DATA PROTECTION POLICY

1 INTRODUCTION

This policy provides a framework to guide Trust and academy staff and strengthen decision-making as they handle personal information resulting to individuals.

This policy is based on

- Data Protection Act 2018
- General Data Protection Regulation 2018
- Information Commissioner's Office (ICO) guidance
- Data protection: toolkit for schools, DfE 2018
- IRMS Information Management Toolkit for Schools
- The Great Academies Education Trust (GAET) Vision and Values.

2 PURPOSE AND OBJECTIVES

Purpose

This policy aims to ensure that the Trust and its academies promote and maintain high standards in the handling of personal information protecting individuals' rights to privacy.

Objectives

The objectives of this policy are to

- Support academy staff and leaders in their routine handling of personal information, including sensitive information, relating to staff, students, parents, employees and other stakeholders.
- Ensure robust procedures are in place to collect, store, share and dispose of data in line with legislation and guidance.
- Ensure procedures are in place to deal with information requests (Subject Access Requests (SARs) and Freedom of Information Requests (FOI))
- Make all staff and stakeholders aware of their responsibilities in relation to data protection legislation and school procedures.

3 GUIDING PRINCIPLES

This policy is guided by legislative duties, national guidance and the GAET Vision and Values

Key legislative duties and national guidance

- The Data Protection Act 2018 controls how personal information is used by organisations, businesses or the government.
- The General Data Protection Regulation 2018 is a regulation in EU law on data protection and privacy for all individual citizens of the EU and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data.
- The ICO guidance is independent UK authority guidance. The organisation aims to uphold information rights in the public interest and promotes openness by public bodies, and data privacy for individuals.
- The Data protection: toolkit for schools, DfE 2018 supports schools to meet the General Data Protection Regulation (GDPR). It provides advice relating to school policies and processes for data management, from collecting and handling the data through to responding quickly and appropriately to data breaches.
- The IRMS Information Management Toolkit for Schools provides detailed guidance, in one place, regarding legislative requirements for the disposal of personal information routinely held by schools.

GAET Vision and Values

Vision

"Great Academies Education Trust will be a truly outstanding, outward facing multi-academy trust supporting its academies, from their starting points, to become outstanding.

All pupils will make exceptional academic progress in all subjects and regardless of age or stage will be work and college ready."

Our academies will be places where pupils are valued as individuals, where they will have opportunities to achieve highly, lead strongly and develop into confident, responsible and successful young adults."

In implementing this policy, the Trust and its employees will work with all other relevant agencies to develop outstanding procedures to deal with personal information. By implementing the policy, data subjects' rights will be upheld and any data requests resolved as quickly as possible. In dealing well with personal information, breaches will be kept to a minimum and will be dealt with appropriately if they arise.

Values
"All individuals will embody our values
Genuine - mutually trusting, open, honest and reflective.
Respect(ful) to all.
Excellent at what they do, striving for excellence and intolerant of mediocrity.

Achievement focussed-understanding that academic excellence is the goal and high aspirations key to each child achieving their academic potential .
Together-believing that we can make the biggest difference when we work as a strong team."

In implementing this policy, the provision for handling personal information is paramount. Anyone requesting information will be treated fairly and honestly. All stakeholders will be involved, as appropriate, in genuine conversation and decision-making. The procedures to handle data requests and data breaches will always challenge mediocrity and strive for excellence. GAET staff will work together with each other, and other parties, to focus on the best possible procedures for handling personal information.

4 EQUALITY

The Great Academies Education Trust ensures that the principles of data protection are upheld to ensure data subjects' rights, regardless of any protected characteristics. We recognise the protected characteristics under the Equality Act 2010. We do not discriminate against anyone on the grounds of their age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, or sexual orientation. This is line with the Equality Act 2010 and covers both direct and indirect discrimination.

5 IMPLEMENTATION GUIDANCE

Data controller registration
The Data Protection Act 2018 requires every organisation that processes personal information to register with the Information Commissioner's Office (ICO). As an organisation that processes personal information, Great Academies Education Trust is registered as a Data Controller with the ICO. This registration includes the closed circuit television (CCTV) systems that are in use at each academy.

Data protection principles
The Data Protection Act 2018 requires that eight data protection principles be followed in the handling of personal data. These principles require that personal data must:

- be fairly and lawfully processed;
- be processed for limited purposes and not in any manner incompatible with those purposes;
- be adequate, relevant and not excessive;
- be accurate;
- not be kept longer than is necessary;
- be processed in accordance with individuals' rights;

- be kept secure; and
- not be transferred to countries outside the EAA without adequate protection.

Fair Processing / Privacy Notice:
The Trust is transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individual's data. Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.
The intention to share data relating to individuals to an organisation outside of the Trust is clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where there is a lawful basis to do so.
Any proposed change to the processing of individual's data shall first be notified to them.

Data Security:
Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.
The security arrangements of any organisation with which data is shared shall also be considered and these organisations shall provide evidence of the competence in the security of shared data.

Photographs and Video:
Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only.
Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources.
Images captured by individuals for personal or recreational use with a mobile phone, digital camera or camcorder are exempt from the DPA (e.g. parents are allowed to take photos of pupils in an academy production, subject to the permission of the Principal).

Monitoring (including CCTV)
See also Trust ICT and e-safety policy
The Academy will only monitor individual staff's ICT use when there are concerns about the individual's use of e-mail, internet, telephone or other data that the member of staff may be using inappropriately. If monitoring is used for training purposes, the individual will be made aware of this at the time.

Data Access Requests (Subject Access Requests):
All individuals whose data is held by us, has a legal right to request access to such data or information about what is held. We shall respond to such requests in line with legislation. See Appendix 1 (Process for dealing with information requests).

Data breaches

A personal data breach is “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service”.
A personal data breach may mean that someone other than the data controller has unauthorised access to personal data. But a personal data breach can also occur if there is unauthorised access within an organisation, or if a data controller’s own employee accidentally alters or deletes personal data.
If you suspect that there has been a data breach you must contact the Trust’s DPO immediately. Further information can be found in the Great Academies Education Trust Personal Data Breach Procedure (appendix 2)

Retention and disposal of data
Personal and sensitive data will be retained in line with retention periods outlined in the IRMS Information Management Toolkit for Schools 2019. The only exception to this is child protection information, which will be kept indefinitely, until such time as the Independent Enquiry on Child Sexual Abuse reaches its conclusions and publishes its recommendations.
The Trust recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk. All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services. All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.
Disposal of IT assets holding data shall be in compliance with ICO guidance.
Each academy must identify a qualified source for disposal of IT assets and collections**.**
Each academy must have documented procedures for transferring information to the next educational establishment when a pupil leaves the school. Secondary academies must have documented procedures for archiving pupil files when students leave at the end of Y11, including paper and computer-based files, to ensure personal information is not kept longer than is necessary.

6 ROLES AND RESPONSIBILITIES

The Trust
The Trust is responsible for ensuring relevant policies and procedures are in place to ensure the Trust and its academies are compliant with data protection legislation.

Data protection officer
Charlotte Treglown is the organisation's data protection officer (DPO) and is responsible for the implementation of this policy. If employees have any questions about data protection in general, this policy or their obligations under it, that cannot be answered by their Line Manager or Principal, they should direct them to Charlotte Treglown, (contactable via 0161 250 2476).

The DPO is responsible for:

- Notifying the Information Commissioner's Office (ICO) in regard to GAET and renewing the Academy's registration annually.
- Advising the Trust on its policies and procedures in relation to data protection.
- Supporting principals with academy compliance with data protection legislation.

Principals

The principal of each academy is responsible for ensuring:

- There is a nominated person in each school who liaises with the Trust's DPO for matters regarding data protection including requests for personal data
- Relevant consent for disclosure of Personal Data is obtained, including routine consent from parents and pupils for using photographs for general academy purposes.
- Data protection statements are included on forms that are used to collect personal data.
- Appropriate data protection training is provided for staff.
- Adequate systems are in place for compliance with this policy.

Nominated staff

Nominated staff shall be responsible for the appropriate processing of personal and sensitive data including

- HR data
- Finance data
- Data held on ICT systems

All staff

Everyone within the academy trust has a responsibility to ensure that they abide by the principles above in handling personal data, and that they comply with data protection legislation. Failure to observe the data protection principles within this policy may result in an employee incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal.

7 LINKS TO OTHER POLICIES

This policy should be read in conjunction with national and local guidance and the following GAET/Academy policies:

- Data Protection Act 2018
- General Data Protection Regulation 2018
- ICO guidance
- IRMS Information Management Toolkit for Schools 2016
- Trust Privacy Notices
- Trust Freedom of Information Policy
- Trust ICT and e-safety policy

8 SOURCES CONSULTED

- Data Protection Act 2018
- General Data Protection Regulation 2018
- ICO guidance
- IRMS Information Management Toolkit for Schools 2019

APPENDICES

Appendix 1

Great Academies Education Trust
Process for dealing with information requests

Each school must nominate a member of staff to liaise with the Trust's Data Protection Officer regarding information requests.
The Trust's Data Protection Officer is Charlotte Treglown.
At Insert School Name, the nominated member of staff for data protection is Insert person's name and role.

Each school must make sure staff members know how to identify a request. For example, parents might not use the term 'subject access request' but might ask to see their child's behaviour record. This is personal data and so data protection rules apply. Similarly, an individual may not say they are requesting information under the Freedom of Information Act but might ask for information about the number of lessons taught by supply teachers, or the sizes of classrooms.

Subject access request (SAR)

Individuals have the right to access the personal data and supplementary information held about them. This allows them to be aware of, and verify the lawfulness of, how the data is processed.
This right applies to everyone whose personal data the school holds, including staff, governors, volunteers, parents and pupils.

The rules: in summary
Under the General Data Protection Regulation (GDPR), in force from 25 May 2018, in most cases, you:

- Must provide the information **free of charge**
- Must comply within **1 month**
- Should provide the information in a commonly used electronic format, if the request was made electronically.

It is helpful if an individual supplies the following information to help school process their request, however, the request does not have to be made in this form.

Name	
Relationship with the school	Please select: Pupil / parent / employee / governor / volunteer Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested	*Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible.*

Process for dealing with a Subject Access Request

1. When a SAR is received, it needs to be passed immediately to the nominated person in school and the date it was received recorded.
2. On receiving a request, contact should be made with the individual by the school via phone to confirm the request was made. Then, the identity of the person making a request must be verified using 'reasonable means'
3. Generally, this means you should ask for two forms of identification, although this won't always be necessary - for example, staff, governors, pupils and many parents will be known to the school, so you could simply ask another staff member to verify their identity
4. The nominated member of staff should make contact with the Trust's Data Protection Officer to discuss the response.

5. In most cases you must provide the information within 1 month, and free of change. If the request is complex or numerous, you can comply within 3 months, but you must inform the individual of this within 1 month and explain why the extension is necessary. If a request is made during the school summer holiday Insert how you will pick up the request and how you will inform the individual that an extension to the timeframe is necessary.
6. If the request is made electronically, you should provide the information in a commonly used electronic format.
7. Once the response is agreed, it should be filed appropriately, e.g. on the pupil's school record, with copies of any attached documents, and retained in line with the retention of the relevant record.
8. A copy should also be filed with the Trust's Data Protection Officer.

'Unfounded or excessive' requests

If the request is unfounded or excessive, you can either:

- Charge a reasonable fee for you to comply, based on the administrative cost of providing the information
- Refuse to respond
- Comply within 3 months, rather than the usual deadline of 1 month - you must inform the individual of this and will explain why

Usually 'unfounded or excessive' means that the request is repetitive, or asks for further copies of the same information.

Refusing a request

When you refuse a request, you must:

- Respond to the individual within 1 month
- Explain why you are refusing the request
- Tell the individual they have the right to complain to the ICO

Freedom of Information Request (FOI)

Anyone has a right to request information from a public authority. You have two separate duties when responding to these requests:

- to tell the applicant whether you hold any information falling within the scope of their request; and
- to provide that information

For a request to be valid under the Freedom of Information Act it must be in writing, but requesters do not have to mention the Act or direct their request to a designated member of staff. Any letter or email to a public authority asking for information is a request for recorded information under the Act.

This doesn't mean you have to treat every enquiry formally as a request under the Act. It will often be most sensible and provide better customer service to deal with it as a normal customer enquiry under your usual customer service procedures, for example, if a prospective parent wants to know how your school supports children with SEND, or whether you have a space for their child.

The provisions of the Act need to come into force only if:

- you cannot provide the requested information straight away; or
- the requester makes it clear they expect a response under the Act.

Process for dealing with a Freedom of Information Request

1. When a FOI request is received, it needs to be passed immediately to the nominated person in school and the date it was received recorded.

2. The nominated member of staff should make contact with the Trust's Data Protection Officer to discuss the response and agree whether the request is simply an enquiry, or a request that must be dealt with under FOI.

3. Contact should then be made with the individual by the school to confirm the request was received, to and to inform them that the request will be dealt with as an FOI request, and to advise of the allowed response time.

4. You normally have 20 working days to respond to a request. Under the Act, most public authorities may take up to 20 working days to respond, counting the first working day after the request is received as the first day. For schools, the standard time limit is 20 school days, or 60 working days if this is shorter.

5. If the request is made electronically, you should provide the information in a commonly used electronic format.

6. Once the response is agreed, it should be filed appropriately, with copies of any attached documents, and retained in line with the retention of the relevant record.

7. A copy should also be filed with the Trust's Data Protection Officer.

Appendix 2

Great Academies Education Trust
Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must **immediately** notify the nominated person in school of the breach.

- The nominated person should **immediately** contact the Trust's DPO, Charlotte Treglown.

- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people

- The DPO will alert the headteacher and the chair of governors

- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality

- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored by the Trust's DPO.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
  - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects

- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored by the Trust's DPO.

- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the school will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The school will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The school must carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of breach of sensitive information could include:

- Details of named children being published on the school website
- Non-anonymised pupil exam results being shared with governors
- Staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen