Harrington Hill Primary School

Address: Mount Pleasant Lane, London E5 9JG | Telephone: 0208 806 7275

Email: admin@harringtonhill.hackney.sch.uk | Website: www.harringtonhill.hackney.sch.uk

# GDPR POLICY

| | | | |
|---|---|---|---|
| **Approved by:** | Governing Body | **Date:** | October 2025 |
| **Last reviewed on:** | October 2025 | | |
| **Next review due by:** | October 2026 | | |

**Harrington Hill Primary School**
**GDPR POLICY**

**Contents**


1. Purpose ..... 3
2. Scope ..... 3
3. General Data Protection Principles ..... 4
4. Lawful processing ..... 4
5. Roles and Responsibilities ..... 5

Employees ..... 5

Pupils over 13 years of age ..... **Error! Bookmark not defined.**

The School - Responsibilities to all data subjects ..... 5

The School - Responsibilities to Pupils ..... 6

Governors ..... 7

6. Photographs, video and CCTV images ..... 7
7. Data Security ..... 7
8. Data Retention and Disposal ..... 8
9. Data Impact Assessments ..... 8
10. Data Subjects right to be forgotten – Data Erasure ..... 9
11. Data Access Requests (Subject Access Requests) ..... 9
12. Breaches ..... 10
13. Notifying the Information Commissioner ..... 10
14. Further information ..... 10

**Purpose**

1.1 The Data Protection legislation (The General Data Protection Regulation (GDPR) and the Data Protection Act 2018) protect individuals with regard to the processing of personal data, in particular by protecting personal privacy and upholding an individual's rights. It applies to anyone who handles or has access to people's personal data.

1.2 This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the GDPR and the Data Protection Act 2018 (DPA 2018). It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

**Scope**

2.1 The GDPR and DPA 2018 have a wider definition of personal data than the Data Protection Act 1998 and includes information generated from cookies and IP addresses if they can identify an individual.

2.2 'Personal data' is any information that relates to an identified or identifiable living individual, which means any living individual who can be identified, directly or indirectly, in particular by reference to—

a. an identifier such as a name, an identification number, location data; or
b. an online identifier; or
c. one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.3 The DPA 2018's wider definition of personal data is broadly defined and is not limited to confidential or sensitive data. It also includes any expression of opinion about an individual, personal data held visually in photographs or video clips (including CCTV) or sound recordings.

2.4 The processing of personal data for must be lawful and fair. Under the DPA 2018 "sensitive processing" means the processing of personal data revealing information on an individual that falls under the following:

- Political opinions;
- Religious or philosophical beliefs;
- Racial/ethnic origin;
- Trade union membership;
- Genetic data;
- Biometric data;
- Health;
- Sex life;
- Sexual orientation.

2.5 This School collects a large amount of personal data every year including: staff records, names and addresses of those requesting prospectuses, examination

marks, references, fee collection as well as the many different types of research data.

2.6 The School may also be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies (e.g. Department of Education) and other bodies.

2.7 To comply with the Data Protection legislation, this School will collect, use fairly, store safely and not disclose personal data to any other person unlawfully.

**General Data Protection Principles**

3.1 The School is accountable and required to demonstrate compliance with six core principles governing processing of personal data:

a. Processing of data is lawful, fair and transparent;
b. Purpose is specified, explicit and legitimate (Purpose limitation);
c. The personal data be adequate, relevant and not excessive (Data minimisation);
d. Data processed is accurate and kept up to date (Accuracy);
e. Personal data be kept for no longer than is necessary (Storage limitation);
f. Personal data is processed in a secure manner (Integrity and confidentiality).

3.2 Under the DPA 2018, the wider territorial scope means that the Regulation applies to any Personal Data of any individual who is located in an EEA country irrespective of the country or territory of the organisation processing the data.

3.3 The School will therefore ensure that its contracts with organisations that may process personal data on its behalf are compliant with the Regulation and offer adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

**Lawful processing**

4.1 The School must have a valid lawful basis in order to process personal data.

4.2 The six lawful basis for processing personal data are:

**(a) Consent**: the individual provides clear consent to process their personal data for a specific purpose;
**(b) Contract**: the member of staff/student/parent has given clear consent for the school to process their personal data for a specific purpose, for example, staff employment contract or pupil placement;
**(c) Legal obligation**: the processing is necessary for the School to comply with the law (not including contractual obligations);
**(d) Vital interests**: the processing is necessary to protect someone's life;
**(e) Public task:** the processing is necessary for the School to perform a task in the public interest/official functions, and the task or function has a clear basis in law;

**(f) Legitimate interests:** the processing is necessary for a legitimate interest or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data, which overrides those legitimate interests.

4.3 The School will generally rely on the following three legal bases for processing data as follows:

(a) Consent;
(b) Contract;
(c) Legal obligation.

4.4 The School will detail its lawful basis for processing personal data in its privacy notice(s).

**Roles and Responsibilities**

Employees

5.1 Every employee, staff member or worker that holds personal information on behalf of the School has to comply with the Data Protection Act when managing that information and must treat all personal data in a confidential manner and follow the guidelines as set out in this document.

5.2 All members of the school community are responsible for taking care when handling, using or transferring personal data.

5.3 All members of the school community have a responsibility for ensuring that data cannot be accessed by anyone who does not have permission to access that data.

5.4 Data breaches can have serious effects on individuals and institutions concerned and can bring the School into disrepute. Members of the School community who breach this Policy and/or the Data Protection legislation will be subject to disciplinary action under the School's Disciplinary Policy, which can include sanctions up to and including dismissal. Such breaches may also lead to criminal prosecution.

The School - Responsibilities to all data subjects

5.5 The School will ensure that it manages and processes personal data properly; and that it protects an individual's right to privacy.

5.6 On request, the School will provide an individual with access to all personal data held on them under a Subject Access Data Request.

5.7 The School has a legal responsibility to comply with the DPA 2018 and the GPDR. The School, as a corporate body, is named as the Data Controller under the DPA 2018.

5.8 The School will consider privacy at the outset and use a data protection by design and by default approach.

5.9 On request, the School will correct any inaccurate personal data and complete any incomplete personal data it holds.

5.10 The School will not exploit any imbalance in power in the relationship between the School and its data subjects.

5.11 The School is committed to ensuring that its staff are aware of data protection requirements and legal requirements and will raise awareness of the importance of compliance.

5.12 The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

**The School - Responsibilities to Pupils**

5.13 As a matter of good practice, this School will use Data Protection Impact Assessments (DPIA) to help assess and mitigate data privacy risks to children.

5.14 Where the School processes data that is likely to result in a high risk to the rights and freedom of its pupils it will always complete a DPIA.

5.15 As a matter of good practice, the School will consult with children aged 13 and over as appropriate when designing its processing.

5.16 If the School relies on consent as the lawful reason for processing data it will ensure that children aged 13 or over understand what they are consenting to. The reasons for lawful processing will appear in the School's Privacy Notice.

5.17 When relying on 'necessary for the performance of a contract' as its the lawful reason for processing data the School will consider the child's competence to understand what they are agreeing to, and to enter into a contract. Where the School believes that a child's competence prohibits informed consent, the School will inform the child of the intention to obtain consent from the child's parent(s)/legal guardian(s). The School will only allow competent children to exercise their own data protection rights.

5.18 Subject to Section 6 below, where the School has relied on consent that was provided by the parent(s)/Legal guardian(s) of the child; when the individual attains 13 years of age the school will comply with request for erasure whenever it can.

5.19 When relying upon 'legitimate interests', we take responsibility for identifying the risks and consequences of the processing, and put age appropriate safeguards in place.

**Governors**

5.20 Governors are responsible for monitoring the School's compliance with the Regulation.

5.21 Governors may periodically review the DPIAs to assess the School's compliance with the Data Protection legislation.

**Photographs, video and CCTV images**

6.1 Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only.

6.2 Unless prior consent from parents/pupils/staff has been given, the School shall not utilise such images for publication or communication to external sources.

6.3 The School is aware that there may be safeguarding and privacy issues stemming from individuals taking still or moving images of a person(s) who could be identified. When taking photographs, parents do not need to obtain the permission of the other parents in case their child appears in the picture. However, the School does ask individuals to respect privacy of others and consider potential safeguarding issues. Parents are asked not to post photographs that contain images of children other than their own on the internet.

**Data Security**

7.1 The School will use proportionate physical and technical measures to secure personal data.

7.2 The School will consider the security arrangements of any organisation with which data is shared shall and where require these organisations to provide evidence of the compliance with the DPA 2018 and GDPR.

7.3 The School will store hard copy data, records, and personal information out of sight and in a locked cupboard. The only exception to this is medical information that may require immediate access during the school day. This will be stored with the School Nurse.

7.4 Sensitive or personal information and data should not be removed from the school site; however, the School acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils.

7.5 To reduce the risk of personal data being compromised any individual taking personal data away from the School site must adhere to the following:

7.5.1 Paper copies of personal data should not be taken off the school site as if misplaced they are easily accessed. If no alternative is available other than to take paper copies of data off the school site then the individual must ensure that the information should not be on view in public places, or left unattended under any circumstances.

7.5.2 Unwanted paper copies of data, sensitive information or pupil files must be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.

7.5.3 Individuals must take care to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.

7.5.4 Where information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.

7.5.5 Teaching staff must ensure that personal data and sensitive personal data is not displayed inadvertently on White Boards during class lessons.

7.5.6 If it is necessary to transport data away from the school, it should be downloaded onto a USB stick. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB, and saved onto the USB only. USB sticks that staff use must be password protected.

7.5.7 Breaches of the policy will be dealt with in accordance with the School's disciplinary policy and could amount to gross misconduct.

**Data Retention and Disposal**

8.1 The School does not retain personal data or information for longer than it is required, however it is recognised that the School will retain some information on employees and pupils after individual has left the School.

8.2 The creation of systems and/or files, which duplicate such data will be avoided; where it is inevitable every care will be taken to ensure that data maintained in secondary systems is accurate and kept up to date. Disposal of IT assets holding data shall be in compliance with ICO guidance.

**Data Impact Assessments**

9.1 The School will conduct assessments to understand the associated risks of processing personal data that it gather/intends to gather to assist in assuring the protection of all data being processed. The School will use these assessments to inform decisions on processing activities.

9.2 Risk and impact assessments shall be conducted in accordance with guidance given by the Information Commissioners Office (ICO).

**Data Subjects right to be forgotten – Data Erasure**

10.1 Data Subjects have the right to request the erasure of their personal data if the data is no longer necessary for the purpose it was collected for. The School will not comply with a request where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the establishment, exercise or defence of legal claims.

10.2 The School will design its processes so that, as far as possible, it is as easy for a data subject to have their personal data erased as it was for the individual to give their consent in the first place.

**Data Access Requests (Subject Access Requests)**

11.1 Individuals whose data is held by the School, have a legal right to request access to such data or information about what is held. No charge will be applied to process the request.

11.2 Requests must be made in writing to the Data Protection Officer and the School will respond to within one month of receiving the request. The one-month period for responding to a request does not begin to run until the School receives any additional information that is necessary to comply with the request.

11.3 Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following organisations without consent:

Other schools

11.3.1 If a pupil transfers from Harrington Hill Primary School to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school.

11.3.2 This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation, which should ensure that there is minimal impact on the child's academic progress because of the move.

**Examination authorities**

11.3.3 This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

**Health authorities**

11.3.4 As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

**Police and courts**

11.3.5 If a situation arises where a criminal investigation is being carried out, the School may have to forward information on to the police to aid their investigation. The School will pass information onto courts as and when it is ordered.

Social workers and support agencies

11.3.6 In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

**Educational division**

11.3.7 The School may be required to pass data on in order to help the government to monitor and enforce laws relating to education.

11.3.8 The Data Protection Officer is:
Elaine Vuong
0208 806 7275

**Breaches**

12.1 The School will normally notify the individual and the ICO of breaches of personal or sensitive data within 72 hours of becoming aware of the breach.

**Notifying the Information Commissioner**

13.1 The School is required to 'notify' the Information Commissioner of the processing of personal data. This information will be included in a public register, which is available on the Information Commissioner's website.

**Further information**

14.1 Additional information on the School's Data Protection obligations is located in its Privacy Notice(s).

14.2 The Data Protection Officer is available to provide advice on this policy and information on how the School applies the GPDR and Data Protection Act. See Section 11.3.8 above for the contact details of the DPO.