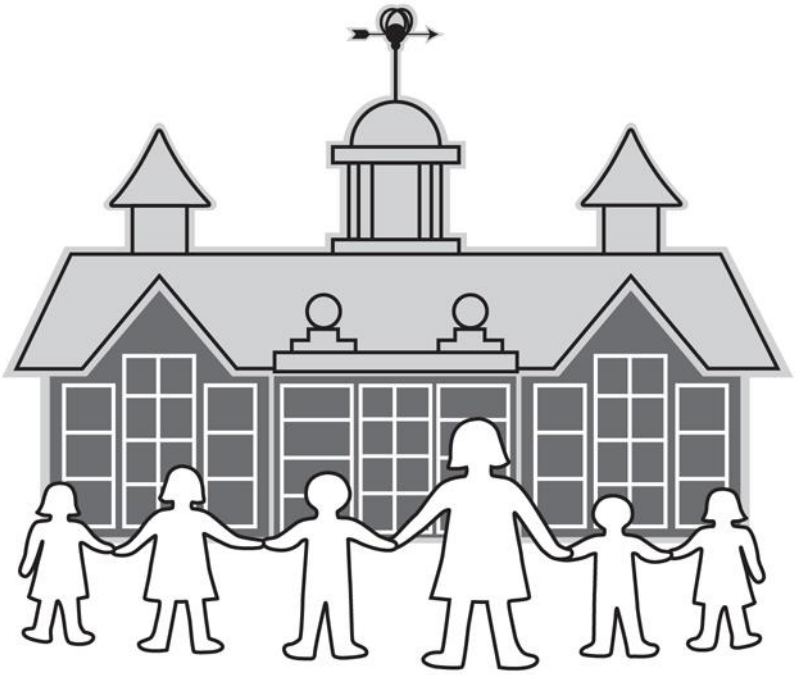
North Ealing Primary School



Data Protection Policy

Committee with oversight for this policy – Resources	
Policy to be approved by - Resources Committee	
Policy last reviewed by the Resources Committee	08/03/2017
Policy last ratified and adopted by Full Governing Body	N/A
Policy / Document due for review	03/2020

North Ealing Primary School
Data Protection Policy

The Governing Body of the school has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The Headteacher and Governors of this School intend to comply fully with the requirements and principles of the Data Protection Act 1985 and the Data Protection Act 2003. All members of staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

Enquiries
Information about the school's Data Protection Policy is available from The School Business Manager. General information about the Data Protection Act can be obtained from the Data Protection Commissioner (www.ico.org.uk).

Fair obtaining and processing
North Ealing Primary School undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data is held, the likely recipients of the data and the data subjects' right of access. If details are given verbally, the person collecting will explain the issues before obtaining the information.

- **Processing** means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.

- **Data subject** means an individual who is the subject of personal data or the person to whom the information relates.

- **Personal data** means data which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be if published in the press, Internet or media.

- **Parent** includes any person having parental responsibility or care of a child.

Registered purposes
The Data Protection Registration entries for the School are available for inspection, by appointment, at the school office. Registered purposes covering the data held at the school are listed on the School's Registration and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subject's consent.

Data integrity
The School undertakes to ensure data integrity by the following methods:

Data accuracy
Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the school of a change of circumstances, their computer record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects every twelve months so they can check its accuracy and make any amendments.

Where a data subject challenges the accuracy of their data, the School will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, the school will try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Governing Body for their judgment. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

Data adequacy and relevance
Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the School will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to

verify certain items of data. The requirement for schools to provide Pupil Census and Work Force Census reports ensures a termly check of pupil data and an annual check of workforce data held. The School Administrator will amend any data that is incorrect. Pupil and staffing records are never deleted from the SIMS software.

Length of time
Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the Head Teacher / School Business Manager to ensure that obsolete data is properly erased.

Subject access
The Data Protection Acts extend to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received from a pupil, the School's policy is that:

Requests from pupils will be processed as any subject access request as outlined below and the copy will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request.

Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.

Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

Processing subject access requests
Requests for access must be made in writing to the Head Teacher.

Pupils, parents or staff may submit a request in writing to the School and the School will respond in not more than 40 days from the request date.

The School will first satisfy itself that the person is correctly identified and that they have an entitlement to the information.

Note: In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 school days in accordance with the current Education (Pupil Information) Regulations.

Authorised disclosures
The School will, in general, only disclose data about individuals with their consent. However there are circumstances under which the School's authorised officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Pupil data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.
- Pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare.
- Pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanor within or in the vicinity of the school.
- Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.
- Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer will be required to sign a form promising not to disclose the data outside the school. Officers and IT personnel working on behalf of the LA are IT liaison/data processing officers, for example in the LA, are contractually bound not to disclose personal data.

Only authorised and trained staff members are allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who **need to know** the information in order to do their work. The school will not disclose

anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything which suggests that they are, or have been, either the subject of or at risk of child abuse.

A **"legal disclosure"** is the release of personal information from the computer to someone who requires the information to do his or her job within or for the school, provided that the purpose of that information has been registered.

An **"illegal disclosure"** is the release of information to someone who does not need it, or has no right to it, or one which falls outside the School's registered purposes.

Data and computer security
North Ealing School undertakes to ensure security of personal data by various approved methods, including limiting access rights, password controls, password controlled data keys and a firewall maintained by the London Grid for learning (LGfL). All staff members with access to sensitive data are required to sign, and adhere to, the requirements of the school's Acceptable Use Agreement which is reviewed annually.

Physical security
Appropriate building security measures are in place, such as alarms, CCTV, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the server room. Disks, tapes and printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.

Procedural security
In order to be given authorised access to the shared computer network, staff will first have undergone an enhanced police check and will also be made aware of the School's required Code of Conduct through induction training. Induction training will ensure staff have knowledge of school protocols and procedures around data protection and will fully understand the need for confidentiality. Reference to staff procedures is highlighted in staff and team meetings. The school's ICT team ensures that ALL members of staff are given appropriate guidance regarding e-safety and protection of personal information.

Any queries or concerns about security of data in the school should in the first instance be referred to the Head Teacher.

Individual members of staff can be personally liable in law under the terms of the Data Protection Act. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

iTrent:
The local authority now use a web based HR and Payroll system. Individual staff members have access to this site through their user name and password. Staff members are responsible for checking that the information held is accurate and are responsible for updating their own personal data. Further information is available from the ITrent support team on 0208 8825 9000.

Further details on any aspect of this policy and its implementation can be obtained from the Head Teacher.

Data Protection Act 1998 – Sensitive personal data.
In this Act "sensitive personal data" means personal data consisting of information as to:

(a) The ethnic or racial origin of the data subject

(b) His political opinions

(c) His religious beliefs or other beliefs of a similar nature

(d) Whether he is a member of a trade union (within the meaning of Trade Union and Labour Relations (Consolidation Act 1992)

(e) His physical or mental health and condition

(f) His sexual life

(g) The commission or alleged commission by him of any offence

(h) Any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

http:/www.legislation.gov/uk/ukpga/1998/29/section2