

General Data Protection Policy

Date written

April 2020

Authorised by

Governing Board

Review Date

Summer 2023





Contents

Contents.....	2
1 Introduction	3
2 Aims	4
3 Legislation and guidance.....	4
4 Definitions	4
5 The data controller	5
6 Roles and responsibilities	5
7 Data protection principles	6
8 Collecting personal data.....	6
9. Sharing personal data	7
10. Subject access requests and other rights of individuals	8
11. Freedom of Information.....	10
12 Parental requests to see the educational record.....	14
13 CCTV.....	14
14 Photographs and videos	14
15 Data protection by design and default.....	14
16 Data security and storage of records	15
17 Disposal of records	15
18 Personal data breaches.....	16
19 Training	16
20 Monitoring arrangements.....	16
Appendix A from our Data Protection Policy: Personal data breach procedure.....	17
Appendix B from our Data Protection Policy: Privacy notice for parents/carers	20
Appendix C from our Data Protection Policy: Privacy notice for staff	24
Appendix D from our Data Protection Policy: Privacy notice for governors and volunteers	28
Appendix E from our Data Protection Policy: Record Retention Schedule.....	33



1 Introduction

This document sets out how our school uses data across all of its operations so that we can achieve our school aims and objectives. We do this within our five PROUD Values described below.



Our children are confident learners, they work hard to succeed with every challenge.



Our children show respect for themselves and other people in our community, our country and our world.



Our children love learning and are keen to learn in our school, at home and in the future.



Our children have strong core skills in communication (reading, writing, speaking and computing), mathematics and have a good understanding of topics across the whole curriculum.



Our children are confident to share their views, listen to other people's ideas and opinions and make decisions that help everyone achieve.

And links to the following articles from the United Nations Convention on the rights of the child.



Article 18 Children have a right to be protected;

Article 28 Children have a right to a good quality education;



2 Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation \(GDPR\)](#) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the [Data Protection Bill](#).

This policy applies to all personal data, regardless of whether it is in paper or electronic format and combines the previously separate policies for Confidentiality and Freedom of Information.

3 Legislation and guidance

This policy meets the requirements of the following legislation:

Data Protection Act 1998

Data Protection Act 2018 (GDPR provisions)

Human Rights Act 1998

Freedom of Information Act 2000

It is based on guidance published by the Information Commissioner's Office (ICO) on the [GDPR](#) and the ICO's [code of practice for subject access requests](#). It also reflects the ICO's [code of practice](#) for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the [Education \(Pupil Information\) \(England\) Regulations 2005](#), which gives parents the right of access to their child's educational record.

4 Definitions

Term	Definition
Personal data	<ul style="list-style-type: none"> • Any information relating to an identified, or identifiable, individual. • This may include the individual's: <ul style="list-style-type: none"> ○ 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	<ul style="list-style-type: none"> • Personal data which is more sensitive and so needs more protection, including information about an individual's: <ul style="list-style-type: none"> ○ 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none">• The identified or identifiable individual whose personal data is held or processed.
Data controller	<ul style="list-style-type: none">• A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

5 The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

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

6 Roles and responsibilities

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

6.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

6.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our DPO role is fulfilled by Judicium Education Services. Day-to-day management of and enquiries regarding data protection are the responsibility of our Assistant Head. Our Assistant Head is contactable via the school office.

6.3 Head of School

The Head of School acts as the representative of the data controller on a day-to-day basis.



6.4 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 DPO in the following circumstances:
 - With any questions about the operation of this policy, 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 European Economic Area
 - 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

7 Data protection principles

The GDPR is based on data protection principles that our school 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.

8 Collecting personal data

8.1 Lawfulness, fairness and transparency

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

1. 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
2. The data needs to be processed so that the school can comply with a legal obligation
3. The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
4. 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
5. 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)
6. 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 which are set out in the GDPR and Data Protection Act 2018.



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).

8.2 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.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the [Information and Records Management Society's toolkit for schools](#).

9. 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 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:

- Where the disclosure is required to satisfy our safeguarding obligations
- 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
- 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 to a country or territory outside the European Economic Area, we will do so in accordance with data protection law



10. Subject access requests and other rights of individuals

10.1 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
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO (contact details available from the school office).

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 DPO.

10.2 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.

10.3 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 at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

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

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

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

10.4 Other data protection rights of the individual

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

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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



11. Freedom of Information

The Freedom of Information Act 2000 (Fol) gives members of the public the right to access official information held by Public Authorities.

Overall responsibility for ensuring that the school meets the statutory requirements of the Fol act lies with the Governors and the Chair of Governors has overall responsibility for information management issues. They have delegated the day-to-day responsibility of implementation to the Executive Headteacher.

The Executive Headteacher is assisted by the Head of School and Admin officers who currently fulfils the role of 'Fol officer'. All School staff are responsible for ensuring that they handle requests for information in compliance with the provisions of the various acts including Data Protection, taking advice from the Fol officer where necessary.

As well as responding to requests for information made under the Fol Act 2000, the school is required to publish information proactively. The Fol Act requires every school to have a publication scheme, and to publish information covered by the scheme. The scheme sets out our commitment to make certain classes of information routinely available, such as policies and procedures, minutes of meetings, annual reports and financial information.

Morden Mount Primary School has adopted the Information Commissioner's Model Publication Scheme in its entirety and have produced a guide to information which sets out the information we hold, where it can be obtained and whether a fee is payable.

11.1 Publication Scheme

The Model Publication Scheme commits Morden Mount Primary School to make information available to the public as part of its normal business activities. The information covered is included in the classes of information mentioned below, where this information is held by the School.

The scheme commits the school to:

- Proactively publish or otherwise make available as a matter of routine, information, including environmental information, which is held by the authority and falls within the classifications below.
- Specify the information which is held by the School and falls within the classifications below.
- Proactively publish or otherwise make available as a matter of routine, information in line with the statements contained within this scheme.
- Produce and publish the methods by which the specific information is made routinely available so that it can be easily identified and accessed by members of the public.
- Review and update on a regular basis the information the authority makes available under this scheme.
- produce a schedule of any fees charged for access to information which is made proactively available.
- make this publication scheme available to the public.

11.2 Categories of information published

The publication scheme guides you to information which we currently publish (or have recently published) or which we will publish in the future. This is split into categories of information known as classes.

The classes of information that we undertake to make available are organised into the following main topic areas:

Who we are and what we do.

Organisational information, locations and contacts, constitutional and legal governance.

What we spend and how we spend it.

Financial information relating to projected and actual income and expenditure, tendering, procurement and contracts.

What our priorities are and how we are doing.



Strategy and performance information, plans, assessments, inspections and reviews.

How we make decisions.

Policy proposals and decisions. Decision making processes, internal criteria and procedures, consultations.

Our policies and procedures.

Current written protocols for delivering our functions and responsibilities.

Lists and Registers.

Information held in registers required by law and other lists and registers relating to the functions of the authority.

The services we offer.

Advice and guidance, booklets and leaflets, transactions and media releases. A description of the services offered.

The classes of information will not generally include:

- Information the disclosure of which is prevented by law, or exempt under the Freedom of Information Act, or is otherwise properly considered to be protected from disclosure.
- Information in draft form.
- Information that is no longer readily available as it is contained in files that have been placed in archive storage, or is difficult to access for similar reasons

11.3 How to request information

If you require a paper version of any of the documents within the scheme, please contact the school by telephone, email or letter. Contact details are set out below.

Email: info@mordenmount.greenwich.sch.uk Tel: **020 8692 2920**

Contact address: **Admin Office**

Morden Mount Primary School

Lewisham Road

London SE13 7QP

To help us process your request quickly, please clearly mark and correspondence “**PUBLICATION SCHEME REQUEST**” (in CAPITALS please). If the information you are looking for isn’t available via the scheme you can still contact the school to ask if we have it.

11.4 Paying for information

Information published on our website is free. Single paper copies of information covered by this publication are provided free unless stated otherwise in section 6. If your request means that we have to do a lot of photocopying or printing, or pay a large postage charge, or if your request is for a priced item (such as some printing publication or videos) we will let you know the cost before fulfilling your request. Where there is a charge this will be indicated by a £ sign in the description box in the next section.



11.5 Classes of information currently published

Information to be published	How the information can be obtained
Class 1 - Who we are and what we do (Organisational information, structures, locations and contacts) This will be current information only	
Who's who in the school	Website
Who's who on the governing body and the basis of their appointment	
Contact details for the Head teacher and for the governing body	
Staffing structure	
School session times and term dates	
Instrument of Government	By request

Class 2 – What we spend and how we spend it (Financial information relating to projected and actual income and expenditure, procurement, contracts and financial audit)	
Annual budget plan and financial statements	Hard copy on request
Capital funding	
Additional funding	
Procurement and projects	
Pay policy	
Staffing and grading structure	
Governors' allowances	

Class 3 – What our priorities are and how we are doing Strategies and plans, performance indicators, audits, inspections and reviews Current information as a minimum	
Government supplied performance data Ofsted report	Website
Performance management policy and procedures adopted by the governing body	Hard copy on request

Class 4 – How we make decisions (Decision making processes and records of decisions)	
Admissions policy/decisions (not individual admission decisions)	Website
Agendas of meetings of the governing body	Hard copy on request
Minutes of meetings of the governing body	Hard copy on request



Class 5 – Our policies and procedures (Current written protocols, policies & procedures for delivering services and responsibilities)	
School policies including: <ul style="list-style-type: none"> • Charging and remissions • Health & safety • Complaints procedure • Staff conduct policy • Discipline and grievances • Staffing structure implementation plan • Information request handling policy • Equality and diversity (including equal opportunities) policies • Staff recruitment policies 	Website Website Website Hard copy on request Hard copy on request Hard copy on request Hard copy on request Website Hard copy on request
Pupil and curriculum policies including: <ul style="list-style-type: none"> • Home-school agreement • Curriculum • Sex education (in relationship policy) • Special educational needs • Accessibility • Equality • Pupil discipline 	Website
Records management and personal data policies including: <ul style="list-style-type: none"> • Information security policies • Records retention destruction and archive policies • Data protection (including information sharing policies) 	Meet with Headteacher to discuss request
Charging regimes and policies <ul style="list-style-type: none"> • Charging policy • Lettings policy 	Website

Class 6 – Lists and registers, currently maintained lists and registers only	
Curriculum circulars and statutory instruments	Meet with Headteacher to discuss request
Disclosure logs	
Asset register	
Any information the school is currently legally required to hold in publicly available registers (this does not include the attendance register)	

Class 7 – The services we offer (Information about the services we offer, including leaflets, guidance and newsletters produced for the public and businesses)	
Extra-curricular activities	Via letters
Out of school clubs	
School publications	

Schedule of Charges	
This describes how the charges have been arrived at	
Photocopying/printing @ 5p per copy (mono)	Actual cost
Photocopying/printing @ 10p per copy (colour)	Actual cost
Postage	Actual cost of Royal Mail standard 2 nd class
Statutory fee	In accordance with any relevant legislation



12 Parental requests to see the educational record

An individual parental responsibility has a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

13 CCTV

We do not use CCTV at Morden Mount Primary School.

14 Photographs and videos

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

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

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

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

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

15 Data protection by design and default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing 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 DPO 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 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
- 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, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

16 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.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our acceptable use agreement)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

17 Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.



18 Personal data breaches

The school 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 set out in appendix A.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

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

19 Training

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

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

20 Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing board.



Appendix A from our Data Protection Policy: Personal data breach procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO by email/ from September 2018 it is anticipated that this will be managed by GDPRiS software.
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
- The DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
 - Loss of control over their data
 - Discrimination
 - Identify theft or fraud
 - Financial loss
 - Unauthorised reversal of pseudonymisation (for example, key-coding)
 - Damage to reputation
 - Loss of confidentiality
 - Any other significant economic or social disadvantage to the individual(s) concerned
- If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored by the School Admin Officer. From September 2018, it is anticipated that this will be managed by GDPRiS software.
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page of the ICO website](#) within 72 hours. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. 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



- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored by the School Admin Officer. From September 2018, it is anticipated that this will be managed by GDPRiS software.
- 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

Actions to minimise the impact of data breaches

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

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is 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 for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Sensitive information for named children being published on the school website

- Only a limited number of authorised staff will have access to upload information onto the school website which is password protected.
- If special category data (sensitive information) is accidentally published on the school website, it will be removed with immediate effect as soon as the breach is discovered and the DPO notified.



- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Non-anonymised pupil exam results or staff pay information being shared with governors

- All documents, paper or electronic will summarise information in such a way that it is not possible to identify individuals.
- If special category data (sensitive information) is accidentally made available via email to governors, the sender must attempt to recall the email as soon as they become aware of the error
- Governors 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 for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the governors who received the email, explain that the information was sent in error, and request that they delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all governors who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

A school laptop/ipad containing non-encrypted sensitive personal data being stolen or hacked

- All devices that contain sensitive information will be password protected
- The school asset register will provide an up to date record of where all devices are located.
- Staff will be responsible for ensuring that all devices are locked away securely when not in use
- Staff taking devices home for work purposes will be required to sign out the item and sign it in on its return.
- In the event of a laptop/ipad being stolen or hacked, the member of staff discovering the breach must notify the DPO immediately.
- The DPO will enlist the support of the IT team to identify the location of the device when it was last in use in an attempt to recover it.

The school's cashless payment provider being hacked and parents' financial details stolen

- The school will only use third parties who provide assurances that their systems are compliant with GDPR regulations.
- Upon receiving notification of the breach from the cashless payment provider, The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The DPO will notify all parents whose details are held on the payment provider's website.



Appendix B from our Data Protection Policy: Privacy notice for parents/carers

(Full policy is available on our school website)

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **pupils**.

We, Morden Mount Primary School are the 'data controller' for the purposes of data protection law.

The contact details for our data protection officer is held by the school office (see 'Contact us' below).

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why we use this data

We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Assess the quality of our services
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **school admin officer** by emailing info@mordenmount.greenwich.sch.uk or phoning 020 8692 2920



Our legal basis for using this data

There are six available lawful bases for collecting and processing data. These are:

1. 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
2. The data needs to be processed so that the school can comply with a legal obligation
3. The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
4. 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
5. 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)
6. The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information

While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data

We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. Our record retention schedule (see Appendix D) sets out how long we keep information about pupils.



Data sharing

We do not share information about pupils with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about pupils with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- The Department for Education – to meet our legal obligations to share certain information with it in order to inform the school's delegated budget share.
- The pupil's family and representatives – where there is a legal right to information.
- Educators and examining bodies.
- Our regulator - Ofsted.
- Schools in our Partnership, as stated in our Partnership Agreement which has been ratified by the Governing Board;
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Central and local government – to comply with the duty placed upon the school
- Our auditors – to comply with legal requirements
- Health authorities – to support the well-being of pupils
- Health and social welfare organisations – to support the safeguarding of pupils.
- Professional advisers and consultants – to support the well-being and education of pupils.
- Charities and voluntary organisations – with consent, to support families
- Police forces, courts, tribunals – to comply with legal requirements.

National Pupil Database

We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census and early years census.

Some of this information is then stored in the [National Pupil Database](#) (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.

For more information, see the Department's webpage on [how it collects and shares research data](#).

You can also [contact the Department for Education](#) with any further questions about the NPD.

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Parents and pupils' rights regarding personal data

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

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.



Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request please contact School Admin Officer (details below) who will acknowledge receipt and pass the complaint to the Data Protection Officer (Judicium Education Services).

Parents/carers also have a legal right to access to their child's **educational record**. To request access, please contact the School Admin Officer (details below).

Other rights

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer/machine, rather than by a person)
- In certain circumstances, have inaccurate data corrected, deleted/destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact the School Admin Officer (details below) who will acknowledge receipt and pass the complaint to the Data Protection Officer (Judicium Education Services).

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact School Admin Officer at Morden Mount Primary School.

- Via email on info@mordenmount.greenwich.sch.uk
- Call 020 8692 2920
- Or write to: School Admin Officer, Morden Mount Primary School, Lewisham Road, London SE13 7QP

The School Admin Officer will acknowledge receipt and pass the complaint on to the Data Protection Officer (Judicium Education Services).

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF



Appendix C from our Data Protection Policy: Privacy notice for staff

(Full policy is available on our school website)

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our school.

We, Morden Mount Primary School are the 'data controller' for the purposes of data protection law.

The contact details for our data protection officer is held by the school office (see 'Contact us' below).

The personal data we hold

We process data relating to those we employ, or otherwise engage, to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, NI number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
- Absence data
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Copy of driving licence/passport
- Photographs
- CCTV footage
- Data about your use of the school's information and communications system

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records
- Criminal records as required by law to enable you to be a governor or volunteer

Why we use this data

The purpose of processing this data is to help us run the school, including to:

- Enable staff to be paid
- Facilitate safe recruitment
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **school admin officer** by emailing info@mordenmount.greenwich.sch.uk or phoning 020 8692 2920



Our lawful basis for using this data

There are six available lawful bases for collecting and processing data. These are:

1. 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
2. The data needs to be processed so that the school can comply with a legal obligation
3. The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
4. 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
5. 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)
6. The individual has freely given clear consent

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school's use of your data.

Collecting this information

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.

Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our record retention schedule.



Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and information about headteacher performance and staff dismissals
- The Department for Education
- Your family or representatives – where there is consent
- Educators and examining bodies
- Our regulator Ofsted,
- Schools in our Partnership, as stated in our Partnership Agreement which has been ratified by the Governing Board
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Trade unions and associations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies
- Employment and recruitment agencies

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Your rights

How to access personal information we hold about you

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

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request please contact School Admin Officer (details below) who will acknowledge receipt and pass the complaint to the Data Protection Officer (Judicium Education Services).



Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact the School Admin Officer (details below) who will acknowledge receipt and pass the complaint on to the Data Protection Officer (Judicium Education Services).

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact School Admin Officer at Morden Mount Primary School.

- Via email on info@mordenmount.greenwich.sch.uk
- Call 020 8692 2920
- Or write to: School Admin Officer, Morden Mount Primary School, Lewisham Road, London SE13 7QP

The School Admin Officer will acknowledge receipt and pass the complaint on to the Data Protection Officer (Judicium Education Services).

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF



Appendix D from our Data Protection Policy: Privacy notice for governors and volunteers

(Full policy is available on our school website)

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our school.

Morden Mount Primary School is the 'data controller' for the purposes of data protection law

We are required under data protection legislation to notify you of the information contained in this privacy notice. This notice does not form part of any contract of employment or other contract to provide services and we may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Contact details for our data protection officer is held by the School Office (see 'Contact us' below).

The personal data we hold

We process data relating to those we employ, or otherwise engage, to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Recruitment information, references and other information included in a CV or cover letter or as part of the application process
- Information about attendance in school or at governor meetings.
- Information about relevant qualifications, experience or training.
- Photographs
- CCTV footage
- Data about your use of the school's information and communications system

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Criminal records as required by law to enable you to be a governor or volunteer

Why we use this data

The purpose of processing this data is to help us run the school, including to:

- Facilitate safe recruitment
- Inform our recruitment and retention policies
- Enable ethnicity and disability monitoring

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **school admin officer** by emailing info@mordenmount.greenwich.sch.uk or phoning 020 8692 2920

Our lawful basis for using this data

There are six available lawful bases for collecting and processing data. These are:

1. 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
2. The data needs to be processed so that the school can comply with a legal obligation
3. The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
4. 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
5. 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)
6. The individual has freely given clear consent

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Comply with a legal obligation
- For governors: to record information about committee membership and responsibilities.
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school's use of your data.

Collecting this information

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.



Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our record retention schedule.

Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and information about headteacher performance and staff dismissals
- The Department for Education
- Your family or representatives – where there is consent
- Educators and examining bodies
- Our regulator Ofsted,
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Trade unions and associations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies
- Employment and recruitment agencies

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Your rights

How to access personal information we hold about you

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

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request please contact School Admin Officer (details below) who will acknowledge receipt and pass the complaint to the Data Protection Officer (Judicium Education Services).

Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact the School Admin Officer (details below) who will acknowledge receipt and pass the complaint on to the Data Protection Officer (Judicium Education Services).

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact School Admin Officer at Morden Mount Primary School.



- Via email on info@mordenmount.greenwich.sch.uk
- Call 020 8692 2920
- Or write to: School Admin Officer, Morden Mount Primary School, Lewisham Road, London SE13 7QP

The School Admin Officer will acknowledge receipt and pass the complaint on to the Data Protection Officer (Judicium Education Services).

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF



Appendix E from our Data Protection Policy: Record Retention Schedule

(Full policy is available on our school website)

Employment Records

FILE DESCRIPTION	RETENTION PERIOD
Job applications and interview records of unsuccessful candidates	Six months after notifying unsuccessful candidates, unless the school has applicants' consent to keep their CVs for future reference. In this case, application forms will give applicants the opportunity to object to their details being retained
Job applications and interview records of successful candidates	6 years after employment ceases
Written particulars of employment, contracts of employment and changes to terms and conditions	6 years after employment ceases
Right to work documentation including identification documents	6 years after employment ceases
Immigration checks	Two years after the termination of employment
DBS checks and disclosures of criminal records forms	As soon as practicable after the check has been completed and the outcome recorded (i.e. whether it is satisfactory or not) unless in exceptional circumstances (for example to allow for consideration and resolution of any disputes or complaints) in which case, for no longer than 6 months.
Change of personal details notifications	No longer than 6 months after receiving this notification
Emergency contact details	Destroyed on termination
Personnel records	While employment continues and up to six years after employment ceases
Annual leave records	Six years after the end of tax year they relate to or possibly longer if leave can be carried over from year to year
Consents for the processing of personal and sensitive data	For as long as the data is being processed and up to 6 years afterwards
Working Time Regulations: Opt out forms Records of compliance with WTR	Two years from the date on which they were entered into Two years after the relevant period
Disciplinary records	6 years after employment ceases
Training	6 years after employment ceases or length of time required by the professional body



FILE DESCRIPTION	RETENTION PERIOD
Staff training where it relates to safeguarding or other child related training	Date of the training plus 40 years
Annual appraisal/assessment records	Current year plus 6 years
Professional Development Plans	6 years from the life of the plan
Allegations of a child protection nature against a member of staff including where the allegation is founded	10 years from the date of the allegation or the person's normal retirement age (whichever is longer). This should be kept under review. Malicious allegations should be removed.

Financial and Payroll Records

FILE DESCRIPTION	RETENTION PERIOD
Pension records	12 years
Retirement benefits schemes – notifiable events (for example, relating to incapacity)	6 years from the end of the scheme year in which the event took place
Payroll and wage records	6 years after end of tax year they relate to
Maternity/Adoption/Paternity Leave records	3 years after end of tax year they relate to
Statutory Sick Pay	3 years after the end of the tax year they relate to
Current bank details	Until updated plus 3 years
Bonus Sheets	Current year plus 3 years
Timesheets/clock cards/flexitime	Current year plus 3 years
Pupil Premium Fund records	Date pupil leaves the provision plus 6 years
National Insurance (schedule of payments)	Current year plus 6 years
Insurance	Current year plus 6 years
Overtime	Current year plus 3 years
Annual accounts	Current year plus 6 years
Loans and grants managed by the School	Date of last payment on the loan plus 12 years
All records relating to the creation and management of budgets	Life of the budget plus 3 years



FILE DESCRIPTION	RETENTION PERIOD
Invoices, receipts, order books and requisitions, delivery notices	Current financial year plus 6 years
Student Grant applications	Current year plus 3 years
Pupil Premium Fund records	Date pupil leaves the school plus 6 years
School fund documentation (including but not limited to invoices, cheque books, receipts, bank statements etc).	Current year plus 6 years
Free school meals registers (where the register is used as a basis for funding)	Current year plus 6 years
School meal registers and summary sheets	Current year plus 3 years

Agreements and Administration Paperwork

FILE DESCRIPTION	RETENTION PERIOD
Collective workforce agreements and past agreements that could affect present employees	Permanently
Trade union agreements	10 years after ceasing to be effective
School Development Plans	3 years from the life of the plan
Visitors Book and Signing In Sheets	6 years
Newsletters and circulars to staff, parents and pupils	1 year (and the School may decide to archive one copy)
Minutes of Senior Management Team meetings	Date of the meeting plus 3 or as required
Reports created by the Head Teacher or the Senior Management Team.	Date of the report plus a minimum of 3 years or as required
Records relating to the creation and publication of the school prospectus	Current academic year plus 3 years



Health and Safety Records

FILE DESCRIPTION	RETENTION PERIOD
Health and Safety consultations	Permanently
Health and Safety Risk Assessments	Life of the risk assessment plus 3 years
Health and safety Policy Statements	Life of policy plus 3 years
Any records relating to any reportable death, injury, disease or dangerous occurrence	Date of incident plus 3 years provided that all records relating to the incident are held on personnel file
Accident reporting records relating to individuals who are under 18 years of age at the time of the incident	Accident book should be retained 3 years after last entry in the book
Accident reporting records relating to individuals who are over 18 years of age at the time of the incident	Accident book should be retained 3 years after last entry in the book
Fire precaution log books	Current year plus 3 years
Medical records and details of: - <ul style="list-style-type: none"> • ·control of lead at work • ·employees exposed to asbestos dust • ·records specified by the Control of Substances Hazardous to Health Regulations (COSHH) 	40 years from the date of the last entry made in the record
Records of tests and examinations of control systems and protection equipment under COSHH	5 years from the date on which the record was made

Temporary and Casual Workers

FILE DESCRIPTION	RETENTION PERIOD
Records relating to hours worked and payments made to workers	3 years

Governing Body Documents

FILE DESCRIPTION	RETENTION PERIOD
Instruments of government	For the life of the School
Meetings schedule	Current year
Minutes – principal set (signed)	Generally kept for the life of the organisation



FILE DESCRIPTION	RETENTION PERIOD
Agendas – principal copy	Where possible the agenda should be stored with the principal set of the minutes
Agendas – additional copies	Date of meeting
Policy documents created and administered by the governing body	Until replaced. ** The School should consider keeping all policies relating to safeguarding, child protection or other pupil related issues such as exclusion until the IICSA has issued its recommendations
Register of attendance at full governing board meetings	Date of last meeting in the book plus 6 years
Annual reports required by the Department of Education	Date of report plus 10 years
Records relating to complaints made to and investigated by the governing body or head teacher	Major complaints: current year plus 6 years. If negligence involved: current year plus 15 years. If child protection or safeguarding issues are involved then: current year plus 40 years.
Correspondence sent and received by the governing body or head teacher	General correspondence should be retained for current year plus 3 years.
Records relating to the terms of office of serving governors, including evidence of appointment	Date appointment ceases plus 6 years
Register of business interests	Date appointment ceases plus 6 years
Records relating to the training required and received by governors	Date appointment ceases plus 6 years
Records relating to the appointment of a clerk to the governing body	Date on which clerk appointment ceases plus 6 years
Governor personnel files	Date of appointment plus 6 years

Pupil Records

FILE DESCRIPTION	RETENTION PERIOD
Details of whether admission is successful/unsuccessful	1 year from the date of admission/non-admission
Proof of address supplied by parents as part of the admissions process	Current year plus 1 year
Admissions register	Entries to be preserved for three years from date of entry
Pupil Record	Primary – Whilst the child attends the School



FILE DESCRIPTION	RETENTION PERIOD
Attendance Registers	3 years from the date of entry
Correspondence relating to any absence (authorised or unauthorised)	Current academic year plus 2 years
Special Educational Needs files, reviews and Education, Health and Care Plan, including advice and information provided to parents regarding educational needs and accessibility strategy	Date of birth of the pupil plus 31 years (Education, Health and Care Plan is valid until the individual reaches the age of 25 years – the retention period adds an additional 6 years from the end of the plan).
Child protection information (to be held in a separate file).	DOB of the child plus 25 years then review Note: These records will be subject to any instruction given by IICSA
Exam results (pupil copy)	1-3 years from the date the results are released
Examination results (school's copy)	Current year plus 6 years
Allegations of sexual abuse	For the time period of an inquiry by the Independent Inquiry into Child Sexual Abuse.
Records relating to any allegation of a child protection nature against a member of staff	Until the accused normal retirement age or 10 years from the date of the allegation (whichever is the longer)
Consents relating to school activities as part of GDPR compliance (for example, consent to be sent circulars or mailings)	Consent will last whilst the pupil attends the school.
Pupil's work	Where possible, returned to pupil at the end of the academic year (provided the School have their own internal policy to this effect). Otherwise, the work should be retained for the current year plus 1 year.
Mark books	Current year plus 1 year.
Schemes of work	Current year plus 1 year
Timetable	Current year plus 1 year
Class record books	Current year plus 1 year
Record of homework set	Current year plus 1 year
Photographs of pupils	For the time the child is at the School and for a short while after. Please note select images may also be kept for longer (for example to illustrate history of the school).
Parental consent forms for school trips where there has been no major incident	End of the trip or end of the academic year (subject to a risk assessment carried out by the School)



FILE DESCRIPTION	RETENTION PERIOD
Parental permission slips for school trips where there has been a major incident	Date of birth of the pupil involved in the incident plus 25 years. Permission slips for all the pupils on the trip should be retained to demonstrate the rules had been followed for all pupils

Other Records

FILE DESCRIPTION	RETENTION PERIOD
Emails 2- 3 years is our recommended timeframe	Emails: E-mail that needs to be kept should be identified by content; for example, does it form part of a pupil record? Is it part of a contract? The retention for keeping these emails will then correspond with the classes of records according to content in the retention schedule. These emails may need to be saved into any appropriate electronic filing system or printed out and placed on a paper file.
CCTV	One calendar month
Privacy notices	Until replaced plus 6 years.
Inventories of furniture and equipment	Current year plus 6 years
All records relating to the maintenance of the School carried out by contractors or employees of the school	Whilst the building belongs to the school.
Records relating to the letting of school premises	Current financial year plus 6 years
Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	Current year plus 6 years then review
Referral forms	While the referral is current
Contact data sheets	Current year then review, if contact is no longer active then destroy