Freedoms Act 2012 when referring to our use of biometric data.
- For the use of surveillance cameras and personal information.

Academies, including free trusts:

- This policy complies with our funding agreement and articles of association.

5. The Data Controller

Our Trust processes personal data relating to parents and carers, pupils, staff, trustees governors, visitors, and others; therefore, it is a data controller. The Trust is registered with the ICO [ICO Reg Number] and has paid its data protection fee to the ICO, as legally required.

6. Roles and responsibilities

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

a. Board of Trustees

The board of trustees ensures that our trust complies with all relevant data protection obligations.

b. Data protection officer

The 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.
They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board of trustees with 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.

c. CEO

Acts as the representative of the Data Controller on a day-to-day basis, but can delegate the responsibility to either the Director of Operations or Data Protection Coordinator.

d. All staff

Staff are responsible for:

- Collecting, storing and processing any personal data under this policy.
- Informing the trust of any changes to their data, such as a change of address.
- Contacting the DPO in the following circumstances:
    - If you have any questions about the operation of this policy, data protection law, retaining personal data, or keeping personal data secure,
    - If they have any concerns about this policy not being followed,
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK.

- If there has been a data breach.
- Whenever they engage in a new activity, it may affect the privacy rights of individuals.
- If they need help with contracts or sharing personal data with third parties.

7. Data protection principles

The UK GDPR is based on data protection principles that our trust must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is required for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

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

8. Collecting personal data

a. Lawfulness, fairness and transparency

We will only process personal data where we have 1 of 6 ‘lawful bases’ (legal reasons) to do so under data protection law:

- 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 must be processed to ensure the vital interests of the individual or another person, i.e. to protect someone’s life.
- The data needs to be processed so that the trust, as a public authority, can perform a task in the public interest or exercise its official authority.
- The data needs to be processed for the legitimate interests of the trust (where the processing is not for any tasks the trust performs as a public authority) or a third party, provided the individual’s rights and freedoms are not overridden.
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given explicit consent.

For special categories of personal data, we will also meet 1 of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent.
- The data must be processed to perform or exercise obligations or rights concerning employment, social security or social protection law.
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made manifestly public by the individual.
- The data needs to be processed for the establishment, exercise or defence of legal claims.
- The data needs to be processed for substantial public interest as defined in legislation.
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law.
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or any other person obliged to confidentiality under law.
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

We will meet both a lawful basis and a condition set out under data protection law for criminal offence data. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given consent.
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made manifestly public by the individual.
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights.
- The data needs to be processed for substantial public interest as defined in legislation.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

a. Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. When we first collect their data, we will explain these reasons to the individuals.
If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.
Staff must only process personal data where necessary to do their jobs.
We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.
In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done under the trust's record retention schedule.

9. Sharing personal data

We will not usually 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 – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils, for example, IT companies or software companies to provide the educational service. When doing this, we will:
    - Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law. Where appropriate we will record the service, and if software poses a risk or uses special category data, a data protection impact assessment will be completed.
    - 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 deliver.

We will also share personal data with law enforcement and government bodies where we are legally required.
We may also share personal data with emergency services and local authorities to help them respond to an emergency that affects any of our pupils or staff.
Where we transfer personal data internationally, we will do so under UK data protection law.

10. Subject access requests and other rights of individuals

a. 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 data is being processed
- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data are concerned.
- Who has the data 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 complain is by following the Trusts complaint policy. If the outcome is unsatisfactory, you can contact 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 are provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

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

If staff receive a subject access request in any form, they must immediately forward it to the DPO.

b. Children and subject access requests

Personal data about a child belongs to that child, 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. A professional who knows the child will be required to make this decision.

For primary trusts:

Children under 13 are generally not considered 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.

For secondary trusts:

Children aged 13 and above are generally 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 not be granted without the express permission of the pupil. A pupil's ability to understand their rights will always be judged case-by-case, by a responsible person known to them in trust.

c. Responding to subject access requests

When responding to requests, we:

- Will 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 (or receipt of the additional information needed to verify identity, where relevant).
- Will provide the information free of charge, unless additional physical copies are required or the request insists on it being posted. The costs will be proportionate to the cost of copying and postage..
- 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.

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 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.

If the request is manifestly unfounded, excessive or vexatious, we may refuse to act on it or charge a reasonable fee to cover administrative costs. We will consider whether the request is repetitive 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 seek to enforce their subject access right through the courts.

d. Other data protection rights of the individual

In addition to the right to make a subject access request (section 10), and to receive information when we are collecting their data about how we use and process it (see section 8), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their data (in certain circumstances)
- Prevent the use of their data for direct marketing
- Object to processing that has been justified based on 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 data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their 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 must immediately forward it to the DPO.

11. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 calendar days of receipt of a written request. The educational record does not consist of SEN related documentation, behaviour logs, minutes of meetings and communications.
If the request is for a copy of the educational record, the trust may charge a fee to cover the cost of supplying it, fees are broken down in Appendix 1.
This right applies as long as the pupil concerned is under eighteen.
There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

12. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive trust dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012.
Parents will be notified before any biometric recognition system is put in place or before their child first takes part in it. The trust will get written consent from at least one Parent before we take any biometric data from their child and process it.
Parents and pupils can choose not to use the trust's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for trust dinners in cash at each transaction if they wish [amend this example as applicable].
Parents 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 continues 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).
Where staff members or other adults use the trust'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 trust will delete any relevant data already captured.

13. CCTV

We may use CCTV in various locations around the trust site to ensure safety. We will follow the ICO's guidance for the use of CCTV and comply with data protection principles.
We do not need to ask individuals' permission to use CCTV, but we clarify where individuals are being recorded. Security cameras are visible and accompanied by prominent signs explaining that CCTV is in use.
CCTV is a tool to ensure safety of the trust and allow the trust to manage security or behavioural incidents, CCTV is not available to parents freely, with out the approval from the Executive Headteacher or COT.
Any enquiries about the CCTV system should be directed to the Data Protection Coordinator or Business Manager.

14. Photographs and videos

As part of our trust activities, we may take photographs and record images of individuals within our trust.
Primary trusts:
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 picture and/or video will be used to both the parent/carer and the pupil.

Data protection legislation does not cover any photographs and videos taken by parents/carers at trust events for their own personal use. However, we will ask that photos or videos with other pupils not be shared publicly or on social media for safeguarding reasons unless all the relevant parents/carers agree.

Secondary trusts:

We will obtain written consent from Parents or pupils aged eighteen and over, for photographs and videos of pupils for communication, marketing and promotional materials. Where we need parental consent, we will clearly explain how the Parent and the pupil will use the photograph and/or video. Where we don't need parental consent, we will clearly explain to the pupil how the picture and/or video will be used.

Data protection legislation does not cover any photographs and videos Parents took at trust events for personal use. However, we will ask that photos or videos with other pupils not be shared publicly on social media for safeguarding reasons unless all the relevant Parents (or pupils where appropriate) agree to this.

All trusts add and adapt to reflect your trust's uses of photographs and videos for communication, marketing and promotional materials:

Where the trust takes photographs and videos, uses may include:

- Within the Trust, on notice boards, trust magazines, brochures, newsletters, etc.
- Outside of Trust, by external agencies such as the trust photographer, newspapers, campaigns
- Online on our trust and trust 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 this way, we will not accompany them with any other personal information about the child to ensure they cannot be identified.

15. Artificial Intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT, Copilot and Google Gemini. The Trust recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

No one will be permitted to enter such data into unauthorised generative AI tools or chatbots to ensure that personal and sensitive data remains secure.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, the Trust will treat this as a data breach and will follow the personal data breach procedure outlined in Appendix 2.

16. Data protection by design and default

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

- Appointing a suitable DPO and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only personal data necessary for each specific purpose of processing should be processed, and it should always be in line with the data protection principles set out in the relevant data protection law (see section 7).
- Completing data protection impact assessments where the trust's processing of personal data presents a high risk to the rights and freedoms of individuals, and when introducing new technologies that handle sensitive or special category data.
- A Processor List will be available for low or medium risk technologies that do not handle sensitive or special category data.
- Integrating data protection into internal documents, including this policy, any related policies and privacy notices.
- Biannually, staff members will be trained on data protection law, this policy, any related policies, and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Appropriate safeguards will be put in place if we transfer personal data outside the UK, where different data protection laws may apply.
- Maintaining records of our processing activities, including:
    - For the benefit of Data Subjects, we make available the name and contact details of our trust and DPO and all information we must share about how we use and process their data (via our privacy notices).
    - For all Personal Data that we hold, we maintain an internal record of the type of data, type of Data Subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure.

17. Data security and storage of records

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

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, staffroom tables, or anywhere else with general access.

- Where personal information needs to be taken off-site, staff must sign in and out from the trust office.
- Passwords at least 10 characters long, containing letters and numbers, are used to access trust computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from different sites.
- Encryption software protects all portable devices and removable media, such as laptops and USB devices.
- Staff, pupils or governors who store personal information on their devices are expected to follow the same security procedures as for trust-owned equipment [insert name of 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 9)

18. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or outdated 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 dispose of records on the trust's behalf safely. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

19. Personal data breaches

The trust will make all reasonable endeavours to ensure that there are no personal data breaches.
In the unlikely event of a suspected data breach, we will follow the procedure in Appendix 2. When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such violations in a trust context may include, but are not limited to:

- A non-anonymised dataset published on the trust website shows the exam results of pupils eligible for the pupil premium.
- Safeguarding information from being made available to an unauthorised person.
- The theft of a trust laptop containing non-encrypted personal data about pupils.

20. Training

All staff and governors receive data protection training as part of their Continuing Professional Development (CPD), which includes updates on changes to legislation, guidance, or the trust's processes.

21. Mental Health and Wellbeing

The trust has an established culture that promotes and enhances the positive mental health of the whole trust community. We recognise that healthy relationships underpin positive mental health and have a significant impact on learning, health, and well-being. We champion the expectation that 'mental health is the individual's responsibility, supported by the whole trust community.' Because of this, where requests from a data subject are demonstrably vexatious, manifestly unfounded or excessive, we may refuse to respond to a SAR.

22. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.
This policy will be reviewed annually and approved by the board of trustees.

23. Publication Schemes - Freedom of Information

All public authorities, including trusts, are required under the Freedom of Information Act to adopt a publication scheme that the Information Commissioner has approved.
There is currently one approved model publication scheme, which has been produced by the Information Commissioner's Office (ICO).
Trusts must adopt the ICO's model scheme and make it publicly available.

24. Appendix 1 – Procedure for Access to Personal Information

Right of access to information

There are three distinct rights of access to personal information held by the Trust or trusts. Under the GDPR and the Data Protection Act 2018, an individual (e.g., a pupil, parent, or member of staff) has the right to request access to their personal information. In certain circumstances, a parent may make a request on behalf of their child (see explanation below).
The Education (Pupil Information) (England) Regulations 2005 grant parents the right to access their child's curricular and educational records.
Keeping children safe in education in England involves statutory guidance for trusts and colleges, outlining legal duties to safeguard and promote the welfare of children.

Processing a request

Requests for personal information must be made either in writing, verbally or via social media. If the initial request does not identify the required information, clarification should be sought.
The identity of the Data Subject must be verified before any personal information is disclosed, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting the production of the following (this list is not exhaustive):

- Passport
- Driving licence
- Utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement
- Parental Responsibility

Individuals are entitled to be told if we are processing their personal information, obtain a copy of that information and other supplementary information – see below.
In addition to a copy of their data, you also have to provide individuals with the following information:

- The purposes for processing their data.
- The categories of personal data concerned;
- The recipients or categories of recipients to whom you disclose the personal data;

- your retention period for storing the personal data or, where this is not possible, your criteria for determining how long you will store it;
- the existence of their right to request rectification, erasure or restriction, or to object to such processing;
- the right to complain to the ICO or another supervisory authority; information about the source of the data, where it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling); and
- The safeguards you provide if you transfer personal data to a third country or international organisation.

Information can be viewed at the trust, with a member of staff on hand to help and explain matters if requested or provided at a face-to-face handover. The views of the applicant should be taken into account when considering the method of delivery. If the applicant has asked for the information to be posted, then special next-day delivery or recorded delivery postal service must be used.

Information relating to children

Children have the same right to access their personal information as adults and the same privacy rights. There is no minimum age in English law; however, current practice accepts that, provided a child is mature enough to understand their rights, a child of or over thirteen shall be considered capable of giving consent. This does not rule out receipt of a valid request from a child of a younger age, as each request should be considered on its merits individually.
When a subject access request is received from a child, it will need to be judged whether the child can understand the implications of their request and the information provided. If the child understands, their request will be handled the same way as an adult's.
Suppose a parent or legal guardian requests on behalf of a child age 13 and over. In that case, the request will only be complied with when assurances are received that the child has authorised the request and that their consent was not obtained under duress or based on misleading information. If the child does not understand, a request from a parent or legal guardian for the child's information will only be complied with when assurances are received that they are acting in the child's best interests.

Response time GDPR & DPA

The response time for complying with a subject access request is as follows:

- 72 hours to acknowledge receipt of your request.
- We can ask for you to narrow down your request.
- One month following the date of receipt. The timeframe does not begin until the trust has received all the information necessary to comply with the request, i.e., proof of identity. If the scope of the request changes we have the right to restart the request.

- If the requests are complex or numerous, we may extend the timeframe by a further two months. If this is the case, you will be informed in writing.

Education Regulations

Requests for information from parents for access to information classified as part of the education record must be responded to within fifteen calendar days. This includes the essential education information, Child and Parental details, Absence details and progress for clarification.

Charges

If the information requested is personal and does not include information contained within educational records, the trust cannot charge unless the request is manifestly unfounded or excessive.
The Trust may charge a “reasonable fee” for the administrative costs of complying with the request. The Trust can also charge a reasonable fee if an individual requests further copies of their data following a request and any postage fees to send Special Delivery. The amount charged will depend on the number of pages provided. The fees work on a sliding scale, as below.

Number of pages	Fee (£’s)
1-19	£1.00
20-29	£2.00
30-39	£3.00
40-49	£4.00
50-59	£5.00
60-69	£6.00
70-79	£7.00
80-89	£8.00
90-99	£9.00
100-149	£12.50
150-199	£15.00
200-249	£17.50

Number of pages	Fee (£'s)
250-299	£20.00
300-349	£25.00
350-399	£30.00
400-449	£35.00
500+	£40,00

Exemptions

Some exemptions to the right to subject access apply in certain circumstances or to certain types of personal information.
Included below are some of the exemptions that apply to a trust. This is not an exhaustive list;

Third-Party information

If the information held identifies other people, then it will sometimes be right to remove or edit that information not to reveal the identity of the third parties unless the third parties have agreed to the disclosure (This is less likely to apply to information identifying teachers or other professionals unless disclosing it would cause them serious harm) reasonable steps will be taken to obtain third-party consent for disclosure.
Where redaction (information edited/removed) has taken place, a full record of the information provided should be retained to establish what was redacted and why an exemption was applied.
When the Trust is not the Data Controller or if the third parties do not consent, cannot be located, or have no response, data will not be disclosed as the Trust must still adhere to the law (it is not our data to share) and the statutory timescale.

Information likely to cause serious harm or distress

The Trust adopts the Serious Harm Test on any information which may cause serious harm to the physical or mental health of the pupil or another individual involved, this information will not be disclosed or it wil be redacted from the document, any information that would reveal that the child is at risk of abuse or information relating to court proceedings will also not be disclosed.

Crime and Disorder

Suppose the disclosure of the information will likely hinder the prevention or detection of a crime. In that case, the information should be withheld in the prosecution or apprehension of offenders or the assessment or collection of any tax or duty.

Legal professional privilege

If the information is general legal advice related to anticipated or pending legal proceedings, it is subject to ‘legal professional privilege’. The disclosure of any communication to or from a legal advisor to another person (including the Data Subject) should not take place unless this has first been discussed with the legal advisor concerned.

References

The right of access does not apply to references given (or to be given) in confidence.

Absence of or invalid consent to disclosure

If the Data Subject is considered incapable of giving valid consent to disclosure (i.e. they cannot understand the nature/implications of the access request), or if it is suspected that the consent was obtained under duress by someone acting on their behalf, or based on misleading information, then access will be refused.

Complaints

Complaints about the above procedures should be made to the Data Protection Officer (DPO), who will decide whether it is appropriate for the complaint to be dealt with under the trust’s complaint procedure.

25. Appendix 2 – 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, governor or Data Processor must immediately notify the DPO or the Data Protection Coordinator.
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will apply the Serious Harm Test to consider whether personal data has been accidentally or unlawfully processed:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- Staff and governors will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.
- If a breach has occurred or is likely to happen, the DPO will alert the Headteacher and the COG.
- The Trust and DPO will make all reasonable efforts to contain and minimise the breach's impact. Relevant staff members or Data Processors should support the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT Representative).
- The DPO will assess the potential consequences (based on how serious and likely they are to happen) before and after implementing steps to mitigate the impacts.
- Using the Serious Harm Test, the DPO will determine whether the breach must be reported to the ICO and the individuals affected.
- The DPO will document the decisions (either way), in case the decisions are challenged later by the ICO or an individual affected by the breach. Documented decisions are stored.
- Where the ICO must be notified, the DPO will do this via the ‘report a breach’ page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the Trust’s awareness of the breach. As required, the DPO will set out:
    - A description of the nature of the personal data breach, including, where possible:

        - The categories and the approximate number of individuals concerned.
        - The categories and an 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 DPO will report as much as possible within 72 hours of the trust's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- Where the trust is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - 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 DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals, for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the following:
    - 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.
- The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

- The DPO and Headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the trust to reduce risks of future breaches.

Actions to minimise the impact of data breaches

We outline below the steps we might take to mitigate the impact of different types of data breaches should they occur, with a particular focus on breaches involving highly sensitive information. We will assess the effectiveness of these actions and modify them as necessary following any data breach.

Set out the relevant actions you will take for different types of risky or sensitive personal data your trust processes. For example:

- Sensitive information being disclosed via email (including safeguarding records)
- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email, the Trust will ask the IT Representative to attempt to recall it from external recipients and remove it from the trust's email system (retaining a copy if required as evidence).
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the Trust will consider whether it's appropriate to 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 Trust will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.
- The Trust will conduct 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 data be removed from their website and deleted.
- If safeguarding information is compromised, the Trust will inform the DSL and discuss whether it should disclose any or all of its local safeguarding partners.

Other types of breaches that you might want to consider could include:

- Details of pupil premium interventions for named children are published on the trust website.
- Non-anonymised pupil exam results or staff pay information being shared with governors.

- A trust laptop containing non-encrypted sensitive personal data is being stolen or hacked.
- The trust's cashless payment provider was hacked, and parents' financial details were stolen.
- Hardcopy reports were sent to the wrong pupils or families.