*'We can and we will'*

# GLEBE PRIMARY SCHOOL

# Data Protection Policy

**Mission Statement:**

At Glebe School we believe in an ethos that values the whole child. We strive to enable all children to achieve their full potential academically, socially and emotionally.

This data protection policy was agreed by the governing body on 11th July 2013.

This policy should be used in conjunction with the Subject Access code of practice attached to this document.

## 1. Introduction

1.1. This policy lays out how Glebe Primary School will comply with its responsibilities under the Data Protection Act 1998.

1.2. All school employees and governors will be bound by its conditions and will be responsible for compliance with the policy and the Act.

1.3. This policy applies to all information that is subject to the Act. This includes all personal data that is processed automatically, any personal data held in a manual form in a relevant filing system and any personal data held in an accessible record.

1.4. The school will nominate a Data Protection officer to oversee the implementation of this policy and to produce guidelines to achieve the standards laid out in this policy.

1.6. A monitoring process will be developed to ensure compliance with this policy.

1.7. The school may take disciplinary action over any breach of the Act and/or this policy by an employee.

## 2. Definitions

2.1. Personal data - Data which relates to a living individual who can be identified from this data. It includes any expressions of opinion and any indications of the intentions of the data controller, or any other person, in respect of the individual.

2.2. Data controller - Headteacher

2.3. Data Processor - A person (other than an employee of the data controller) who processes personal data on behalf of a data controller.

2.4. Data subject - An individual who is the subject of personal data.

2.5. Principles - There are 8 data protection principles which personal data must be processed in accordance with. See appendix 1 for the list in full

## 3. Notification

3.1. Under the Act, Data Controllers are required to notify the Information Commissioner of the processing which they under take.

3.2. The school will maintain its register entry and regularly review its processing to ensure that its register entry is accurate and up to date.

## 4. Information Handling and collection (1st and 2nd Principles)

4.1. The school will process all personal data for the purpose of providing an effective delivery of service in accordance with the aims, responsibilities and obligations of the school.

4.2. All personal data will be processed in accordance with the school's notification with the Information Commissioner.

4.3. The school will, at the point of collection, inform individuals of the purposes for which their personal data is collected.

4.4. Personal data will only be collected where there is a specific purpose. It will not be used for any other purpose except where allowed by the Act or required by law.

## 5. Record management (3rd, 4th, and 5th Principles)

5.1. The school will take steps to ensure that the personal data they hold is accurate in respect of matters of fact and, where necessary, kept up to date

5.2. Opinions recorded on a file will be carefully and professionally expressed.

5.3. The school will not hold personal data for longer than it is reasonably required and will be responsible for setting up retention policies for the record held.

## 6. Security (7th Principle)

6.1. All staff are responsible for ensuring that personal data is held securely at all times.

6.2. Access to all school IT systems will be password protected and only authorised personnel will have access.

6.3. Paper files and manual records containing personal data will be kept in a secure environment.

6.4. When working off site, staff are responsible for ensuring that personal data is held securely.

6.5. Records will be safely and responsibly disposed of when they are no longer required.

6.6. All members of staff will adhere to the school's IT security policies and procedures

## 7. Individual rights (6th Principle)

7.1. The school will process personal data in line with an individual's Rights. (See appendix 2 for full list)

7.2. The Act gives individuals a general right of access to their personal data. This is called the Right of Subject Access. Under the Act, a Data Controller has 40 days to respond to any subject access request made in writing.

7.3. All requests for personal data from individuals will be dealt with in accordance with the school's Access policy and procedures.

## 8. Criminal offences

8.1. The Act creates a number of criminal offences (see appendix 3 for full list.)

8.2. Any member of staff that is found guilty of a criminal offence under the Act may face disciplinary action.

8.3. Any member of staff who is accused of a criminal offence under the Act must report it immediately to the Data Protection Officer.

8.4. Any member of staff who suspects a criminal offence has been committed must report it to the Data Protection Officer.

## 9. Disclosures

9.1. The school reserves the right to disclose information under certain circumstances where allowed by law.

9.2. Disclosures routinely made by the school are listed in the school's notification with the Information Commissioner.

9.4. When a request for disclosure is made the school will consider each request individually and where a disclosure takes place, the school will only disclose the minimum amount required.

9.5. In order to meet its responsibilities, the school will share data with organisations it is obliged to share data with e.g. Ofsted. The school will ensure that the data sharing is in compliance with the law and this policy.

## 10. Complaints, enforcement and dealing with breaches

10.1. All complaints regarding Data Protection are to be passed immediately to the Data Protection Officer.

10.2. Any member of staff who suspects that a breach of the Act has or will occur, must report it to the Data Protection Officer.

10.2. All staff are expected to co-operate in full with any investigation undertaken by the Data Protection Officer, the monitoring officer or the Information Commissioner into an alleged breach of the Act.

## 11. Contact information

11.1. The School Data Protection officer is the Headteacher

11.2 The Local Authority Data Protection Officer can be contacted at

Data Protection Officer,

Legal Services (3E/04), Chief Executive's Office,

Civic Centre, High Street, Uxbridge, UB8 1UW Tel: 01895 55(6923)

Email: RIngle@hillingdon.gov.uk

11.3. More information about the Data Protection Act is available from

The Information Commissioners Office

Tel: Call our helpline on **0303 123 1113** (local rate – calls to this number cost the same as calls to 01 or 02 numbers).

Web address: https://ico.org.uk/for-the-public/official-information/

How to respond to requests for information in schools:

https://ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf

Storing and releasing references:

https://ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf

Updated September 2014
To be reviewed September 2016 reviewed by Mr Alford and Mrs Marks
To be reviewed September 2017

**Appendix 1**

## 8 Data Protection Principles

1. Personal data shall be processed fairly and lawfully.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under the Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data.

**Appendix 2**

## Individual's Rights

The Act gives rights to individuals in respect of personal data held about them by others. These rights are:

1. Right of Subject Access

2. Right to Prevent Processing Likely to Cause Damage or Distress

3. Right to Prevent Direct Marketing

4. Rights in Relation to Automated Decision Making

5. Right to take action for compensation if an individual suffers damage by any contravention of the Act by the data controller

6. Right to take action to rectify, block, erase or destroy inaccurate data

**Appendix 3**

## Criminal Offences under the Data Protection Act 1998

1. Processing without notification

2. Failure to notify the Information Commissioner of changes to the notification register entry

3. Failure to Comply with an Enforcement or Information Notice served by the Information Commissioner

4. Knowingly and recklessly making a false statement in compliance with an Information Notice.

5. Unlawful obtaining, disclosing or procuring the disclosure of personal data.

6. Unlawful selling of personal data.

7. Enforced Subject Access.

Anyone found guilty of a criminal offence could face a fine of up to £5000 in the magistrate's court or an unlimited fine in a crown court.