# THE NEW RUSH HALL SCHOOL

# DATA PROTECTION POLICY

Date Policy Created:
Reviewed: Nov 2013

Headteacher: Mr J V d'Abbro
Chairman of Governors: Mr Greg Sage

THE NEW RUSH HALL SCHOOL

A London Borough of Redbridge School

**NEW RUSH HALL SCHOOL**

**DATA PROTECTION POLICY**

## CONTENTS



**NEW RUSH HALL SCHOOL**

**DATA PROTECTION POLICY**

This document is a statement of the aims and principles of the School, for ensuring the confidentiality of sensitive information relating to staff, pupils, parents and governors.
The Headteacher is responsible for ensuring that the school complies with the Data Protection Act 1998.

## Introduction

New Rush Hall School needs to keep certain information about its employees, students and other users to allow it to monitor, for example, performance, achievements, and health and safety. 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, New Rush Hall School must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 ( the 1998 Act). In summary these state that personal data shall:

- Be processed fairly and lawfully;
- Obtained only for lawful purposes, and is not further used in any manner incompatible with those original purposes;
- Be accurate and, where necessary, kept up to date;
- Is adequate, relevant and not excessive in relation to the purposes for which it is processed;
- Not be kept for longer than is necessary for those purposes;
- Processed in accordance with the rights of data subjects under the DPA;

- Be protected by appropriate technical and organizational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage; and
- Not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection of the personal information.

New Rush Hall 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 matters.

The School has three Designated Data Controllers: They are the Headteacher, the Head of School and the Business Manager.

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 Head of School in the first instance.

**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.

- Paper-based personal data must be stored in secure systems with locks. Access to such records must be controlled.

- The school no longer maintains pupil paper-based pupil records. These are now held on the school server. Under no circumstances shall any employee copy or remove these records from the server.

- When a pupil departs from the school all records should be transferred securely.

- Personal information should not be stored on mobile devices or privately owned computer equipment.

- Members of the Senior Management Team may need to store personal information on mobile devices from time to time. In such cases these employees have a responsibility to ensure that appropriate encryption software is installed on their mobile devices.

- **Employees are not permitted to store personal data on memory sticks. Failure to comply with this will lead to disciplinary procedures.**

Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe; or

- 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; and

- Transfer of pupil data must be made using the Secure Server (S2S).

- Documents sent via email that contain data that can identify individuals must be encrypted and password protected in accordance with the security protocol outlined by the Head of School.

**Rights to Access 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. Such requests will be answered within 40 calendar days of receipt.

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.

**Subject Access**

Individuals have the right to requests the personal information a school holds abut them – the right of subject access. Subject access requests (SARs) will be answered within 40 calendar days of receipt. A standard fee of £100 be charged for answering a SAR. A valid SAR should be made in writing. The requester's identity will need to be confirmed. Parents can make a SAR on their children's behalf if the children are deemed too young to look after their own affairs or they have consented to their parents doing this on their behalf. All SARs will should be forwarded to the Head of School. *(It should be noted that SARs are separate to the right of access to educational records under the Pupil Information Regulations which give a parent the right to information in their child's educational record).*

**Sharing Personal Information**

Sharing personal information involves providing it to another organization or person so that they can make use of it. It does not extend to the use of personal information within the school, including use by the Governing Body. The main organisations that the school share personal data with are :-

- Local Authorities
- Other schools and educational bodies; and
- Social Services

The three most important aspects to consider when sharing data are :-

- Making sure you are allowed to share it by checking with the Head of School;
- Ensuring that adequate security is in place to protect it. (This includes checking that the recipient's arrangements are secure enough to receive the information).
- Double check that the information is going to the correct address;
- Only send the information that needs to be sent.

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 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, for example.

**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. Because 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.

**Photographs**

The school may take photos for inclusion in printed prospectus or other school publications or promotional materials including the website. The use of photographs will only be done with specific consent.

**Publication of School Information**

Certain items of information relating to School staff will be made available via searchable directories on the public Web site, 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 and in accordance with guidance issued by The Records Management Society. (See Appendix 1).

**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.