DATA PROTECTION POLICY

1 STATEMENT OF INTENT

Great Academies Education Trust (GAET) is committed to all aspects of data protection and takes seriously its duties, and the duties of its employees, under the Data Protection Act 1998. The Data Protection Act 1998 (the DPA) aims to promote high standards in the handling of personal information protecting individuals rights to privacy. The DPA applies to anyone holding information about living individuals in electronic format and in some cases on paper. As each academy within the Trust is a holder of personal records they must also follow this act.

2 AIMS

This policy aims to set out how GAET deals with personal data, including personnel files, images captured on CCTV and data subject access requests, and employees' obligations in relation to personal data.

3 OBJECTIVES

The policy is designed to:

- provide guidance on the activities and controls in place throughout the Trust in relation to data protection
- identify key roles in the organisation in relation to data protection
- clarify the responsibilities of all staff in relation to data protection

4 IMPLEMENTATION GUIDANCE & ROLES AND RESPONSIBILITIES

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 on 0161 250 2598).

Data controller registration
The Data Protection Act 1998 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 1998 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 secure; and
- not be transferred to countries without adequate protection.

Who is covered?
The DPA covers staff, pupils, parents and any other individuals for which the Academy Trust holds personal details. 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).

Who is responsible for ensuring that the Trust complies with the DPA?
The DPO working with the company secretary is responsible for ensuring the Trust complies with the DPA and each Principal is responsible for ensuring that their academy complies with the DPA, working with the DPO to achieve the following:

- Notifying the Information Commissioner's Office (ICO) in regard to GAET and renewing the Academy's registration annually.
- Keeping the ICO up to date with changes in how GAET and the academies process data.
- Approving consent for disclosure of Personal Data, including routine consent from parents and pupils for using photographs for general academy purposes.
- Ensuring data protection statements are included on forms that are used to collect personal data.
- Acting as a central point of advice for staff on data protection matters.
- Co-ordinating requests for personal data.
- Arranging appropriate data protection training for staff.
- Keeping up to date with the latest data protection legislation and guidance.
- Ensuring adequate systems are in place for compliance with this policy.

However *everyone within the academy trust* has a responsibility to ensure that they abide by the principles listed above in handling personal data. If you are unsure about the action you are taking with regard to personal data you must check with your Manager/the Principal to ensure you are complying with the DPA.

Some of the questions you can ask yourself to ensure that the action you are taking will comply with the DPA are:

- Do I really need this information about an individual? Do I know what I'm going to use it for?
- Do the people whose information I hold know that I've got it and are they likely to understand what it will be used for? Would any of them be surprised at what I'm doing with their personal information?
- If I'm asked to pass personal information on am I sure it's okay to do so under the DPA? (check with your manager if unsure)
- Am I satisfied that the personal information I hold is secure be it on the computer or paper based?
- Is the personal data held accurate and up to date?
- Do I delete/destroy personal information (securely) as soon as I have no need for it?
- Is access to personal information limited only to those with a strict need to know? Who will have access to this information if I place it on computer file or hold on a paper record?

Ensure that any personal data that you hold is only shared with other members of academy staff or authorities who are entitled to have access to this data. If you have any queries or concerns you must raise them with your manager / the Principal immediately.

As an individual you also have a responsibility to ensure that the details held about you are accurate and kept up to date for example ensuring that the Trust is notified if you move house.

Monitoring (including CCTV)
See 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.

Employees' obligations regarding personal information
If an employee acquires any personal information in the course of his/her duties, he/she must ensure that:

- the information is accurate and up to date, insofar as it is practicable to do so;
- the use of the information is necessary for a relevant purpose and that it is not kept longer than necessary; and
- the information is secure.

In particular, an employee should ensure that he/she:

- uses password-protected and encrypted software for the transmission and receipt of emails;
- sends fax transmissions to a direct fax where possible, with a secure cover sheet;
- locks files in a secure cabinet; and
- uses a secure password when accessing emails on a mobile device (iPad, tablet, phone, etc.)

Where information is disposed of, employees should ensure that it is destroyed. This may involve the permanent removal of the information from the server, so that it does not remain in an employee's inbox or trash folder. Hard copies of information may need to be confidentially shredded. Employees should be careful to ensure that information is not disposed of in a wastepaper basket/recycle bin.

If an employee acquires any personal information in error by whatever means, he/she shall inform their Line Manager / the Principal immediately and, if it is not necessary for him/her to retain that information, arrange for it to be handled by the appropriate individual within the organisation.

Where an employee is required to disclose personal data to any other country, he/she must ensure first that there are adequate safeguards for the protection of data in the host country. For further guidance on the transfer of personal data outside the UK, please contact the Principal.

An employee must not take any personal information away from the organisation's premises (except in circumstances where he/she has obtained the prior consent of the Principal to do so).

If an employee is in any doubt about what he/she may or may not do with personal information, he/she should seek advice from their Line Manager / the Principal / the Data Protection Officer. If he/she cannot get in touch with them, he/she should not disclose the information concerned.

To assist employees with these obligations, GAET will provide some or all of the following as appropriate:

- password protected/encrypted hard disk drives
- secure network access
- password protected email
- access to encrypted email software when necessary
- ability to lock computers between use

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.

What must we do if there is a breach?

If you suspect that there has been a data breach you must contact the Trust's Governance Officer immediately. Containment and recovery is key and any delay in reporting the breach could severely jeopardize this. Serious breaches should be reported to the Information Commissioners Officer and in these circumstances a timeline of events will be requested to effectively demonstrate that the breach has been dealt with a timely and appropriate manner.

Consequences of non-compliance
All employees are under an obligation to ensure that they have regard to the eight data protection principles (see above) when accessing, using or disposing of personal information. 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. For example, if an employee accesses another employee's employment records without the requisite authority, the organisation will treat this as gross misconduct and instigate its disciplinary procedures. Such gross misconduct will also constitute a criminal offence.

Review of procedures and training
GAET will provide training to all employees on data protection on induction and on a regular basis thereafter.

If there are any queries concerning this policy or you require further assistance or training please contact the Principal or your manager.

Complaints
Complaints and enquiries about this policy or the application of this policy should be made to the Principal of the relevant academy in the first instance.

5 MONITORING, EVALUATION AND REVIEW

This policy will be reviewed and amended by a small group comprising of officers and the Principal from each Academy. The recommendations of this group will be submitted to the Academy Trust Board and each Board of Governors for consideration and, where applicable, approval.

The Academy Trust will review this policy at least every two years and assess its implementation and effectiveness. The policy will be promoted and implemented throughout the Academy Trust.

Date: July 2017
Date for next review: July 2019