Osmani Primary School
Vallance Road
London
E1 5AD

Tel: 020 7247 8909
Fax: 020 7247 9906
Email: admin@osmani.towerhamlets.sch.uk

www.osmaniprimaryschool.org.uk

Osmani Primary School

Reach For The Stars

# Data Protection Policy and Privacy Notices

## Our Motto

Reach For The Stars

## Our Vision Statement

Our vision is to develop an inclusive school, which promotes and achieves excellence, and continues to nurture the values, confidence and skills of pupils, staff and the community, in order to meet the emerging opportunities of the 21st century.
Our vision and values support **Articles 2, 12, 15, 19, 24, 27, 28, 29, 31** of the UN Convention on the Rights of a Child.

## Our Rights

- ★ **Article 19:** We have the right to be safe.
- ★ **Article 28:** We have the right to quality education.
- ★ **Article 12:** We have the right to give our opinion and listen to others.
- ★ **Article 15/31:** We have the right to join in and be part of a team.
- ★ **Article 29:** We have the right to develop our personalities, talents and abilities.

## Our Values

★ **S**triving **T**eamwork **A**ll Included **R**esponsibility **S**uccess ★

★ **Striving:** Our aim is that we are a school that:
- **uses our Growth Mind-set (learning from mistakes and always willing to have a go)**
- **never gives up and always find ways of improving**
- **enjoys challenges and aims high**

★ **Teamwork:** Our aim is that we are a school that:
- **encourages and supports each other to be the best we can be**
- **learns from each other**
- **listens to and respects each other's ideas**

★ **All Included:** Our aim is that we are a school that:
- **has high expectations of everyone**
- **encourages everyone to take an active part in learning and life of our school**
- **nurtures and celebrates what makes each and every one of us unique**

★ **Responsibility:** Our aim is that we are a school that:
- **takes ownership of the choices we make**
- **takes ownership/charge of our own learning**
- **looks after each other and our school**

★ **Success:** Our aim is that we are a school that:
- **provides an education that encompasses academic, creative, social, emotional, physical and cultural development**
- **celebrates our efforts and achievements**

## Equal Opportunities and the Single Equality Scheme

We believe that all those who work in Osmani - children and adults - have the right to be treated fairly and with respect by everyone connected with the school.
We aim for Osmani to be a safe, supportive place, where all children and adults feel valued as individuals, whatever their ability, age, disability, gender identity, marriage or civil partnership, pregnancy & maternity, race, religion or belief, sex and sexual orientation.
The school aims to foster the social and personal skills of co-operation, sharing and mutual respect.

## UN Rights of the Child and Global Goals

This policy supports the school in addressing Article 28 (Right to Education) and Article 29 (Goals of Education) of the **UN Convention on the Rights of the Child.**
**It also supports the following Global Goals:** Goal 4 (Quality Education), Goal 8 (Work and Economy)

## Contents

## 1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents and carers, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.
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 UK GDPR.
It also reflects the ICO's guidance 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.

## 3. Definitions

<table>
<tr><th>Term</th><th colspan="3">Definition</th></tr>
<tr><td>Personal data</td><td colspan="3">Any information relating to an identified, or identifiable living individual. This may include the individual's:<br>• Name (including initials)<br>• Identification number<br>• Location data<br>• Online identifier, such as a username<br>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</td></tr>
<tr><td rowspan="2">Special categories of personal data</td><td colspan="3">Personal data which is more sensitive and so needs more protection, including information about an individual's:</td></tr>
<tr><td>• Racial or ethnic origin<br>• Political opinions<br>• Religious or philosophical beliefs<br>• Trade union membership</td><td>• Genetics<br>• Biometrics (eg fingerprints, eye patterns), where used for identification</td><td>• Health – physical or mental<br>• Sex life or sexual orientation</td></tr>
<tr><td>Processing</td><td colspan="3">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.</td></tr>
<tr><td>Data subject</td><td colspan="3">The identified or identifiable individual whose personal data is held or processed.</td></tr>
<tr><td>Data controller</td><td colspan="3">A person or organisation that determines the purposes and the means of processing of personal data.</td></tr>
<tr><td>Data processor</td><td colspan="3">A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.</td></tr>
<tr><td>Personal data breach</td><td colspan="3">A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.</td></tr>
</table>

## 4. 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.

## 5. 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.

### 5.1 Governing board

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

### 5.2 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.
Full details of the DPO's responsibilities are set out in their job description.
Our DPO is **Asad Muzammal** and is contactable via DPO@EduAction.org.uk

### 5.3 Headteacher

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

### 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 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 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 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.

## 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 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 or another person i.e. 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 or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

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

  - The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
  - The data 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 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 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.

### 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 when appropriate. In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

## 8. Sharing personal data

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – 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 contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with law enforcement and government bodies where legally required to do so.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 data protection law.

## 9. Subject access requests and other rights of individuals

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

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

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

### 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.

### 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 (or receipt of the additional information needed to confirm identity, where relevant)
- 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 may not disclose information for a variety of reasons, such as if it:

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

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

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

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

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

## 10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

## 11. 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 prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to **Thofur Ali, Home School Liaison Officer**

## 12. Photographs and videos

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

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

Where the school takes photographs and videos, 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. See our **Online Safety, School Website and Digital Imaging Policies** for more information on our use of photographs and videos.

## 13. 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 data protection 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/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
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws will 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

## 14. 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 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 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media
- 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 **Online Safety Policy and 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)

## 15. 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.
**See the Records Disposal Policy for more information.**

## 16. 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 1.
When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it.
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 pupils

## 17. 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.

## 18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.
This policy will be reviewed every 2 years and shared with the full governing board.

## 19. Links with other policies and documents

This data protection policy is linked to our:

- Freedom of Information Publication Scheme
- Staff ICT Security Policy and Staff Internet Agreement
- Pupil Online Safety Policy
- School Website Policy
- Digital Media Policy
- Records Disposal Policy
- Pupil Privacy Notice
- Workforce Privacy Notice

## Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the DPO by contacting a member of the SLT and following their instructions
- 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
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, 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 and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types 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 before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- 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 in a protected folder in the school's computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and 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 of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach

    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - 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 in a protected folder in the school's computer system.
- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible
- The DPO and headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

## Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, 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
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners

# Appendix 2: Privacy Notice for Parents and Pupils

## 1. Introduction

Under UK data protection law, individuals have a right to be informed about how our 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 at our school.

We, Osmani Primary School, are the 'data controller' for the purposes of UK data protection law.

Our data protection officer is **Asad Muzammal** and is contactable via **DPO@EduAction.org.uk**

## 2. The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about your child 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
- Exclusion information
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support provider

We may also collect, use, store and share (when appropriate) information about your child that falls into "special categories" of more sensitive personal data. This includes, but is not restricted to, information about:

- Any medical conditions we need to be aware of, including physical and mental health
- Photographs and CCTV images captured in school
- Characteristics, such as ethnic background or special educational needs

We may also hold data about your child that we have received from other organisations, including other schools, local authorities and social services and the DfE.

## 3. Why we use this data

We use the data listed above to:

a) support pupil learning
b) monitor and report on pupil attainment progress
c) provide appropriate pastoral care
d) assess the quality of our services
e) keep children safe (food allergies, medical conditions or emergency contact details)
f) to meet statutory duties placed upon us, e.g. by the Department for Education
g) to communicate with parents via newsletters
h) to share school activities via school social media and the school website

## 4. Our lawful basis for using this data

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing parent and pupil information are:

- for the purposes of (a), (b), (c) & (d) above; in accordance with the legal basis of **public task.** Collecting this data is necessary for tasks that the school are required to perform as part of their statutory function
- for the purposes of (e) above; in accordance with the legal basis of **vital interests**. Processing this data is necessary in order to protect someone's life

- for the purposes of (f) above; in accordance with the legal basis of **legal obligation**. Data collected for the DfE census information is covered by:
    - section 537A of the Education Act 1996
    - the Education Act 1996 s29(3)
    - the Education (School Performance Information) (England) Regulations 2007
    - regulations 5 and 8 School Information (England) Regulations 2008
    - the Education (Pupil Registration) (England) (Amendment) Regulations 2013
- For the purposes (g) and (h) above; Where we have obtained the parent's or pupil's consent to use the data in a certain manner. Where we have obtained consent to use 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.

Occasionally, where the processing is not part of our performing tasks as a public authority, we may process data under the lawful basis that it is in our **legitimate interests** or the legitimate interests of a third party to do so. In these circumstances we would be using the data in a way that would be reasonably expected by the parent or pupil concerned and the processing will have a minimal privacy impact or there will be a compelling justification for the processing.

Some of the reasons listed above for collecting and using parents' or pupils' personal data may overlap and it may be that more than one lawful basis applies to our processing of the data.
No decisions are made by the school through automated decision making (including profiling).

## 5. Our basis for using special category data

For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in UK data protection law:

- We have obtained your explicit consent to use your child's personal data in a certain way
- We need to perform or exercise an obligation or right in relation to employment, social security or social protection law
- We need to protect an individual's vital interests (i.e. protect your child's life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for the establishment, exercise or defence of legal claims
- We need to process it for reasons of substantial public interest as defined in legislation
- We need to process it 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
- We need to process it 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
- We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in UK data protection law. Conditions include:

- We have obtained your consent to use it in a specific way
- We need to protect an individual's vital interests (i.e. protect your child's life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- We need to process it for reasons of substantial public interest as defined in legislation

## 6. Collecting this data

We collect the majority of parent and pupil information via enrolment and admissions forms, Common Transfer Files (CTF) or other secure file transfers from a pupil's previous school.

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

Most of the data we hold about your child will come from you, but we may also hold data about your child from:

- Other schools
- Local authorities, social services and health authorities
- Government departments or agencies
- Police forces, courts, tribunals

## 7. How we store this data

We keep personal information about your child while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary. **Our Records Disposal Policy** sets out how long we keep information about pupils. You can request a copy of this policy by contacting the school office.

We have put in place appropriate security measures to prevent your child's personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. You can find out more about this in our **Data Protection Policy**

We will dispose of your child's personal data securely when we no longer need it.

## 8. Who we share data with

We do not share information about your child 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 UK data protection law), we may share personal information about your child with:

- The pupil's previous and future schools
- The Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.
- Our local authority (Tower Hamlets) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.
- Government departments or agencies such as our regulator OFSTED
- Suppliers and service providers to enable them to provide the services contracted. These include:
    - ICT technical support services
    - Online education resource providers and platforms
    - Catering services
    - Residential trip and activity centres
    - Sports coaches and providers
- Our auditors
- Health professionals
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Police forces, courts, tribunals

### 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 for Education 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 third parties, such as other organisations which promote children's education or wellbeing in England. These third parties must agree to strict terms and conditions about how they will use the data.

For more information, see the Department for Education'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 your child's personal data to a third-party country or territory, we will do so in accordance with UK data protection law.

In cases where we have to set up safeguarding arrangements to complete this transfer, you can get a copy of these arrangements by contacting us.

## 9. Your rights

### How to access personal information that we hold about your child

You have a right to make a 'subject access request' to gain access to personal information that we hold about your child.

If you make a subject access request, and if we do hold information about your child, we will (subject to any exemptions that apply):

- 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 child's personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact us (see 'Contact us' below).

## 10. Your right to access your child's educational record

Parents, or those with parental responsibility, also have the right to access their child's educational record (which includes most information about a pupil). This right applies as long as the pupil is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

To make a request, please contact **Thofur Ali, Home School Liaison Officer** at parents@osmani.towerhamlets.sch.uk

## 11. Your other rights regarding your child's data

Under UK data protection law, you have certain rights regarding how your child's personal data is used and kept safe. For example, you have the right to:

- Object to our use of your child's personal data
- Prevent your child's data being used to send direct marketing
- Object to and challenge the use of your child's 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
- In certain circumstances, have the personal data we hold about your child deleted or destroyed, or restrict its processing
- Withdraw your consent, where you previously provided it for the collection, processing and transfer of your child's personal data for a specific purpose
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact us (see 'Contact us' below).

## 12. 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.

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

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

## 13. Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**.

Our data protection officer is:

**Asad Muzammal** and is contactable via **DPO@EduAction.org.uk**

However, our **data protection lead** has day-to-day responsibility for data protection issues in our school.

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact them:

**Remi Atoyebi**-Headteacher at admin@osmani.towerhamlets.sch.uk

# Appendix 3: Workforce Privacy Notice

## 1. Introduction

Under UK data protection law, individuals have a right to be informed about how our 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, Osmani Primary School are the 'data controller' for the purposes of UK data protection law.
Our data protection officer is **Asad Muzammal** and is contactable via **DPO@EduAction.org.uk**

## 2. The personal data we hold

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

- Contact details
- National Insurance numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Performance and Appraisal outcomes
- Medical information
- Outcomes of any disciplinary procedures

We may also collect, use, store and share (when appropriate) information about you that falls into "special categories" of more sensitive personal data. This includes, but is not restricted to, information about:

- Any health conditions you have that we need to be aware of
- Sickness records
- Photographs and CCTV images captured in school
- Trade union membership

We may also collect, use, store and share (when appropriate) information about criminal convictions and offences.

We may also hold data about you that we have received from other organisations, including other schools and social services, and the Disclosure and Barring Service in respect of criminal offence data.

## 3. Why we use this data

We use the data listed above to:

a) Enable you to be paid
b) Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
c) Support effective performance management
d) Inform our recruitment and retention policies
e) Allow better financial modelling and planning
f) Enable equalities monitoring
g) Improve the management of workforce data across the sector
h) Support the work of the School Teachers' Review Body

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

## 4. Our lawful basis for using this data

These are defined under data protection legislation and for personally identifiably information are:

- To fulfil a contract with you
- You have given **consent** for one or more specific purposes
- Processing is necessary to comply with the school's **legal obligations**
- Processing is necessary to protect your **vital interests**
- Processing is necessary for tasks in the **public interest** or exercise of authority vested in the controller (the provision of education)
- Processing is necessary for the school's **legitimate interests** or the legitimate interests of a third party.

When we process special category information, which is deemed to be more sensitive, the following lawful basis are used:

- You have given explicit consent
- Employment, social security and social protection
- It is necessary to fulfil the school's obligations or your obligations
- It is necessary to protect your vital interests
- Processing is carried out by a foundation or not-for-profit organisation (includes religious, political or philosophical organisations and trade unions)
- Reasons of public interest in the area of public health.

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 can withdraw consent if you wish to do so.

## 5. Collecting this data

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

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.

Most of the data we hold about you will come from you, but we may also hold data about you from:

- Local authorities
- Government departments or agencies
- Police forces, courts, tribunals

## 6. How we store this data

We keep personal information about you while you work at our school. We may also keep it beyond your employment at our school if this is necessary. Our **Records Disposal Policy** sets out how long we keep information about staff.
You can request a copy of this policy by contacting the school office.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. You can find out more about this in our **Data Protection Policy**

We will dispose of your personal data securely when we no longer need it.

## 7. Who we share data with

We do not share information about you 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 UK 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
- Government departments or agencies including our regulator, OFSTED.

Suppliers and service providers including:

- ICT technical support services
- Online education resource providers and platforms
- Catering services
- Residential trip and activity centres

- Financial organisations
- Our auditors
- Health authorities
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals

### Transferring data internationally

We may share personal information about you with the relevant international third parties, where different data protection legislation applies:

Where we transfer your personal data to a third-party country or territory, we will do so in accordance with UK data protection law.

In cases where we have to set up safeguarding arrangements to complete this transfer, you can get a copy of these arrangements by contacting us.

## 8. How to access personal information that we hold about you

You have a right to make a 'subject access request' to gain access to personal information that we hold about you. If you make a subject access request, and if we do hold information about you, we will (subject to any exemptions that may apply):

- 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 us (see 'Contact us' below).

### Your other rights regarding your data

Under UK data protection law, you have certain rights regarding how your personal data is used and kept safe. For example, you have the right to:

- Object to our use of your personal data
- Prevent your data being used to send direct marketing
- Object to and challenge 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
- In certain circumstances, have the personal data we hold about you deleted or destroyed, or restrict its processing
- Withdraw your consent, where you previously provided it for the collection, processing and transfer of your personal data for a specific purpose
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact us (see 'Contact us' below).

## 9. 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.

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

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

## 10. Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**.

Our data protection officer is:

**Asad Muzammal** and is contactable via **DPO@EduAction.org.uk**

However, our **data protection lead** has day-to-day responsibility for data protection issues in our school.

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact them:

**Remi Atoyebi**-Headteacher at admin@osmani.towerhamlets.sch.uk