DATA PROTECTION POLICY

Title	**Data Protection Policy**
Owner	**Headteacher and Schools Data Protection Officer**
Version Number	**1**
Review Frequency	**Every 2 years**
Current Review	**Completed May 2018**
Review Due	**April 2019**

INTRODUCTION

This document sets out Mersey Park Primary School policy regarding Data Protection; it is based on the new 2018 Data Protection Act, (The Act) and The General Data Protection Regulation (GDPR) (EU) 2016/679. This policy will be reviewed and revised as the School develops policies under Information Management legislation such as Freedom of Information Act and Human Rights Act 1998, which both enhance the protection and the individual rights given under the Data Protection legislation. The purpose of The Act is to regulate the way that personal information about living individuals is obtained, stored, used and disclosed. The legislation grants rights to individuals:

1. Right to be informed

We must be completely transparent with you by providing information 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language'. Our privacy notice is one of the ways we try and let you know how data is handled (see school's privacy policy –school website)

2. Right of access

You have the right to access your personal information except where:

- It contains confidential information about other people and the School has to balance the rights of other individuals
- Includes information a care professional thinks will cause serious harm to your or someone else's physical or mental wellbeing
- Information which may prejudice an investigation if disclosed

3. Right to rectification

You have the right without undue delay to request the rectification or updating of inaccurate personal data.

4. Right to restrict processing

You can ask for there to be a restriction of processing such as where the accuracy of the personal data is contested. This means that we may only store the personal data and not further process it except in limited circumstances

5. Right to object

You can object to certain types of processing such as direct marketing. The right to object also applies to other types of processing such as processing for scientific, historical research or statistical purposes (although processing may still be carried out for reasons of public interest).

6. Rights on automated decision making and profiling
The law provides safeguards for you against the risk that a potentially damaging decision is taken without human intervention. The right does not apply in certain circumstances such as where you give your explicit consent.

7. Right to data portability
Where personal data is processed on the basis of consent and by automated means, you have the right to have your personal data transmitted directly from one data controller to another where this is technically possible.

8. Right to erasure or 'right to be forgotten'
You can request the erasure of your personal data when:

i) the personal data is no longer necessary in relation to the purposes for which it was collected and processed.
ii) the School's lawful basis for processing your personal data was consent and you no longer provide your consent and there is no other legal ground for the processing , or
iii) you object to the processing and there are no overriding legitimate grounds for the processing.

For further information on the rights of individuals see the ICO's advice and guidance at www.ico.gov.uk

DEFINITIONS
To aid understanding of this document, the following key definitions found in both The Act and GDPR need to be understood:

Personal data
personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria i.e. chronologically ordered sets of manual records containing personal data. The Act extends this to personal data held by an FOI public authority to include manual unstructured systems.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive personal data
The Act and GDPR refers to sensitive personal data as “special categories of personal data”
Special category data:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.
Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to their processing (see Article 10).

Controller
*‘a **Controller** is a natural or legal person or organisation which determines the purposes and means of processing personal data’; and*

Processor
*‘a **Processor** is a natural or legal person or organisation which processes personal data on behalf of a Controller’.*

Processing
‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Data subject:
‘identified or identifiable natural person’

PRINCIPLES
The Act contains 6 Principles relating to the collection, use, processing, and disclosure of data, and the rights of data subjects to have access to personal data concerning themselves.

These Principles are listed below:

- First data protection principle - requirement that processing be lawful and fair;
- Second data protection principle - requirement that purposes of processing be specified, explicit and legitimate;
- Third data protection principle - requirement that personal data be adequate, relevant and not excessive;
- Fourth data protection principle - requirement that personal data be accurate and kept up to date;

- Fifth data protection principle - requirement that personal data be kept for no longer than is necessary;
- Sixth data protection principle - requirement that personal data be processed in a secure manner.

Further information, including advice on all aspects of The Act is available from The Office of The Information Commissioner see website at www.ico.gov.uk

POLICY

Mersey Park Primary School supports the objectives of The Act and is bound by its regulation with regard to personal data. This policy is designed to ensure that the confidentiality of personal data is maintained and to increase the access given to individuals to information relating to them. The Policy is designed to complement other School policies, which relate to personal data in some way. These include but are not limited to HR policies, Information Sharing Protocols and any future policies or protocols agreed by the school including those with external partners.

Mersey Park Primary School will hold the minimum personal data necessary to enable it to perform its functions. The data will be deleted in accordance with the Retention and Destruction Policy of the School. Every effort will be made to ensure that data is accurate and up to date, and that inaccuracies are corrected quickly.

The school will provide to any individual who makes a written request for their personal data; a reply stating whether or not we hold personal data about them. A copy of that information in clear language will be given, unless specific legal exemptions apply. We must fulfil a request for access to personal data within 30 calendar days. The data subject has the right to have records amended if they are inaccurate. There will be no financial charge for this service.

Data sharing within school will only be conducted as per the lawful basis for processing the personal data and within the stated Principles of The Act and GDPR. For further information see our Privacy notice (school website) for its lawful basis for processing personal and special category data; who and why we are required to share personal information; and your rights.

The appointed Data Protection Officer – Jane Corrin must decide on a case by case basis whether disclosure would be appropriate under your Right of Access as certain limited exemptions apply (See 2 Rights of Access above).

The school ensures that personal data is treated as confidential. IT systems are designed to comply with the Data Protection Principles. This ensures that access to personal data can be restricted to identifiable system users. We are committed in its aim that all appropriate staff will be properly trained, fully informed of their obligations under the Act, and made aware of their personal liabilities. The school expects all of its staff to comply fully with this Policy and the Data Protection Principles. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures following from this Policy.

It is the responsibility of the Data Protection Officer to assist the school to ensure compliance with this Policy, to specify the procedures to be adopted, and to ensure Mersey Park Primary School abides by the legislation. The main duties of the Data Protection Officer in relation to Data Protection are:

1. Maintenance of Mersey Park Primary School's external notifications under the Act, acting as the interface with the Office of the Information Commissioner.

2. Development, update and publication of Data Protection procedures.

3. Ensure compliance with Data Protection procedures and practices.

4. Initial contact point for corporate non social care subject access requests.

5. In conjunction with Human Resources, organise education and training seminars regarding Data Protection issues.

In addition to the formal responsibilities outlined above, all staff have a duty to observe the Data Protection Principles and the procedures referred to in this document.

Jane Corrin
Data Protection Officer
May 2018