Marriott Primary

Achieving Together

DATA PROTECTION POLICY

Approved	**15th June 2021**
Signed **(Chair of Governors)**	***Steve Wilson***
Reviewed (Due: 15th June 2024)	
Signed **(Chair of Governors)**	

Contents

Introduction

1.1 Marriott Primary School (MPS) collects, holds and processes data about its pupils, parents, employees, applicants, stakeholders, contractors and other individuals in order to carry out its educational aims and organisational functions.

1.2 Data Protection legislation defines 'personal data' as any information relating to an identified, or an identifiable natural person (the 'data subject').

1.3 MPS is committed to protecting the rights and freedoms of individuals with respect to the processing of their personal data.

Purpose and Scope

2.1 The purpose of this policy is to ensure compliance with the UK General Data Protection Regulation (UK GDPR) and related Data Protection legislation.

2.2 MPS is registered with the Information Commissioner's Office (ICO) as a Data Controller. This policy incorporates guidance from the ICO and outlines how MPS will discharge its duties and obligations to comply with Data Protection legislation.

2.3 This policy applies to all parts of MPS and to all personal data held and processed by the organisation. This includes data held in any system or format, whether electronic or manual.

2.4 This Policy applies to all members of staff except when acting in a private or non-MPS capacity. The term 'staff' means anyone working in any context within MPS. This includes but is not limited to temporary, visiting, casual, voluntary and agency workers, parents when engaged on school duties such as accompanying school trips, those employed by MPS and Governors and members of committees. This Policy also applies to all locations from which personal data is stored and accessed including off-school premises.

2.5 It is the responsibility of all school staff to ensure that personal data is processed in accordance with Data Protection legislation and that pupils, parents, and staff are advised about their responsibilities.

2.6 This policy is not, and should not be confused with, our Privacy Notice (a statement which informs data subjects how their personal data is used by MPS).

2.7 This policy should be read in conjunction with responsibilities and obligations outlined in the following documents, which supplement this policy where applicable:

- Staff employment contracts and comparable documents which impose confidentiality obligations in respect of information held by MPS;
- Any other contractual obligations or staff policies which impose confidentiality or data management obligations in respect of information held by MPS;
- The Data Retention Policy which governs the appropriate retention and disposal of MPS information;
- MPS's Data Breach Policy which sets out the procedure to be followed if a personal data breach takes place;
- IT and information security policies, procedures and terms and conditions which concern the confidentiality, integrity and availability of MPS information including rules about IT acceptable use, user accounts, internet, email, and network and wireless facilities.

Policy Statement

3.1 MPS is committed to complying with Data Protection legislation through its everyday working practices.

3.2 Complying with Data Protection legislation may be summarised as, but is not limited to:

- understanding, and applying as necessary, the data protection principles when processing personal data;
- understanding, and fulfilling when necessary, the rights given to data subjects under Data Protection legislation;
- understanding, and implementing as necessary, MPS's accountability obligations under Data Protection legislation.

3.3 In accordance with Data Protection legislation, additional conditions and safeguards will be applied to ensure that special category data (sensitive personal data) is handled appropriately. Special category personal data is information relating to an individual's:

- race or ethnic origin;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- health;
- sex life or sexual orientation.

3.4 Criminal convictions or offences (alleged or proven) are not technically defined as special category personal data but are afforded similar protections.

Data Protection Principles

4.1 Data Protection legislation requires that MPS, its staff and others who process or use any personal information, comply with the data protection principles.

4.2 The data protection principles state that personal data should be:

i. processed lawfully, fairly and in a transparent manner;
ii. collected for specified, explicit and legitimate purposes;
iii. adequate, relevant and limited to what is necessary;
iv. accurate and where necessary kept up to date;
v. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data is processed;
vi. processed in a manner that ensures appropriate security of the personal data.

4.3 Accountability is central to Data Protection legislation, and as a Data Controller, MPS is responsible for compliance with the principles and must be able to demonstrate this to data subjects and the UK regulator, the ICO.

Data Subject Rights

5.1 The rights given to data subjects under Data Protection legislation are:

- the right to be informed;
- the right of access to the information held about them (though a Subject Access Request);
- the right to rectification;
- the right to erasure;

- the right to restrict processing;
- the right to data portability;
- the right to object;
- rights in relation to automated decision-making and profiling.

5.2 Under Data Protection legislation, data subjects have the right of access to their personal data held by MPS.

5.3 Any individual who wishes to exercise this right should contact the school by phone on 0116 2832433 or by email at admin@marriott.leicester.sch.uk or our Data Protection Officer on 01757 616885 or info@bls-ltd.co.uk

Roles and Responsibilities

6.1 As a Data Controller (or when acting as a joint Data Controller or a Data Processor), MPS has a corporate responsibility for the following:

- complying with Data Protection legislation and holding records to demonstrate this;
- cooperating with the ICO, as the UK regulator of Data Protection legislation;
- responding to regulatory / court action and paying administrative levies and fines issue by the ICO.

6.2 MPS's Governing Body is responsible for reviewing and approving this policy.

6.3 The MPS Co-Head Teachers are responsible for assessing the overall risk profile of MPS and ensuring appropriate resources and processes are in place and implemented to enable compliance with Data Protection legislation.

6.4 MPS 's Data Protection Officer is responsible for:

- monitoring MPS's compliance with Data Protection legislation including managing internal data protection activities, raising awareness, training, and the conduct of internal audits;
- advising MPS on its Data Protection obligations (including the use of Data Protection Impact Assessments);
- acting as MPS 's point of contact for the ICO with regard to Data Protection legislation;
- acting as an available point of contact for data subjects.

6.5 The MPS Business Manager, in collaboration with other relevant leadership teams, is responsible for:

- providing advice, guidance, training and tools / methods to assist MPS and staff in complying with this policy, in liaison with the Data Protection Officer, and taking account of ICO and other regulatory guidance and relevant case law;
- publishing and maintaining core Privacy Notices and other MPS-wide data protection documents;
- managing Subject Access Requests;
- advising on, managing and / or handling Data Protection Impact Assessments, data subject complaints, and personal data breaches, as advised by the Data Protection Officer.

6.6 The senior and middle leadership teams are responsible for:

- ensuring that all staff within their areas are aware of this policy, and understand the role of data protection principles in their day-to-day working practices through induction, training, and performance monitoring;

- ensuring that personal data within their areas is processed in line with this policy and associated policies and procedures;
- supporting internal and external audits to ensure compliance with Data Protection legislation;
- developing and reviewing information surveys to document information assets containing personal data in their areas, including databases, relevant filing systems, and the purposes of processing, to inform MPS 's Information Asset Register.

6.7 Compliance with Data Protection legislation is the personal responsibility of all members of MPS who process personal data.

6.8 New members of staff are required to complete mandatory information governance training as part of their MPS induction.

6.9 Staff members, as appropriate for their role and in order to enable MPS to comply with Data Protection legislation, are responsible for:

- completing the information governance training, and refresher training annually and / or if their role changes significantly;
- ensuring that any personal data they process adheres to this policy and any associated information security policies;
- ensuring any personal data they process complies with the data protection principles;
- following relevant advice, guidance and tools / methods provided in relation to information governance;
- when processing personal data on behalf of MPS, only using it as necessary for their contractual duties and / or other MPS roles and not disclosing it unnecessarily or inappropriately;
- recognising, reporting internally with immediate effect, and cooperating with any remedial work arising from personal data breaches in accordance with the Data Breach Policy;
- recognising, reporting internally with immediate effect, and cooperating with the fulfilment of Subject Access Requests;
- ensuring they do not disclose personal data to a third party without establishing there is a lawful basis for doing so. MPS may have a duty to disclose personal data to authorised bodies, such as the police and other organisations in order to comply with its legal or statutory obligations under Data Protection legislation. Any requests to disclose personal data for non-routine reasons should be directed to the School Business Manager who will respond on behalf of MPS.

6.10 The responsibilities outlined under paragraph 6.9 apply to volunteers and agency staff when processing personal data on behalf of MPS.

6.11 Any breach of this policy may be treated as misconduct under MPS's relevant disciplinary procedures and could lead to disciplinary actions or sanctions.

Policy Review

7.1 This policy will be updated as necessary to reflect best practice, relevant case law, and to ensure compliance with any changes or amendments to Data Protection legislation.