GREAT HEIGHTS ACADEMY TRUST

Data Protection Policy

1. Introduction

1.1 It is necessary for the Trust to collect personal data relating to pupils, parents, staff, governors, service providers and external agencies who work with the Trust in order to carry out its function.

1.2 In some instances the Trust may also be required by law to collect certain specified personal data to comply with the requirements of relevant central government departments.

1.3 The Trust is registered as a **data controller** meaning that it is legally responsible for handling (both storing and processing) such information in accordance with legislation.

1.4 All personal information held by the Trust will be stored and handled in accordance with the Data Protection Act 2018 and the General Data Protection Regulations.

1.5 The Trust ensures that when sharing any data with third parties (e.g. payroll providers, external HR providers or other service providers) that those third parties are compliant with the relevant data protection laws and the information is shared securely.

This policy sets out the following information:

- The purpose and scope of the policy,
- Definitions of key terms used in the policy,
- The responsibilities and requirements on the Trust,
- The data principles and information relating to data collection and processing,
- Information relating to privacy notices,
- Information regarding the role of the Data Protection Officer,
- Individual's rights,
- Subject access request,
- Data Protection Impact Assessments,
- Data breaches,
- Consent,
- CCTV,
- Data Security,
- Details relating to the implications of breaching the policy,
- ICO and notification obligations.

2. Purpose and Scope

2.1 The purpose of this policy is to ensure that the Trust and its employees are aware of the relevant data protection legislation in force and are handling data in compliance with this legislation.

2.2 In the course of their work many Trust employees will be required to take part in the acquisition, recording, handling, storage and processing of personal data and this must always be in accordance with this policy and the relevant legislation as outlined above.

2.2 This policy will help those employees to understand the meaning and significance of such legislation in relation to assisting the performance of the practical duties of their employment.

2.3 The Trust will ensure that (in addition to those employees directly involved in the handling of data) all members of staff, governors, volunteers, trainees, external contractors and/or consultants and any partners of the Trust who may have access to any personal data will receive appropriate information and/or training to make them fully aware of their individual and corporate responsibilities in this regard.

2.5 Such information or training will include making all employees (and others listed in the preceding clause) aware that breaches of data protection legislation have the potential to expose both the individual and the responsible organisation to possible legal action (both criminal and civil).

2.6 This policy should be approved by the Governors and read by all employees, volunteers, contractors and other third parties when handling personal data controlled by the Trust. The policy should be made available on the Trust website.

Definitions

Data controller	A data controller is the individual or the legal person who controls and is responsible for the keeping and use of the personal information in either digital or paper format (or both). A data controller determines the purposes and means of processing personal data.
Data Processor	A data processor is responsible for processing the personal data on behalf of the data controller. Data processors must maintain records of personal data and processing activities.
Data Protection Legislation	The Data Protection Act 2018 and the General Data Protection Regulations and any other legislation from time to time in force.
Data Subject	The person who the personal data belongs to.
ICO	Information Commissioners Office; the office responsible for monitoring compliance with data protection laws and investigating and penalising breaches.
Personal data	Personal data is any information relating to an identified or identifiable natural person (data subject) which would allow you to identify (or makes it possible to identify) that person.
Processing	Processing refers to the recording, handling, using and sharing of personal data.
Subject Access Request	A data subject's right to request access to the information that a company or organisation holds about them including why they hold

	this information, what they do with this information and who they share it with.
Data Protection Impact Assessment	A process to help identify and minimise the data protection risks of a project which involves data processing; particularly useful when introducing a new data processing process, system or technology.

Responsibilities and requirements

3.1 As a data controller the Trust is responsible for ensuring that it only collects the required data necessary to carry out its role as an educational provider. The Trust recognises that obtaining additional data to that which is necessary is contrary to the Data Protection Laws.

3.2 The Trust is responsible for obtaining, storing and handling that data in a secure manner and will keep records of what data is held and the purposes for which it is held.

3.3 The Trust is responsible for ensuring that it only shares data with third parties where this is necessary for providing the full educational experience for the children. The Trust is required to ensure that it only shares that data which is required by the third party for performing its function and it shares this data in a secure way.

3.4 The Trust is responsible for ensuring that any third party accessing or processing data controlled by the Trust will do so in a safe and secure manner and in compliance with the data protection laws in force.

3.5 The Trust is required to notify data subjects as to the personal data they hold in relation to that data subject as well as the legal basis for holding that data, how the Trust uses that data, who the data may be shared with and how it is stored. This is done in the privacy notices (please see the section of this policy entitled 'Privacy Notices' for further information).

3.6 The Trust is required to appoint a Data Protection Officer (more information about the role of the data protection officer is set out under the section entitled 'Data Protection Officer' below).

3.7 The Trust is required to register itself as a data controller with the Information Commissioners Office.

3.8 The Trust is required to obtain full records of all personal data held and maintain these records in accordance with the Records Management and Retention policy.

3.9 The Trust has an obligation to deal with any subject access requests in a timely manner (further information regarding this is set out under the Subject Access Request section below).

3.10 The Trust Board has overall responsibility for ensuring that the Trust complies with its obligations under the relevant data protection laws and this policy.

Data Principles, Collection and Processing

4.1 The GDPR sets out the data protection principles which the Trust must comply with. These principles state that personal data must be:

4.1.1 Processed lawfully, fairly and in a transparent way.

4.1.2 Collected for a specified, explicit and legitimate purpose.

4.1.3 Adequate, relevant and limited to what is necessary for the purposes for which it is processed.

4.1.4 Accurate and up to date.

4.1.5 Kept for no longer than is necessary for the purpose for which it is processed.

4.1.6 Processed in a way that ensures it is secure.

4.2 When collecting personal data from parents/children/staff/third parties, the Trust must only collect the personal data necessary for the purpose that the data is required.

4.3 The Trust must have a valid lawful basis for collecting and processing personal data. There are six lawful bases available and most require the processing to be necessary. The Trust must determine the lawful basis for collecting and processing the personal data prior to collection.

4.4 The lawful bases are:

4.4.1 Consent – the individual has given clear consent for the Trust to process their personal data for a specific purpose.

4.4.2 Contractual – the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering a contract.

4.4.3 Legal Obligation – the processing is necessary for you to comply with the law (not including contractual obligations).

4.4.4 Vital Interests – the processing is necessary to protect someone's life.

4.4.5 Public Task – the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

4.4.6 Legitimate Interest – the processing is necessary for your legitimate interests 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. (This cannot apply if you are public authority processing data to perform your official tasks, this would include Trusts).

4.5 The Trust must only then use the personal data for the purpose for which it has been collected. If they require the use of that personal data for another purpose they must contact the data subject to notify them of this.

4.6 The personal data collected must be kept in compliance with the Records Management and Retention Policy.

4.7 If the Trust uses any third parties for processing personal data (e.g. progress tracking systems) then it is Trust's responsibility to ensure that the third party complies with data protection laws when processing that data.

Privacy Notices

5.1 Privacy notices should be prepared by the Trust in order to inform the data subjects about the data processing it carries out.

5.2 Privacy notices must include information such as the personal data required, why that personal data is required, what the personal data will be used for, how the personal data will be stored/shared/processed, who the data protection officer is and the rights that an individual has in relation to their personal data.

5.3 Privacy notices should be prepared for any personal data obtained by the Trust but will most commonly be split into a privacy notices for parents/children and a privacy notice for staff/volunteers/contractors.

5.4 The Trust should publish the relevant privacy notices on to the Trust's website.

Data Protection Officer

6.1 The Trust is a public authority for the purposes of the Data Protection Act and therefore requires a data protection officer (DPO).

6.2 A DPO should be appointed by all Trusts in England and the officer should be someone who is independent from the processing of personal data.

6.3 The DPO should have specialist knowledge of data protection laws and the requirements on the Trust for compliance, and should be someone who is able to advise and influence the senior leadership of the Trust.

6.4 The DPO will assist the Trust in monitoring internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (see the section on this further on in this policy) and act as a point of contact for data subjects and the supervisory authority (ICO).

6.5 The DPO's details must be made available to the data subjects, this is done through the privacy notices for the Trust.

6.6 The Trust can refer to Article 39 GDPR for further definition of the tasks of the DPO.

Individual's Rights

7.1 The GDPR provides the following rights for individuals:

7.1.1 The right to be informed – about the collection and use of their personal data. The key is that the Trust is transparent about the collection and use of personal data. This information is set out in the privacy notice.

7.1.2 The right of access – see the subject access request section of this policy at point 8 below.

7.1.3 The right to rectification – this provides the right to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request to rectify either verbally or in writing and the Trust will have one month to respond to that request.

7.1.4 The right to erasure – (also known as the right to be forgotten) This is not an absolute right and only applies in certain circumstances. An individual can make a request and the Trust would have one month to respond to such a request. The Trust should refer to their Records Management and Retention policy for information about deleting personal data.

7.1.5 The right to restrict processing – Individuals have a right to request the restriction or suppression of their personal data in certain circumstances. Again, this is not an absolute right and only applies in certain circumstances. When processing is restricted you are only permitted to store the personal data, but not use it.

7.1.6 The right to data portability – This gives the individual the right to obtain and reuse their personal data for their own purposes across different services.

7.1.7 The right to object – gives an individual the right to object to the processing of their personal data in certain circumstances. Individuals have an absolute right to stop their data being used for direct marketing. In other circumstances the Trust will be able to continue processing personal information if there is a compelling reason to do so.

7.1.8 Rights in relation to automated decision making and profiling – (this refers to making a decision solely by automated means without any human involvement). Profiling is automated processing of personal data to evaluate certain things about an individual.

7.2 All individuals have the rights set out above. If the Trust receives a request in relation to any of the above rights then the Trust should contact the DPO for further advice. A procedure for dealing with such requests is set out at Appendix 1 to this policy.

Subject Access Request

8.1 A subject Access Request is the term used for an individual's right to request to view their personal information that is held by the Trust. It is also known as the right of access referred to at 7.1.2 of this policy.

8.2 A data subject has the right to find out what data is held on them and how it is used. An individual should make a subject access request before exercising the other information rights set out in section 7 above.

8.2 Subject Access Requests can be made verbally or in writing but, to assist individuals in making such requests, the Trust has prepared a subject access request form which can be obtained from the Trust office and is set out in Appendix 2 below.

8.3 The Trust should respond to any subject access request within one month of receipt of such request. The Trust should contact the DPO if they receive a subject access request.

8.4 The Trust is only obliged to provide information relating to the data subject and is not able to provide any personal information which may identify another individual unless the Trust has that individual's consent. The Trust is also not permitted to provide any personal information that may be capable of identifying an individual other than the requesting data subject.

8.5 The Trust should provide a copy of the privacy notice or refer the data subject to the privacy notice on the website, as well as providing the information, as part of the subject access request.

8.6 The Trust should keep a record of all subject access requests; the record should include details about the date of the request and the date of the response.

8.7 The Trust can refuse to provide information as part of a subject access request in certain circumstances, for example, the information has been provided following a previous request and there has been no changes to the information held or the way it is processed since that initial request. Where the Trust refuses to provide information requested it must document this and the reasons for the refusal.

8.8 Personal data about a child belongs to that child and not the child's parents/carers. Parents are able to make a subject access request on behalf of their child where the child is unable to understand their rights and the implications of a subject access request. Children under 12 years old are generally not considered mature enough to understand these rights although each case ought to be considered on its facts.

8.9 The procedure for what to do if you receive a subject access request is set out in Appenidix 2 to this policy.

Data Protection Impact Assessments

9.1 A data protection impact assessment (DPIA) should be carried out when the processing of data is likely to result in a high risk to the individuals. It is good practice to carry out a DPIA when carrying out activities that require data processing.

9.2 The DPIA must describe the nature, scope, context and purposes of the processing; assess necessity, proportionality and compliance measures in place; identify and assess risks to the individual and identify any additional measures to mitigate those risks.

9.3 Once the DPIA has been carried out the Trust should sign off the project/activity requiring the data processing and record the outcomes of the DPIA.

9.4 In carrying out your DPIA, you should seek advice from DPO, where necessary.

9.5 It is important to keep a record of your DPIA for each activity.

9.6 If the risk to personal information is identified as a result of the DPIA and the risk cannot be mitigated against then the Trust must contact the ICO before proceeding with the activity.

Data Breaches

10.1 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It includes breaches which resulted from both accidental and deliberate causes.

10.2 If anyone within the Trust suspects that there has been a data breach they must report this to the DPO and senior leadership team as soon as possible.

10.3 Any breach which is likely to result in a high risk of adversely affecting an individuals' rights and freedoms will need to be reported to the ICO, within 72 hours of becoming aware of that breach.

10.4 In assessing risk to the rights and freedoms the Trust should have regard for Recital 85 GDPR.

10.5 If a breach is likely to result in a high risk to the rights and freedoms of individuals, the Trust must inform those concerned directly and without undue delay.

10.6 The Trust must keep a record of all breaches, whether reported or not. If a breach has not been reported, a record must be kept of the reasons for not reporting.

10.7 The procedure for dealing with a data protection breach is set out in Appendix 3.

Consent

11.1 The Trust must obtain consent from parents/pupils for obtaining and processing certain personal data such as the use of photographs (particularly for marketing purposes such as brochures and websites).

11.2 The consent must be freely given, specific, informed and unambiguous and confirmed by a statement or clear affirmative action.

11.3 A record must be kept of all consents provided.

11.4 A consent form must set out the ways an individual may be able to change or withdraw their consent.

11.5 The Trust must seek guidance from the DPO if it has any queries relating to obtaining consent.

CCTV

12.1 The Trust may use CCTV in and around Trust to ensure the safety of all children whilst in Trust. The Trust will comply with the ICO's code of practice for the use of CCTV at all times.

12.2 We are not required to ask permission from individuals for using the CCTV around Trust but we do make it clear that CCTV is in use. We do this by making the CCTV cameras clearly visible and by displaying signs explaining that CCTV is in use.

12.3 Whilst an individual may make a subject access request to view CCTV footage, the Trust will need to consider the points made in clause 8.4 above in deciding whether it is appropriate to allow such a request.

Data Security

13.1 The Trust will ensure that all data is collected, stored, processed and shared in a secure manner; whether the data is held in electronic or paper format.

13.2 The Trust will ensure that any digital sharing of personal data is done in accordance with the Trusts Acceptable Use policy.

13.3 Where data is shared with a third party who is responsible for processing that data for a particular purpose, the Trust must ensure that the third party is compliant with the GDPR and DPA.

13.4 Any personal data that is no longer needed will be disposed of in line with the Record Management and Retention policy and will be disposed of securely.

Breach of Policy

14.1 The Head teacher and the DPO are responsible for reviewing and monitoring compliance with this policy.

14.2 Any reports of staff, governors or third parties breaching this policy should be reported to the DPO and investigated fully. Any breaches will be taken seriously.

Information Commissioners Office and Notification

15.1 The Trust is registered as a data controller with the ICO and will renew this registration on an annual basis as required by the legislation.

Relationship with existing policies

This policy should be read in conjunction with the following policies:

- Privacy notices
- Freedom of Information policy
- Record management and retention policy
- Acceptable Use policy

Appendix One:

An individual may contact the Trust in order to request any of their rights set out in clause 7.1 of this policy. The request may be verbal or in writing and could be made to any member of staff.

If you believe that a request has been made by an individual for any of the rights set out in 7.1.1 – 7.1.8 of this policy then please follow the procedure below when dealing with such a request.

1. Acknowledge receipt of the request as soon as possible (it may also be necessary at this stage to clarify your understanding of the request being made). The acknowledgement should be sent within 3 working days of receipt.

2. Speak to the senior leadership team (SLT) and the DPO for advice about the particular request that you have received. It may not be possible (in law) to carry out the particular request so an assessment will need to be made of all the circumstances. You will need to pass the request to the SLT and DPO within 3 working days of receipt and confirm to the SLT and DPO that you have acknowledged receipt.

3. The DPO and SLT should consider the request as soon as reasonable practicable and should provide a response to the request within one month of initial receipt by the Trust.

4. The Trust should keep a record of all such requests made. The record should include the date of receipt, details of the request (which right was requested), the date of response and the outcome. If it is not possible to carry out the request then the record should state the reasons why this was not possible.

The most common request likely to be received is the right to access (also known as a subject access request). Further details on the process for dealing with a subject access request are set out in Appendix Two of this policy.

Appendix Two – Subject Access Requests

An individual can make a subject access request in any form whether verbal or in writing. The Trust has a subject access request form which they should encourage individuals to complete if they wish to make a subject access request but it is not necessary for the individual to use that form for their request.

When dealing with a subject access request the Trust should have regard to the procedure set out in Appendix One.

The Trust should also note the following:

1. An individual is only entitled to their own personal data and, in some instances, it may be necessary to establish the identity of the individual making the request before any information is provided.

2. You are not able to provide personal data that may be capable of identifying another individual unless you have that individual's consent. It is therefore necessary to carefully consider all personal data on the subject requesting access prior to disclosure.

3. In addition to providing the individuals personal data you will also need to provide the following information:
    a. The purpose for which you process their personal information,
    b. The categories of personal information concerned,
    c. Information of any third parties that you share the personal information with,
    d. The retention period of storing the personal data or criteria for establishing the retention period,
    e. The existence of the other rights the individual has, set out in clause 7 of this policy,
    f. The right to complain to the ICO,
    g. Information about the source of the data, where it was not obtained directly from the individual,
    h. The existence of any automated decision-making (including profiling) of the personal data,
    i. The safeguards in place if and when the personal information is transferred to a third country or international organisation (this one is unlikely to apply to the Trust).

4. When assessing what information to provide as part of a subject access request you should first be guided by the request made and note that you will need to provide any records you have relating to the request including (but not limited to) records on SIMs, CPOMs, the child's file and emails.

5. In responding to the subject access request the Trust should use the subject access information form.

Appendix Three – Data Breach Procedure

If you suspect a data breach has occurred please follow the procedure set out below:

1. Report the suspected breach as soon as possible to a member of the senior leadership team.

2. Make a written record of the suspected breach and the date it was reported to the SLT on the data breach log.

3. The SLT may wish to contact the DPO at this stage for advice.

4. The SLT/DPO should consider if any action is required to contain the breach if there is an ongoing threat to the security of personal data (e.g. if the computer systems have been hacked then consider changing passwords etc).

5. The SLT/DPO should investigate the suspected breach to establish how it happened and what the impact of the breach has been.

6. The SLT/DPO should consider whether the matter needs to be reported to the ICO. A data breach should be reported to the ICO unless you are satisfied that it is unlikely to result in a risk to the individual's rights and freedoms.

7. If a matter is to be reported to the ICO then the report needs to be made within 72 hours from being aware that a breach has occurred.

8. The SLT/DPO should consider whether they need to contact any individuals' to notify them of the breach and the action taken.

9. The SLT/DPO should record the outcome of the investigation and any action taken in the data breach log. They should include whether the matter was reported to the ICO and, if the matter was not reported to the ICO, it will need to include the reasons why.

10. Assess the procedure/issue which led to the breach and consider whether changes need to be made.

11. Inform The Trust Board regarding the data breach and resulting action taken.