



Hamstead Hall Academy Trust

DATA PROTECTION POLICY

1. Introduction

- 1.1 The Hamstead Hall Academy Trust (referred to as "The Trust" and any or all of its Academies) collects and uses certain types of personal information about staff, pupils, parents, and other individuals who come in contact with its Academies, in order to provide education and associated functions.
- 1.1 The Trust may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly, securely and in accordance with the General Data Protection Regulation (GDPR) and other related legislation.
- 1.2 The GDPR applies to all computerised data and manual files that come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable by a specific criterion.

2. Policy Statement

- 2.1 The Board and management of Hamstead Hall Academy Trust are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information Hamstead Hall Academy Trust collects and processes in accordance with the General Data Protection Regulation (GDPR).
- 2.2 Compliance with the GDPR is described by this policy and other relevant policies, along with connected processes and procedures.
- 2.3 The GDPR and this policy apply to all of Hamstead Hall Academy Trust's personal data processing functions, including those performed on pupils', clients', employees', volunteers', suppliers' and partners' personal data, and any other personal data the organisation processes from any source.
- 2.4 This policy applies to all governors, employees and volunteers of Hamstead Hall Academy Trust and any other interested parties, such as outsourced suppliers of services. Any breach of the GDPR will be dealt with under the disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.
- 2.5 Partners and any third parties working with or for Hamstead Hall Academy Trust and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may

access personal data held by Hamstead Hall Academy Trust without having first entered into a data confidentiality agreement, which imposes on the third party obligations no less onerous than those to which Hamstead Hall Academy Trust is committed, and which gives Hamstead Hall Academy Trust the right to audit compliance with the agreement.

3. Links to other Policies

The Data Protection Policy is to read in conjunction with the:

- ICT Policy
- CCTV Policy
- Data Retention Schedule

4. Roles and Responsibilities

- 4.1 The Trust is a registered data controller.
- 4.2 The Trust Board and all those in managerial or supervisory roles throughout Hamstead Hall Academy Trust are responsible for developing and encouraging good information handling practices. The Trust Board is ultimately accountable for ensuring that The Trust complies with all relevant legislation including for data protection.
- 4.3 The Data Protection Officer (DPO) is responsible for overall coordination of data protection including ICO registration and overseeing responses to subject access requests.

5. Personal Data

- 5.1 'Personal data' is information that identifies an individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain.
- 5.2 A sub-set of personal data is known as 'special category personal data'. This special category data is information that reveals:
 - 5.2.1 race or ethnic origin;
 - 5.2.2 political opinions;
 - 5.2.3 religious or philosophical beliefs;
 - 5.2.4 trade union membership;
 - 5.2.5 physical or mental health;
 - 5.2.6 an individual's sex life or sexual orientation;
 - 5.2.7 genetic or biometric data for the purpose of uniquely identifying a natural person.

- 5.3 Special Category Data is given special protection, and additional safeguards apply if this information is to be collected and used.
- 5.4 Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.
- 5.5 The Trust does not intend to seek or hold Special Category Data (previously known as sensitive personal data) about staff or students except where we have been notified of the information, or it comes to the attention of our Academies via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff or students are under no obligation to disclose to our academies their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and / or parenthood are needed for other purposes, e.g. pension entitlements).

6. Data Protection Principles

- 6.1 All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Hamstead Hall Academy Trust's policies and procedures are designed to ensure compliance with the principles.
- 6.2 The six data protection principles as laid down in the GDPR are followed at all times:
 - 6.2.1 personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met;
 - 6.2.2 personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;
 - 6.2.3 personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;
 - 6.2.4 personal data shall be accurate and, where necessary, kept up to date;
 - 6.2.5 personal data processed for any purpose(s) shall not be kept in a form which permits identification of individuals for longer than is necessary for that purpose / those purposes;
 - 6.2.6 personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

6.3 In addition to this, Hamstead Hall Academy Trust is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law.

6.4 Hamstead Hall Academy Trust and its Academies is committed to complying with the Principles in 6.2 at all times.

This means that the Hamstead Hall Academy Trust will:

6.4.1 inform individuals about how and why we process their personal data through the privacy notices which we issue;

6.4.2 be responsible for checking the quality and accuracy of the information;

6.4.3 regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the data retention schedule;

6.4.4 ensure that when information is authorised for disposal it is done appropriately;

6.4.5 ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant security policy requirements at all times;

6.4.6 share personal information with others only when it is necessary and legally appropriate to do so;

6.4.7 set out clear procedures for responding to requests for access to personal information known as subject access requests;

6.4.8 report any breaches of the GDPR in accordance with the procedure

7. Conditions for processing in the first Data Protection principle

7.1 The individual has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given.

7.2 The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering into a contract with the individual, at their request.

7.3 The processing is necessary for the performance of a legal obligation to which we are subject.

7.4 The processing is necessary to protect the vital interests of the individual or another.

7.5 The processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in us.

7.6 Outside of fulfilling our public task, the processing is necessary for a legitimate interest of The Trust or that of a third party,

except where this interest is overridden by the rights and freedoms of the individual concerned.

8. Use of personal data by Hamstead Hall Academy Trust

- 8.1 Hamstead Hall Academy Trust processes personal data on pupils, staff and other individuals such as visitors. In each case, the personal data must be processed in accordance with the data protection principles as outlined in paragraph 6.2 above.

Pupils

- 8.2 The personal data held regarding pupils includes contact details, assessment / examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs.
- 8.3 The data is used in order to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the academy as a whole is doing, together with any other uses normally associated with this provision in a school environment.
- 8.4 The Hamstead Hall Academy Trust may make use of limited personal data (such as contact details) relating to pupils, and their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with pupils of the academy, but only where consent has been provided for this.

In particular Hamstead Hall Academy Trust may:

- 8.4.1 transfer information to any association society or club set up for the purpose of maintaining contact with pupils or for fundraising, marketing or promotional purposes relating to the academy but only where consent has been obtained first;
- 8.4.2 make personal data, including sensitive personal data, available to staff for planning curricular or extra-curricular activities;
- 8.4.3 keep the pupil's previous school informed of his/ her academic progress and achievements e.g. sending a copy of the school reports for the pupil's first year at the Academy to their previous school;
- 8.4.4 use photographs of pupils in accordance with the associated photography procedures.

- 8.5 Any wish to limit or object to any use of personal data should be notified to the Data Protection Officer in writing, which notice will be acknowledged by the relevant school in writing. If, in the view of the Data Protection Officer the objection cannot be maintained, the individual will be given written reasons why the Hamstead Academy Trust cannot comply with their request.

Staff

- 8.6 The personal data held about staff will include contact details, employment history, information relating to career progression, information relating to DBS checks and photographs, as well as information required to administer your terms and conditions of employment including occupational pensions.
- 8.7 The data is used to comply with legal obligations placed on the Trust in relation to employment, and the education of children in a school environment. The Trust may pass information to other regulatory authorities where appropriate, and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.
- 8.8 Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as “spent” once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.
- 8.9 Any wish to limit or object to the uses to which personal data is to be put should be notified to the Data Protection Officer who will ensure that this is recorded, and adhered to if appropriate. If the Data Protection Officer is of the view that it is not appropriate to limit the use of personal data in the way specified, the individual will be given written reasons why the Academy cannot comply with their request.

Information relating to DBS checks

- 8.9.1 DBS checks are carried out on the basis of the academy trust’s legal obligations in relation to the safer recruitment of Staff as stipulated in the Independent School Standards Regulations and the DBS information (which will include personal data relating to criminal convictions and offences) is further processed in the substantial public interest, with the objective of safeguarding children. Retention of the information is covered by the Data Retention Schedule.
- 8.9.2 Access to the DBS information is restricted to those staff who have a genuine need to have access to it for their job roles. In addition to those provisions of the GDPR and the Data Protection Act 2018, disclosure of this information is restricted by section 124 of the

Police Act 1997 and disclosure to third parties will only be made if it is determined to be lawful.

Other Individuals

- 8.10 Hamstead Hall Academy Trust may hold personal information in relation to other individuals who have contact with the school, such as volunteers and guests. Such information shall be held only in accordance with the data protection principles, and shall not be kept longer than necessary.

9. Security of personal data

- 9.1 All governors, employees and volunteers are responsible for ensuring that any personal data that Hamstead Hall Academy Trust holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Hamstead Hall Academy Trust to receive that information and has entered into a confidentiality agreement.
- 9.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. All personal data should be treated with the highest security and must be kept:
- in a lockable room with controlled access; and/or
 - in a locked drawer or filing cabinet; and/or
 - if computerised, password protected in line with corporate requirements in the Access Control Policy; and/or
 - stored on computer media which are encrypted in line with the Secure Disposal of Storage Media Procedure.
- 9.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised personnel. All governors, employees and volunteers are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort
- 9.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation. As soon as manual records are no longer required for day-to-day business use, they must be removed to secure archiving or securely destroyed
- 9.5 Personal data may only be deleted or disposed of in line with the Records Retention Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed, as required by the Secure Disposal of Storage Media Procedure, before disposal.

9.6 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

9.7 For further details as regards security of IT systems, please refer to the ICT Policy.

10. Disclosure of personal data to third parties

10.1 Hamstead Hall Academy Trust must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All governors, employees and volunteers should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of Hamstead Hall Academy Trust's business.

10.2 The following list includes the most usual reasons that Hamstead Hall Academy Trust will authorise disclosure of personal data to a third party:

10.2.1 To give a confidential reference relating to a current or former employee, volunteer or pupil;

10.2.2 for the prevention or detection of crime;

10.2.3 for the assessment of any tax or duty;

10.2.4 for administration of pensions and employee benefits;

10.2.5 where it is necessary to exercise a right or obligation conferred or imposed by law upon the Academy (other than an obligation imposed by contract);

10.2.6 for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);

10.2.7 for the purpose of obtaining legal advice;

10.2.8 for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);

10.2.9 to publish the results of public examinations or other achievements of pupils of the Academy;

- 10.2.10 to disclose details of a pupil's medical condition where it is in the pupil's interests to do so and there is a legal basis for doing so, for example for medical advice, insurance purposes or to organisers of school trips. The legal basis will vary in each case but will usually be based on explicit consent, the vital interests of the child or reasons of substantial public interest (usually safeguarding the child or other individuals);
 - 10.2.11 to provide information to another educational establishment to which a pupil is transferring;
 - 10.2.12 to provide information to the Examination Authority as part of the examination process; and
 - 10.2.13 to provide information to the relevant Government Department concerned with national education. At the time of the writing of this Policy, the Government Department concerned with national education is the Department for Education (DfE). The Examination Authority may also pass information to the DfE.
- 10.3 The DfE uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified from them. On occasion the DfE may share the personal data with other Government Departments or agencies strictly for statistical or research purposes.
- 10.4 Through any of its Academies, Hamstead Hall Academy Trust may receive requests from third parties (i.e. those other than the data subject, the Academy, and employees of the Academy) to disclose personal data it holds about pupils, their parents or guardians, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned, or Hamstead Hall Academy Trust or any of its Academies.
- 10.5 All requests for the disclosure of personal data must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer (DPO).

11. Confidentiality of pupil concerns

- 11.1 Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, the Trust/or the academy will maintain confidentiality unless it has reasonable grounds to believe that the

pupil does not fully understand the consequences of withholding their consent, or where the academy believes disclosure will be in the best interests of the pupil or other pupils. Disclosure for a safeguarding purpose will be lawful because it will be in the substantial public interest.

12. Subject access requests (SARs)

- 12.1 Anybody who makes a request to see any personal information held about them by Hamstead Hall Academy Trust or an individual academy is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure, provided that they constitute a "filing system" (see clause 1.5).
- 12.2 The Data Protection Officer is responsible for co-ordinating all SARs.

13. Right to object to processing

- 13.1 An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest where they do not believe that those grounds are adequately established.
- 13.2 Such considerations are complex and must always be referred to the DPO. Where such an objection is made, it must be sent to the DPO within 2 working days of receipt, who will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.
- 13.3 The DPO shall be responsible for notifying the individual of the outcome of their assessment within twenty working days of receipt of the objection.

14. Right to rectification

- 14.1 An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent to the DPO within 2 working days of receipt, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.
- 14.2 Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data, and communicated to the individual. The individual shall be given the option of a review under the data protection complaints procedure, or an appeal direct to the Information Commissioner.

- 14.3 An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

15. Right to erasure

- 15.1 Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:
- 15.1.1 where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;
 - 15.1.2 where consent is withdrawn and there is no other legal basis for the processing;
 - 15.1.3 where an objection has been raised under the right to object, and found to be legitimate;
 - 15.1.4 where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);
 - 15.1.5 where there is a legal obligation on the Academy Trust to delete.
- 15.2 The Data Protection Officer will make a decision regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

16. Right to restrict processing

- 16.1 In the following circumstances, processing of an individual's personal data may be restricted:
- 16.1.1 where the accuracy of data has been contested, during the period when the Academy is attempting to verify the accuracy of the data;
 - 16.1.2 where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;
 - 16.1.3 where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim;
 - 16.1.4 where there has been an objection made, pending the outcome of any decision.

17. Right to portability

- 17.1 If an individual wants to send their personal data to another organisation they have a right to request that the Trust provides their information in a structured, commonly used, and machine readable format. As this right is limited to situations where the Academy Trust is processing the information on the basis of consent or performance of a contract, the situations in which this right can be exercised will be quite limited. If a request for this is made, it should be forwarded to the Data Protection Officer within 2 working days of receipt, who will review and revert as necessary.

18. Breach of any requirement of the GDPR

- 18.1 Any and all breaches of the GDPR, including a breach of any of the data protection principles shall be reported as soon as it is/ they are discovered, to the DPO.
- 18.2 Once notified, the DPO shall assess:
- 18.2.1 the extent of the breach;
 - 18.2.2 the risks to the data subjects as a consequence of the breach;
 - 18.2.3 any security measures in place that will protect the information;
 - 18.2.4 any measures that can be taken immediately to mitigate the risk to the individuals.
- 18.3 Unless the DPO concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the Trust, unless a delay can be justified.
- 18.4 The Information Commissioner shall be told:
- 18.4.1 details of the breach, including the volume of data at risk, and the number and categories of data subjects;
 - 18.4.2 the contact point for any enquiries (which shall usually be the DPO);
 - 18.4.3 the likely consequences of the breach;
 - 18.4.4 measures proposed or already taken to address the breach.
- 18.5 If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the DPO shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

18.6 Data subjects shall be told:

- 18.6.1 the nature of the breach;
- 18.6.2 who to contact with any questions;
- 18.6.3 measures taken to mitigate any risks.

18.7 The DPO shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed at board level and a decision made about implementation of those recommendations.

