MOWBRAY
Education Trust

Data Protection Policy

June 2023

Document Type	External and available to all staff
Last Review Date	Summer Term 2023
Next Review Date	Summer Term 2024 (Annually)
Owner	Executive Lead for Governance and Compliance
Author	Executive Lead for Governance and Compliance
Version	3.1
Status	Approved by Audit Finance and Risk Committee June 2023

Contents

This policy covers all our educational establishments:

- Ab Kettleby Primary School
- Brownlow Primary School
- The Grove Primary School
- Iveshead School
- John Ferneley College
- Oasis Family Centre
- Sherard Primary School
- Somerby Primary School

Where this policy states 'school' this means any of our educational establishments and the wider Trust.

1) Aims

Our Trust aims to ensure that all personal data collected about school staff, pupils, parents, governance volunteers, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.
This Data Protection policy is the overarching policy for data security and protection for Mowbray Education Trust (hereafter referred to as 'us', 'we' or 'our').

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

2) Legislation and guidance

This policy meets the requirements of the:

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

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

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with our funding agreement and articles of association.

3) Definitions

TERM	DEFINITION
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.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: › Racial or ethnic origin › Political opinions › Religious or philosophical beliefs › Trade union membership › Genetics › Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes › Health – physical or mental › Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4) The data controller

The Mowbray Education Trust (the trust) processes personal data relating to parents, pupils, staff, governance volunteers, visitors and others, and therefore is a data controller.

The trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5) Roles and responsibilities

This policy applies to **all 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.

5.1 Trust board

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

5.2 Data protection officer

The Data Protection Officer (DPO) is the first point of contact for individuals whose data the school processes, and for the ICO. Our DPO is:

SPS DPO Services

Email: sps-dpo-services@isystemsintegration.com

Correspondence address:

SPS SPO Services
I Systems Integration
Devonshire House
29-31 Elmfield Road
Bromley
Kent
BR1 1LT
Tel: 0208 050 1387

5.3 Operations Department

The trust and individual educational establishments will delegate oversight of the implementation of this policy, monitor our compliance with UK data protection law, and develop related policies and guidelines where applicable to the Trust Operations Department.

In conjunction with the DPO as required, they will provide reports of their activities directly to the Audit, Finance and Risk committee of the Trust Board and, where relevant, report to the Board their advice and recommendations on school data protection issues.

The Operations Department acts as the representative of the data controller on a day-to-day basis. They should seek guidance from the DPO as required. Contact them;

Trust Operations Department, Mowbray Education Trust, c/o John Fernley College, Scalford Road, Melton Mowbray, LE13 1LH, Tel: 01664 565901 or email dataprotection@mowbrayeducation.org .

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the Operations Department and/or DPO in the following circumstances:
    - With any questions about the operation of this policy, UK data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6) Data protection principles

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

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

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

7) Collecting personal data

7.1 Lawfulness, fairness and transparency

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

- The data needs to be processed so that the school can **fulfil a contract** with the

individual, or the individual has asked the school to take specific steps before entering into a contract
    - The data needs to be processed so that the school can **comply with a legal obligation**
    - The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
    - The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, and carry out its official functions
    - The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**
- For special categories of personal data, we will also meet one of the special category conditions for processing under UK data protection law.

  - The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
  - The data needs to be processed to perform or exercise obligations or rights in relation to **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 reasons of **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 by 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

  For criminal offence data, we will meet both a lawful basis and a condition set out under UK data protection law. 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 reasons of **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 UK 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.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

John Ferneley College & Iveshead only - If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

7.2 Limitation, minimisation and accuracy

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

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

Staff must only process personal data where it is necessary in order to do their jobs. We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased at the earliest possible opportunity after the inaccuracy is known and confirmed.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in line with the Trust's Data Retention Policy, details of which can be requested by e- mailing operations@mowbrayeduction.org .

8) Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils
  – for example, IT companies.

When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

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

9) Subject access requests and other rights ofindividuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests must be submitted in writing, either by letter, or email to the Operations Department. They should include:

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

If staff receive a subject access request, they must immediately forward it to the Operations Departments.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

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

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

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

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

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at anytime
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the Operations Department. If staff receive such a request, they must immediately forward it to the Operations Department.

10) Parental requests to see the educational record

Whilst within academies; parents, or those with parental responsibility, DO NOT have a legal right to free access to their child's educational record (which includes most information about a pupil), however we will usually provide this if there is no deemed reason not to do so. Requests are considered on a case-by-case basis. Please contact the Headteacher of the individual school in the first instance.

11) Biometric recognition systems

We do not currently use, nor plan to use, any biometric recognition systems.

12) CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Headteacher of the individual

school in the first instance.

13) Photographs and videos

At school, on occasions we take photographs and film pupils as part of our core activity of education. This occurs as part of normal teaching, learning, assessment and safeguarding procedures; and as such we do not need to seek consent for these activities.

However, in addition to this, we really value using photographs and videos of pupils to showcase what they do in school and show what life at our school is like to others. Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters,etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

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

To obtain consent for this we have a 'Consent for images' section within our admissions .

This form is valid for the period of time that your child is on roll at school. Images will not be republished by the school once the child has left; but please note that images would remain on social media 'timelines' indefinitely and on the school website until updated.

Once you have submitted the consent form, if you wish to make any changes to it or to remove/refuse consent, please contact the individual school office.

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

14) Data protection by design and default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant UK data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the Operations Department will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices

- Regularly training members of staff on UK data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of course completion
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:

    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, 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

15) Data security and storage of records

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

16) Disposal of records

Personal data that is no longer needed will be disposed of securely in accordance with UK data protection law. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with UK data protection law.

17) Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the event of a suspected data breach, we will liaise with our DPO. When appropriate, the DPO will report the data breach to the ICO within 72 hours.

18) Training

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

19) Links with other policies

This data protection policy is linked to our: https://www.mowbrayeducation.org/policies

- Freedom of information publication scheme
- Online Safety Policy
- ICT & Internet Acceptable Use Policy

- Remote Learning Policy
- School Safeguarding Policies (see school websites)
- Social Media Policy

Log of Changes to Document

Version	Date	Page	Change	Approver:
V1.0	25/05/18	All pages	Approved by MET Board	Group Operations Manager
V2.0	Oct-19	All pages	Annual Review with the following changes made; **Page 1 –** Table updated	MET Group Operations
			Page 2 – Full contents table added **Page 3** – 'Aims' updated with new wording **Page 7 – Sec.7.2 –** Added reference to 'Data Retention Policy' and how to obtain details **Page 11** – **Sec. 14** - 5th bullet point - Records reference changed from 'attendance' to 'course completion' as on- line training now required every 2 years **Page 12** – Log of changes table added.	
V2.0	Oct-19	All pages	Draft for Annual approval	MET Audit Committee
V2.0	31.10.19	All pages	Approved	MET Trust Board
V2.0	Aug-20	All pages	Annual Review with the following changes made: **Page 1 –** Table updated **Page 5 –** DPO Tel. number added	Group Data Protection Lead
V2.0	Sept-20	All pages	For re-approval	MET Trust Board
V2.0	Nov-20	All pages	Re-approved Section 5.1 – addition of Trust wording Section 1, 4 & 18 – Governors changed to governance volunteers to reflect new Governance model/terminology	MET Trust Board

V2.0	Apr-21	All pages Sec. 1 Sec. 2 Sec. 5.4 Sec. 5.3 Sec. 6 Sec. 7.1 Sec. 7.2 Sec. 8 Sec. 9.1 Sec. 9.3 Sec. 13 Sec. 14 Sec. 15 Sec. 16 Sec. 19	Removed links to EU legislation and replaced with ref to 'UK data protection law' Addition of Annually to review period Added link to the UK GDPR legislation Changed wording around transferring personal data outside the 'European Economic Area' (EEA) to transferring it outside the 'UK' Additional Data Lead details and grammar correction Replaced 'GDPR' with 'UK GDPR' Additional wording added for special categories and criminal offence data Addition of keeping data accurate Changed wording around data protection law to 'UK data protection law' Addition 3 more SAR rights Updated wording on when we may not disclose information and when we refuse a request Updated and added wording ref consent and photo'/video's taken by parents Changed wording around transferring personal data outside of the 'European Economic Area (EEA)' to transferring it outside of the 'UK' Added wording about using 3rd party to safely dispose of records Added UK data protection law (AFR feedback) Addition of Sec.19 – links with other policies	AFR (Jun-21)
V2.0	Oct-21	All	Annual review – no changes made	Data Protection Lead
V3.0	Jun-22	All Intro Sec 19 Sec 7.2	General readability edits Added in reference to cover Iveshead Added in new Social Media Policy link Wording improved to remove 'when appropriate' to 'possible opportunity after the inaccuracy is known and confirmed'.	MET Trust Board
V3.1	Jun23	P3 P5 Whole document	1.0 Addition of wording to define aim of policy. 5.1 Changed delegated oversight department for the Trust from Group Data Protection Lead to Operations Department. Change of contact for staff from DPL to Operations Department.	