THE GREETLAND ACADEMY TRUST

Data Protection Policy

1. INTRODUCTION

This policy applies to all personal data held by The Greetland Academy Trust. **Personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

The obligations outlined in this policy apply to all those who have access to personal data, whether they are employees, governors, employees of associated organisations or temporary staff. It includes those who work from home, who must follow the same procedures as they would in an office environment.

Any individual who knowingly or recklessly processes data for purposes other than those for which it is intended or makes an unauthorised disclosure is liable to prosecution. All individuals permitted to access personal data must agree to comply with this policy.

2. POLICY STATEMENT

The Greetland Academy Trust has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

The policy adheres to ICO (2018) 'Guide to the General Data Protection Regulation (GDPR)' https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

and is implemented in conjunction with The Trust's ICT Acceptable Use Policy, Freedom of Information Act Policy and Publications Scheme.

Under the GDPR, the data protection principles set out the main responsibilities for organisations.

Article 5 of the GDPR requires that personal data shall be:-

- Fairly & lawfully processed;
- Obtained for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and kept up to date;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. ACCOUNTABILITY

The Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

The Trust will provide comprehensive, clear and transparent privacy policies.

Records of activities relating to higher risk processing will be maintained, such as the processing of activities that:

- Are not occasional.
- Could result in a risk to the rights and freedoms of individuals.
- Involve the processing of special categories of data or criminal conviction and offence data.
- Internal records of processing activities will include the following:
- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

4. DATA PROTECTION OFFICER

The DPO is Debbie Pettiford. Debbie is independent of the Trust and has been appointed via a service level agreement. Debbie will:

- inform and advise the trust about their obligations to comply with the GDPR and other data protection laws.
- monitor The Trust's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.
- has professional experience and knowledge of data protection law, particularly that in relation to schools.
- report to the Trust Board.
- operate independently and will not be dismissed or penalised for performing her task.

Sufficient resources will be provided to the DPO to enable her to meet her GDPR obligations.

5. LAWFUL BASES FOR PROCESSING DATA:

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever we process personal data:

(a) Consent: the individual has given clear consent for us to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for us 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 us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for our 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.

CONSENT

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given.

The Trust ensures that consent mechanisms meet the standards of the GDPR.

Consent can be withdrawn by the individual at any time.

Where a child is under the age of 16 **[or younger if the law provides it (up to the age of 13)]**, the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

THE RIGHT TO BE INFORMED

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

THE RIGHT TO ACCESS

Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

The academy will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the academy may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the Trust holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the Trust will ask the individual to specify the information the request is in relation to.

THE RIGHT TO RECTIFICATION

Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in question has been disclosed to third parties, the Trust will inform them of the rectification where possible.

Where appropriate, the Trust will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

THE RIGHT TO ERASURE

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

The Trust has the right to refuse a request for erasure where the personal data is being 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
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims
- Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.
- Where personal data has been made public within an online environment, the Trust will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

THE RIGHT TO RESTRICT PROCESSING

Individuals have the right to block or suppress the school's processing of personal data.

In the event that processing is restricted, the Trust will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

The Trust will restrict the processing of personal data in the following circumstances:

Where an individual contests the accuracy of the personal data, processing will be restricted until the Trust has verified the accuracy of the data

Where an individual has objected to the processing and the Trust is considering whether their legitimate grounds override those of the individual

Where processing is unlawful and the individual opposes erasure and requests restriction instead

Where the Trust no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, the Trust will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The Trust will inform individuals when a restriction on processing has been lifted.

THE RIGHT TO DATA PORTABILITY

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

The Trust will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual.

The Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, the Trust will consider whether providing the information would prejudice the rights of any other individual.

The Trust will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, the Trust will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

THE RIGHT TO OBJECT

The Trust will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.
- Where personal data is processed for the performance of a legal task or legitimate interests:
- An individual's grounds for objecting must relate to his or her particular situation.

The Trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

The Trust will stop processing personal data for direct marketing purposes as soon as an objection is received.

The Trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.
Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the Trust is not required to comply with an objection to the processing of the data.
- Where the processing activity is outlined above, but is carried out online, the Trust will offer a method for individuals to object online.

PRIVACY BY DESIGN AND PRIVACY IMPACT ASSESSMENTS

The Trust will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the Trust has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy.

A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

DATA BREACHES

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The Trust Board will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the Trust becoming aware of it.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the Trust will notify those concerned directly.

DATA SECURITY

Paper records will be managed so that access is restricted to those who need to use the information and stored in secure locations to prevent unauthorised access.

Computer systems will be designed and computer files created with adequate security levels to preserve confidentiality. Those who use the school's computer equipment will have access only to the data that is both necessary for the work they are doing and held for carrying out that work.

The Trust ensures that confidential paper records have restricted access and that digital data is password protected and regularly backed up off-site.

Visitors to areas of the academies containing sensitive information are supervised at all times.

The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

The Trust takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

The Trust is responsible for continuity and recovery measures are in place to ensure the security of protected data.

6. PUBLICATION OF INFORMATION

The Trust publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Minutes of meetings
- Annual reports
- Financial information

Classes of information specified in the publication scheme are made available quickly and easily on request.

The Trust will not publish any personal information, including photos, on its website without the permission of the affected individual.

7. CCTV AND PHOTOGRAPHY

The Trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All CCTV footage will be kept for six months for security purposes; the IT Director is responsible for keeping the records secure and allowing access.

The Trust will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

If the school wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil. Precautions, as outlined in the Acceptable Use of Digital Technologies Online (e-Safety) Policy, are taken when publishing photographs of pupils, in print, video or on the academy websites.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

DATA RETENTION

Data will not be kept for longer than is necessary.

Unrequired data will be deleted as soon as practicable.

Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Paper documents will be shredded and electronic memories deleted, once the data should no longer be retained.
DBS data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

Data provided by the DBS will never be duplicated.

Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

POLICY REVIEW

This policy will be kept under review in order to keep it in line with relevant legislation.

April 2018