

# MONA PREPARATORY SCHOOL

## DATA PRIVACY/PROTECTION POLICY

Mona Preparatory School (MPS) collects and uses personal data about staff, students, parents and other individuals who come into contact with the school. This personal data is gathered to enable MPS to provide the best education services possible and other associated functions. In addition, there may be a legal requirement to collect and use data to ensure that the school complies with its statutory obligations.

### **Purpose**

The Data Privacy/Protection policy is intended to ensure that personal data is dealt with lawfully, fairly correctly and securely and in accordance with the Data Protection Act 2020 (DPA). Further, this policy applies to all personal data, regardless of the way it is collected, recorded, stored and used before ultimately being destroyed when no longer required.

### **Key Terms**

#### **Data Subject:**

As outlined in the Data Protection Act, a data subject is an individual whose personal data is being collected by an entity being the Data Controller, wherein the personal data is solicited, stored and/or processed. MPS's data subjects are current, past and prospective parents, students, members of staff, suppliers and contractors.

**Stakeholders:** Any individual/entity having vested or common interest in the operation of MPS i.e., students, parents, suppliers, contractors, staff members and board members.

**Data controller:** A data controller is defined under the Act as “any person or public authority, who, either alone or jointly or in common with other persons, determines the purposes for which and the manner in which any personal data are, or are to be processed”. The data controller is responsible for: appointing a data protection officer (DPO), ensuring registration of MPS as a data controller is completed with the Office of the Information Commissioner, working with the school to ensure that privacy impact assessments are done and annual data protection impact assessment (DPIA); whilst ensuring it is done and submitted to the OIC within 90 days after the end of each calendar year.

**Data processor:** A data processor is defined under the Act as “any person, (other than an employee of the data controller), who processes the personal data on behalf of the data controller”.

**Data protection officer:** A data protection officer is defined under the Act as ‘any person responsible for monitoring an organization’s compliance with the provisions of the Data Protection Act; informing the school of its data protection obligations, and assisting data subjects with enforcing their personal data rights’.

**Personal data:** Personal data is defined under the Act as ‘data (however stored) relating to a living individual, or an individual who has been deceased for less than 30 years, who can be identified from that data alone or from that data and other data in the possession of, or likely to come into the possession of, the data controller, and which includes any expression of opinion about that individual and any indication of the intentions of the data controller or any other person in respect of that individual’.

**Sensitive data:** Sensitive personal data is defined under the Act as personal data consisting of any of the following information in respect of a data subject:

- genetic data or biometric data;
- filiation, racial, or ethnic origin;
- political opinions, philosophical beliefs, religious beliefs, or other beliefs of a similar nature;
- membership in any trade union;
- physical or mental health or condition;
- sex life; or
- the alleged commission of any offense by the data subject or any proceedings for any offense alleged to have been committed by the data subject.

**Biometric data:** Biometric data is defined as any data relating to the physical, physiological, or behavioral characteristics of that individual, which allows for the unique identification of the individual, and includes:

- physical characteristics such as the photograph or other facial image, fingerprint, palm print, toe print, footprint, iris scan, retina scan, blood type, height, vein pattern, or eye color, of the individual, or such other biological attribute of the individual as may be prescribed; and
- behavioral characteristics such as a person's gait, signature, keystrokes, or voice.

### **Why the need to collect/keep personal data?**

Personal data is being kept under our control to ensure that we have sufficient contact details for parents, guardians, suppliers, students and staff members so that we are able to effectively and efficiently communicate with these stakeholders when and if the need arises.

In the case of students, concise medical data and photographs for identification purpose are also processed in an effort to render sufficient care to, as well as ensure the safety and security of our students.

Basic demography data is then sent to our website and SmartTerm providers to create accounts for email communications, and access to learning resources that are being shared from the school. There is no further sharing from this point.

This data will be kept for the duration of your tenure/business with the school and for at least an additional seven (7) years as stipulated by law.

### **Data Protection Principles**

The DPA establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the DPA;
7. Personal data shall be kept secure, specifically, protected by an appropriate degree of security;
8. Personal data shall not be transferred to a State or territory outside of Jamaica unless that State or territory ensures an adequate level of protection for the rights and freedoms of the data subjects in relation to the processing of personal data.

### **General Statement**

MPS is committed to maintaining the above principles at all times. Therefore, the school will:

- Inform individuals why the data is being collected and when it is collected
- Inform individuals when their data is shared, why and with whom it was shared
- Check the quality and the accuracy of the data it holds with the pertinent data subject
- Ensure that data is not retained for longer than is necessary
- Ensure that when obsolete data is destroyed, it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal data from loss, theft and unauthorised access or disclosure, irrespective of the format in which it is recorded
- Share data with others only when it is legally and professionally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal data
- Ensure all staff are aware of, and understand data protection policies and procedures

### **Data Collection**

MPS collects personal data electronically through the use of our website, SmartTerm, email and our accounting software. In addition, MPS also collects personal data via soft and hard copies of registration form and various surveys conducted from time to time. The data gained by way of these technologies/channels include but is not limited to names of students and parents, contact details, and addresses.

MPS collects personal data to create profiles from the completed registration forms, correspondence and professional observations and evaluations. This is to support student learning, as well as to monitor and provide progress reports, provide appropriate counseling or pastoral care and assess the quality of our services. Categories of personal data within Student Profiles include:

- Personal Data (name, age, sex, address)
- Medical Data (allergies, medical conditions, name of GP)
- Attendance Data
- Behavioural Data
- Assessment Data
- Academic Records/Data

Although some data is mandatory, in compliance with the DPA, we will inform you whether you are required to provide certain student data to us or if you have a choice in this.

### **Data Storage and Security**

Data gained electronically are stored on servers hosted by our website provider, our Learning Management System (LMS) provider SmartTerm and on computers in our offices. Physical copies of data gained are stored in cabinets that reside in our administrative office to which only the administrative team has access. Data is stored for the duration of the child's tenure at MPS in addition to seven years beyond the students' attendance at MPS.

### **Data Sharing**

The Act imposes a general obligation on data controllers to obtain consent before transferring personal data to third parties. The Act also requires data controllers to ensure that such third parties are subject to similar data protection obligations and that they have certain technical and organisational measures in place to safeguard against a security breach before transferring personal data.

MPS respects the privacy of all students and their families. No personal or sensitive personal data will be shared without explicit consent unless stipulated by law. In the interest of security, MPS provides all class teachers with a student list containing key medical data, pick-up rights and contact numbers as provided on the registration forms. It is the responsibility of the student, or their parents, to ensure this data is correct and up to date.

During activities, staff and invited representatives occasionally take photographs of students and their activities. These photos may be used for publication purposes unless otherwise stipulated.

### **Your Rights**

You are entitled to request access to the personal data held about you by MPS. Requests for data must be made in writing to [iserve@monaprep.edu.jm](mailto:iserve@monaprep.edu.jm) and will be dealt with by MPS within the time period stipulated by the DPA. This request must be made from the email listed on our file.

In compliance with the DPA, the identity of the requestor must be established before the disclosure of any data in the form of a passport, driver's license or other form of recognised legal ID. The data within the Student Profile belongs to the named student, regardless of age. As stipulated by the Act, should parents wish to gain access, the rights granted to a student being the data subject, may be exercised by a parent or legal guardian of the student, or by the student in any case where the law recognises the capacity of the student to act on their own behalf.

In addition, you also have the right to:

- object to the processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for direct marketing
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

## Consent and Privacy Notice

I \_\_\_\_\_ (Parent's/Guardian's full name), the legal parent/guardian of  
\_\_\_\_\_  
\_\_\_\_\_ (Child's full name) consent to giving the above data to Mona  
Preparatory School for the purpose of \_\_\_\_\_ (state purpose).

This data will be stored for the duration of your tenure/business with Mona Preparatory School and an additional seven (7) years as stipulated by law. During this time, you reserve the right of access, rectification, restriction and objection/withdraw at any time in writing to the MPS.

### Mona Preparatory School

*This communication including any attachment transmitted with it, is intended only for the use of the individual or entity to whom it is addressed. If you are not an intended recipient, any review, disclosure, conversion to hard copy, dissemination, reproduction or other use of any part of this communication is strictly prohibited. If you believe you received this communication in error or without authorisation, please notify us immediately by return e-mail or telephone, and permanently delete the entire communication from any computer, hard drive, or other storage medium.*

### Data Breaches

Data breaches create reputational, legal, financial and many other types of risk for organisations. Data security is addressed in the DPA and requires that appropriate procedures are in place to detect, report and investigate data breaches. A data controller is required to report any security breach in respect of the data controller's operations that affects or may affect personal data to the Office of the Information Commissioner within 72 hours of becoming aware of the breach.

The report must include:

- the facts surrounding the security breach;
- a description of the nature of the security breach, including the categories, number of data subjects concerned, and the type and number of personal data concerned;
- the measures taken or proposed to be taken to mitigate or address the possible adverse effects of the breach;
- the consequences of the breach; and
- the name, address, and other relevant contact data of its DPO.

A data controller is also required to report any security breach to each data subject, whose personal data has been affected by such breach within such time as prescribed. The report must include:

- the nature of the security breach;
- the measures taken or proposed to be taken to mitigate or address the possible adverse effects of the breach; and
- the name, address, and other relevant contact data of its DPO.

### Complaints

Complaints will be dealt with in accordance with the school's complaints policy.

### Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every two years. The policy review will be undertaken by the MPS Human Resource Committee or a nominated representative.

### Contacts

If you have any enquiries concerning this policy, please contact MPS at [iserve@monaprep.edu.jm](mailto:iserve@monaprep.edu.jm).

Date notice is adopted:

October 15, 2024

Next review:

October 15, 2025