The Grey Coat Hospital

Data Protection Policy

POLICY NAME:	Data Protection Policy
GOV COMMITTEE:	Personnel Committee
POLICY REVIEW TIMING:	2 Years

1. INTRODUCTION

1.1. The Grey Coat Hospital ("the Academy") collects and uses certain types of personal information about staff, pupils, parents and other individuals who come into contact with the Academy in order provide education and associated functions. The Academy 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 and securely and in accordance with the General Data Protection Regulation and other related legislation.

1.2. The GDPR applies to all computerised data and manual files if they 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 on the basis of specific criteria (so you would be able to use something like the individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different physical location.

1.3. This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, and shall be reviewed every 2 years.

2. PERSONAL DATA

- Personal data is data which relates to a living individual who can be identified:
- from this data; or
- from this data and other information which is in the possession of, or is likely to come into the possession of, the data controller.
- Examples of personal data can include, but are not limited to:
- names
- addresses
- telephone numbers
- dates of birth
- National Insurance numbers
- employee numbers
- named email addresses
- account details
- CCTV images
- photographs
- personal opinions
- internet browsing history

- static/dynamic IP addresses

Special Categories of personal data (also known as sensitive personal data) include:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- the processing of genetic data;
- biometric data for uniquely identifying an individual;
- data concerning health or data concerning an individual's sex life;
- sexual orientation;
- medical information.

Special Category information is given special protection, and additional safeguards apply if this information is to be collected and used.

2.1. Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

2.2. The Academy does not intend to seek or hold sensitive personal data about staff or students except where the Academy has been notified of the information, or it comes to the Academy's attention 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 the Academy 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).

3. THE DATA PROTECTION PRINCIPLES

3.1. The six data protection principles as laid down in the GDPR are followed at all times:

- 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;

- personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;

- personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;

- personal data shall be accurate and, where necessary, kept up to date;
- 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;
- 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.

3.2. In addition to this, the Academy is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law (as explained in more detail in paragraphs 7 and 8 below).

4. CONDITIONS FOR PROCESSING IN THE FIRST DATA PROTECTION PRINCIPLE

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

4.2. 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.

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

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

4.5. 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.

4.6. The processing is necessary for a legitimate interest of the Academy Trust or that of a third party, except where this interest is overridden by the rights and freedoms of the individual concerned

5. USE OF PERSONAL DATA BY THE ACADEMY

5.1. The Academy holds personal data on pupils, staff and other individuals such as visitors. In each case, the personal data must be treated in accordance with the data protection principles as outlined in paragraph 3.1 above.

Pupils

5.2. 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.

5.3. 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.

5.4. The Academy 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 to this.

5.5. In particular, the Academy may:

- transfer information to an 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;
- make personal data, including sensitive personal data, available to staff for planning curricular or extra-curricular activities;
- Use photographs of pupils in accordance with the photograph policy.
- Transfer limited data to a university or other educational institution for purposes of taking part in research projects, but only where consent has been provided.

5.6. Any wish to limit or object to any use of personal data should be notified to the Director of Finance and Operations in writing, which notice will be acknowledged by the Academy in writing. If, in the view of the Director of Finance and Operations the objection cannot be maintained, the individual will be given written reasons why the Academy cannot comply with their request.

Staff

5.7. The personal data held about staff will include contact details, employment history, information relating to career progression, information relating to DBS checks, photographs, information relating to payroll.

5.8. The data is used to comply with legal obligations placed on the Academy in relation to employment, and the education of children in a school environment. The Academy 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.

5.9. 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.

5.10. Any wish to limit or object to any use of personal data should be notified to the Director of Finance and Operations in writing, which notice will be acknowledged by the Academy in writing. If, in the view of the Director of Finance and Operations the objection cannot be maintained, the individual will be given written reasons why the Academy cannot comply with their request.

Other Individuals

5.11. The Academy 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.

6. SECURITY OF PERSONAL DATA

6.1. The Academy Trust will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this Policy and their duties under the GDPR. The Charity will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

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

7. DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES

7.1. The following list includes the most usual reasons that the Academy will authorise disclosure of personal data to a third party:

- To give a confidential reference relating to a current or former employee, volunteer or pupil;
- for the prevention or detection of crime;
- for the assessment of any tax or duty;
- 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);
- for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);
- for the purpose of obtaining legal advice;
- for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);
- to publish the results of public examinations or other achievements of pupils of the Academy;
- to disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips;

- to provide information to another educational establishment to which a pupil is transferring;
- to provide information to the Examination Authority as part of the examination process; and
- 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.

7.2. 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.

7.3. The Academy 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 the Academy.

7.4. All requests for the disclosure of personal data must be sent to the Director of Finance and Operations, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

8. CONFIDENTIALITY OF PUPIL CONCERNS

8.1. 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 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.

9. SUBJECT ACCESS REQUESTS

This policy has regard to the latest guidance at https://www.gov.uk/guidance/data-protection-in-schools/dealing-with-subject-access-requests-sars

Below is an extract from this guidance:

"Requesting a SAR is a child's right. A child can request access to information about themselves from any education setting that holds data about them.

A child does not have to be a certain age to make a SAR.

The Information Commissioner's Office (ICO) provides guidance on the rights of children when making SARs.

If the young person is under 13 and is making their own request, you will need to consider whether they will be able to understand your response, but this shouldn't be a barrier to supplying them with their information.

If the young person is over 13, you should treat the request the same way as if an adult made it, provided there are no issues with the child's competency.

Parents or carers can also make a SAR on behalf of a young person. If the young person is 13 or over, check whether they are happy for their personal data to be shared with their parent or carer.

When a child of any age submits a SAR, you should assess if they can understand the information they will receive in response to their request.

If you believe the child has the maturity and understanding to request and receive the information, you should respond directly to the child, regardless of their age. If a child requests a SAR themselves, this demonstrates some maturity and understanding about their right of access their personal information.

You should not respond directly to the child if you believe they:

- do not have the maturity or competence to act independently
- have a health condition that limits their understanding
- have given consent for a representative or someone with parental responsibility to act on their behalf

In these cases, contact the child and ask if they agree for their parent or carer to make the request on their behalf.

The ICO provides guidance on SARs from young people."

9.1. Anybody who makes a request to see any personal information held about them by the Academy Trust 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 1.2).

9.2. All requests should be sent to the Director of Finance and Operations within 3 working days of receipt, and must be dealt with in full without delay and at the latest within one month of receipt.

9.3. Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 12, or over 12 but with a special educational need which makes understanding their information rights more difficult), a person with parental

responsibility can make a request on their behalf. The Director of Finance and Operations must, however, be satisfied that:

9.3.1. the child or young person lacks sufficient understanding; and

9.3.2. the request made on behalf of the child or young person is in their interests.

9.4. Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances the Academy Trust must have written evidence that the individual has authorised the person to make the application and the Director of Finance and Operations must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

9.5. Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

9.6. A subject access request must be made in writing. The Academy Trust may ask for any further information reasonably required to locate the information.

9.7. An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

9.8. All files must be reviewed by the Director of Finance and Operations before any disclosure takes place. Access will not be granted before this review has taken place.

9.9. Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

10. EXEMPTIONS TO ACCESS BY DATA SUBJECTS

10.1. Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

10.2. There are other exemptions from the right of subject access. If we intend to apply any of them to a request then we will usually explain which exemption is being applied and why.

11. OTHER RIGHTS OF INDIVIDUALS

11.1. The Academy Trust has an obligation to comply with the rights of individuals under the law, and takes these rights seriously. The following section sets out how the academy will comply with the rights to:

11.1.1. object to Processing;

11.1.2. rectification;

11.1.3. erasure; and

11.1.4. data Portability.

Right to object to processing

11.2. 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 (grounds 4.5 and 4.6 above) where they do not believe that those grounds are made out.

11.3. Where such an objection is made, it must be sent to the Director of Finance and Operations within 2 working days of receipt, and the Director of Finance and Operations 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.

11.4. The Director of Finance and Operations shall be responsible for notifying the individual of the outcome of their assessment within five working days of receipt of the objection.

Right to rectification

11.5. 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 the Director of Finance and Operations 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.

11.6. 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.

11.7. 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.

Right to erasure

11.8. Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

- where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;
- where consent is withdrawn and there is no other legal basis for the processing;
- where an objection has been raised under the right to object, and found to be legitimate;

- where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);

- where there is a legal obligation on the Academy Trust to delete.

11.9. The Director of Finance and Operations 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.

Right to restrict processing

11.10. In the following circumstances, processing of an individual's personal data may be restricted:

- where the accuracy of data has been contested, during the period when the Academy is attempting to verify the accuracy of the data;

- where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;

- 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;

- where there has been an objection made under para 8.2 above, pending the outcome of any decision.

Right to portability

11.11. If an individual wants to send their personal data to another organisation they have a right to request that the Academy 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 Director of Finance and Operations within 2 working days of receipt, and the Director of Finance and Operations will review and revert as necessary.

12 . BREACH OF ANY REQUIREMENT OF THE GDPR

12.1. 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 discovered, to the Director of Finance and Operations 12.2. Once notified, the Director of Finance and Operations shall assess:

- the extent of the breach;
- the risks to the data subjects as a consequence of the breach;
- any security measures in place that will protect the information;

any measures that can be taken immediately to mitigate the risk to the individuals.

12.3. Unless the Director of Finance and Operations 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 Academy Trust, unless a delay can be justified.

12.4. The Information Commissioner shall be told:

12.4.1 details of the breach, including the volume of data at risk, and the number and categories of data subjects;
12.4.2 the contact point for any enquiries
12.4.3 the likely consequences of the breach;
12.4.4 measures proposed or already taken to address the breach

12.5. If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the Director of Finance and Operations 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.

12.6. Data subjects shall be told:

12.6.1 the nature of the breach;

12.6.2 who to contact with any questions;

12.6.3 measures taken to mitigate any risks.

12.7. The Director of Finance and Operations 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 by the board and a decision made about implementation of those recommendations.

13. CONTACT

13.1 If anyone has any concerns or questions in relation to this policy they should contact the Director of Finance and Operations