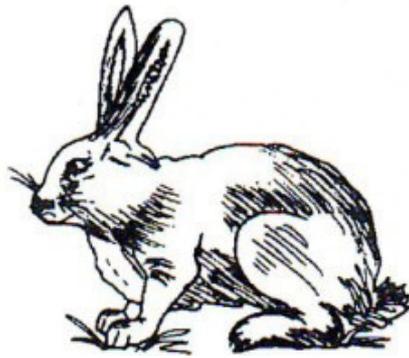


# *Data Protection Policy*



*Harefield Junior School*

*Reviewed February 2017*

**The School is implementing the General Data Protection Regulation (GDPR) and we use data to facilitate our duties regarding the education and well being of our pupils. We are implementing GDPR regarding staff. The GDPR will apply from 25<sup>th</sup> May 2018.**

## **Data Protection Policy**

This document is a statement of the aims and principles of the School, to ensure the confidentiality of sensitive information relating to staff, pupils, parents and governors.

### **Introduction**

Harefield Junior School needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Harefield Junior School must comply with the 8 Data Protection Principles which are set out in the Data Protection Act 1998.

In summary these state that personal data:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for that purpose.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to any other country without adequate protection.

Harefield Junior School and all staff or others who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the School has developed this Data Protection Policy.

This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the School from time to time. Any failures to follow the policy can therefore result

in disciplinary proceedings.

### **The Data Controller and the Designated Data Controllers**

The School as a body corporate is the Data Controller under the 1998 Act, and the Governors are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day-to-day matter.

The School has Designated Data Controllers: they are B Lloyd, and T.Kencroft. We also seek technical support from our maintenance company Azteq.

Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the appropriate Designated Data Controller, who would be the Administrator.

### **Responsibilities of Staff**

All staff are responsible for:

- Checking that any information that they provide to the School in connection with their employment is accurate and up to date.
- Informing the School of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The School cannot be held responsible for any errors unless the staff member has informed the School of such changes.

If and when, as part of their responsibilities, staff collect information about other people (e.g. about a student's course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff set out in the Schools Data Protection Code of Practice.

### **Data Security**

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing or via web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should:

- Be kept in a locked filing cabinet, drawer, safe, locker or class cupboard.

- If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up.
- If a copy is kept on storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

### **Disposal of hard drive data and ICT assets**

The head teacher and Computing Coordinator are responsible for organising the disposal of redundant IT equipment.

We use the company 'PRM Green Technologies' to collect and destruct old and redundant IT equipment- this includes data destruction and certification. Any disposed of equipment is taken off the inventory and is authorised and signed off by the head teacher.

### **Rights to Access Information (Freedom of Information)**

All staff, parents and other users are entitled to:

- Know what information the School holds and processes about them or their child and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the School is doing to comply with its obligations under the 1998 Act.

This Policy document and the School's Data Protection Code of Practice address in particular the last three points above. To address the first point, the School will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the School holds and processes about them, and the reasons for which they are processed.

All staff, parents and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should complete the *Subject Access Request Form* and submit it to the Designated Data Controller. The person will need to prove their identity by an appropriate means acceptable to the data controller.

The School will make a charge of £10 on each occasion that access is requested, although the School has discretion to waive this.

The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 20 days, as required by the 1998 Act.

## **Subject Consent**

In many cases, the School can only process personal data with the consent of the individual. In some cases, if the data is sensitive, as defined in the 1998 Act, express consent must be obtained. Agreement to the School processing some specified classes of personal data is a condition of acceptance of employment for staff. This included information about previous criminal convictions.

Jobs will bring the applicants into contact with children. The School has a duty under the Children's Act 1989 and other enactments to ensure that staff are suitable for the job. The School has a duty of care to all staff and students and must therefore make sure that employees and those who use School facilities do not pose a threat or danger to other users. The School may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The School will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency.

## **Processing Sensitive Information**

Sometimes it is necessary to process information about a person's health, criminal convictions, or race. This may be to ensure that the School is a safe place for everyone, or to operate other School policies, such as the Sick Pay Policy or the Equal Opportunities Policy. This information is considered sensitive under the 1998 Act, staff (and students where appropriate) will be asked to give their express consent for the School to process this data. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason. This also applies to any information about pupils where disclosure may cause serious harm to their physical and/or mental wellbeing or if it discloses abuse or court proceedings.

## **Publication of School Information**

Certain items of information relating to School staff will be made available via searchable directories on the public website, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with the School.

## **Retention of Data**

The School has a duty to retain some staff and student personal data for a period of time following their departure from the School, mainly for legal reasons, but also for other purposes such as being able to provide references or academic transcripts. Different categories of data will be retained for different periods of time.

## **Conclusion**

Compliance with the 1998 Act is the responsibility of all members of the School. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution. Any complaints should be logged with the head teacher and or computing coordinator.