



# Data Protection Policy

Policy reviewed by Academy Transformation Trust on	October 2017
--	--------------

This policy links to:	Located:
<ul style="list-style-type: none"><li>• Freedom of Information Policy</li><li>• Freedom of Information Publication Scheme</li><li>• Safeguarding Policy</li><li>• HR Policies and Procedures</li><li>• E-Safety Policy</li><li>• Social Media Policy</li><li>• CCTV Policy</li></ul>	

Review Date – June 2018



## **Our Mission**

To provide the very best education for all pupils and the highest level of support for our staff to ensure every child leaves our academies with everything they need to reach their full potential.

We promise to do everything we can to give children the very best education that gives them the best opportunity to succeed in life. All of our academies have it in them to be outstanding and achieving this comes down to our commitment to our pupils, staff and academies.

## **Our commitment**

We are committed to taking positive action in the light of the Equality Act 2010 with regard to the needs of people with protected characteristics. These are age, disability, pregnancy and maternity, religion and belief, race, sex, sexual orientation, gender reassignment and marriage and civil partnership.

We will continue to make reasonable adjustments to avoid anyone with a protected characteristic being placed at a disadvantage.

## Information relating to the Data Protection Policy

The Data Controller is ATT and Great Heath Academy

The Trust Data Protection Officer is Ian Cleland

The academy Data Protection Officer is Steven Vincent

The Trust will:

- Carry out regular checks to monitor and assess the processing of personal data and to ensure ATT's/the academy's notification to the Information Commissioner is updated to take account of any changes in processing of personal data.

The Trust/academy will:

- Ensure that there is a single point of contact with the overall responsibility for Data Protection (the Data Protection Officer)
- Provide awareness for all members of staff who handle personal information
- Provide clear lines of report and supervision for compliance with Data Protection
- Carry out regular checks to monitor and assess the processing of personal data and to ensure ATT's/the academy's notification to the Information Commissioner is updated to take account of any changes in processing of personal data.



## Introduction

Under the multi-academy trust arrangements, ATT is responsible for activities of its academies even though some functions may have been delegated to local Principals or Academy Committees, ultimate responsibility lies with the MAT. ATT is the legal entity responsible for the processing of personal data by our academies. ATT is the data controller (jointly) and is responsible for the processing and is entity subject to DPA registration obligations.

Our academies are shown as trading names on the ATT entry with the Information Commissioners' Office. It is important that parents and children see who is responsible for processing of personal data.

ATT and our academies need to collect personal information about people we work with, in order to carry out our core business of supporting learning and to provide our services. Such people include pupils, parents, Governors, employees (past, present and prospective), suppliers and other business contacts.

In addition, ATT may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. on a computer screen or on paper) this personal information must be dealt with properly to ensure compliance with the Data Protection Act 1998.

The personal information held by ATT is extremely important to ensure the success of ATT and in order to maintain the confidence of ATT pupils, parents, employees and stakeholders (identified above). ATT must ensure it treats personal information lawfully and correctly.

ATT fully supports and complies with the eight principles of the Data Protection Act 1998.

## Contents

1	Adherence to the Eight Principles of the Data Protection Act 1998	6
2	CCTV	8
3	ATT's Commitment	8
4	Monitoring	8
5	Complaints	8
6	Definitions	9
	Appendix 1 – Suggested wording for the Privacy Notice for pupil data to be displayed in individual academy websites – Primary academies	10
	Appendix 2 - Suggested wording for the Privacy Notice for pupil data to be displayed in individual academy websites – Secondary academies	12
	Appendix 3 - Suggested wording for the Privacy Notice for pupil data to be displayed in individual academy websites	14

## 1 Adherence to the Eight Principles of the Data Protection Act 1998

### 1.1 Personal data shall be processed fairly and lawfully.

*Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the Data Controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.*

### 1.2 Personal data shall be obtained only for one or more specified lawful purposes and shall not be further processed in any manner incompatible with the purpose of those purposes.

*Data obtained for specified purposes must only be used for those purposes identified.*

### 1.3 Personal data shall be adequate, relevant and not excessive.

*Information which is not strictly necessary for the purpose of which it is obtained should not be collected. If data is given or obtained which is excessive to the purpose it should be immediately deleted or destroyed.*

### 1.4 Personal data shall be accurate and where necessary, kept up to date.

*Data which is kept for a long time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate. It is the responsibility of individuals to ensure that data held by ATT is accurate and up to date. Individuals should notify ATT of any changes in circumstances to enable personal records to be updated accordingly. It is the responsibility of ATT to ensure any notification regarding change of circumstances is noted and acted upon.*

### 1.5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for the purpose or purposes.

*ATT discourages the retention of personal data for longer than is required. Considerable amounts of data are collected on current staff and pupils. Once a member of staff or pupil has left ATT, it will not be necessary to retain all the information held on them. Some data will be kept for longer periods than others.*

*Staff and pupil information will be retained for the time periods set out by the Information and Records Management Society within their information management toolkit for schools. This reflects statutory requirements and recommendations for best practice.*

[https://c.ymcdn.com/sites/irms.site-ym.com/resource/collection/8BCEF755-0353-4F66-9877-CCDA4BFEEAC4/2016\\_IRMS\\_Toolkit\\_for\\_schools\\_v5\\_Master.pdf](https://c.ymcdn.com/sites/irms.site-ym.com/resource/collection/8BCEF755-0353-4F66-9877-CCDA4BFEEAC4/2016_IRMS_Toolkit_for_schools_v5_Master.pdf)

### 1.6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

*Data subjects have the following rights regarding data processing and the data that is recorded about them:*

- *A right of access to a copy of the information comprised in their personal data*
- *A right to object to processing that is likely to cause or is causing damage or distress*
- *A right to prevent processing for direct marketing*

- *A right to object to decisions being taken by automated means*
- *A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed*
- *A right to claim compensation for damages caused by a breach of this Act.*

**1.7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data.**

*All staff are responsible for ensuring that any personal data (on others) which they hold is kept securely and that it is not disclosed to any unauthorised third party.*

*All personal data should be accessible only to those who need to use it. You should form a judgement based upon the sensitivity and value of the information in questions, but always consider keeping personal data, examples might be data should be kept:*

- *In a lockable room with controlled access*
- *In a locked drawer or filing cabinet*
- *Password protected if in electronic format*
- *Securely electronically (e.g. secure back-ups).*

*Care should be taken to ensure that electronic device screens are not visible except to authorised staff and that passwords are kept confidential. Electronic devices should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised persons. Personal information should not be kept on external hard drives or USB drives.*

*Care must be taken to ensure that appropriate security measures are in place for the deletion and disposal of personal data. Manual records should be shredded or disposed of as confidential waste. Hard drives or redundant electronic devices should be wiped clean before disposal.*

*This policy also applies to staff who process personal data off-site. Off-site processing presents potentially greater risk of loss, theft or damage to personal data. Staff should take particular care when processing data at home or in other locations.*

**1.8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.**

*Data must not be transferred outside of the European Economic Area (EEA) – the EU Member states together with Iceland, Liechtenstein and Norway without the explicit consent of the individual. Members of ATT should be particularly aware of this when publishing information on the internet, which can be accessed from anywhere around the globe. Transfer includes placing data on a website (or file sharing site) that can be accessed from outside of the EEA. When sensitive data is passed electronically (such as by email) between ATT and a third party it shall always be in a secure (encrypted) manner.*

## 2 CCTV

- 2.1 Images of people are covered by the Data Protection Act 1998 and so is information about people which is derived from images (e.g. vehicle registration numbers etc.) Ensure all procedures are followed when installing CCTV and any captured information should be processed under the principles of the Data Protection Act 1998 and this Policy. Further information about the Data Protection Code of Practice in relation to CCTV use is issued by the ICO.

<https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf>

## 3 ATT's Commitment

- 3.1 ATT will implement the requirements of the Data Protection Act 1998 and Data Retention Regulations 2009 and any subsequent amendments or regulations.

- 3.2 ATT will ensure that:

- The Trust or academy Data Controller will have overall responsibility for the implementation of the processes and procedures to ensure the requirements of the Data Protection Act 1998 are fulfilled
- All staff are aware of their responsibilities under the Data Protection Act 1998
- All staff are aware of their responsibilities under the Data Retention Regulations 2009
- Staff are trained and supported to adhere to the Data Protection Act 1998 including dealing with requests under Subject Access Requests
- ATT must ensure that the principles of this policy are followed for remote and/or home working, and the technology is in place to support this.

## 4 Monitoring

- 4.1 ATT will maintain a register of all requests made under the Data Protection Act 1998 that do not fall within the remit of the Data Protection Registration and the action taken for each request.
- 4.2 ATT will review this policy and associated procedures to ensure it remains up to date or when new legislation or regulations are released.

## 5 Complaints

- 5.1 If you are not satisfied with the response you receive from us or we have not been able to resolve your complaint and you feel that formal complaint needs to be made, then this should be addressed to the Information Commissioners' Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.



## 6 Definitions

**Data** means information which:

- (a) Is being processed by means of equipment operating automatically in response to instructions given for that purpose
- (b) Is recorded with the intention that it should be processed by means of such equipment
- (c) Is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system
- (d) Does not fall within paragraphs (a), (b) or (c) but forms part of an accessible record as defined by section 68
- (e) Is recorded information held by a public authority and does not fall within paragraphs (a) to (d).

**Personal data** means data which relate to a living individual who can be identified. This includes expressions of opinion about the individual.

**Sensitive data** means personal data consisting of information that could be used in a discriminatory way (e.g. racial or ethnic data) and is likely to be of a private nature. It should be treated with greater care than other personal information.

**Data subject** means an individual who is subject to personal data.

**Data Controller** means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

**Data processor**, in relation to personal data, means any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller.

**Relevant filing system** means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

## Appendix 1 – Suggested wording for the Privacy Notice for pupil data to be displayed in individual academy websites – Primary academies

### Data Protection Act 1998: How we use pupil information

We collect and hold personal information relating to our pupils and may also receive information about them from their previous school, Local Authority and/or Department for Education (DfE). We use personal data to:

- Support our pupils' learning
- Monitor and report on their progress
- Provide appropriate pastoral care
- Assess the quality of our services.

This information will include their contact details, national curriculum assessment results, attendance information, any exclusion information, where they go after they leave us and personal characteristics (e.g. ethnic group, any special educational needs and relevant medical information). *For pupils enrolling for post-14 qualifications, the Learning Records Service will give us the Unique Learner Number (ULN) and may also give us details about your learning or qualifications.*

We will not give information about our pupils to anyone without your consent unless the law and our policies allows us to do so. If you want to receive a copy of the information about your son/daughter that we hold, please contact the Principal, Mr. S. Vincent on 01638 713430 or via [office@greatheathacademy.attrust.org.uk](mailto:office@greatheathacademy.attrust.org.uk). *We are required, by law, to pass some information about our pupils to the Department for Education (DfE). This information will, in turn, then be made available for use by the Local Authority.*

DfE may also share pupil level personal data that we supply to them, with third parties. This will only take place where legislation allows it to do so and it is in compliance with the Data Protection Act 1998.

Decisions on whether DfE releases this personal data to third parties are subject to a robust approval process and are based on a detailed assessment of who is requesting the data, the purpose for which it is required, the level of sensitivity of data requested and the arrangements in place to store and handle this data. To be granted access to pupil level data, requestors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of data. For more information on how this sharing process works, please visit <https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract>

For information on which third party organisations (and for which project) pupil level data has been provided to, please visit <https://www.gov.uk/government/publications/national-pupil-database-requests-received>

If you need more information about how ATT, our Local Authority and/or DfE collect and use your information please visit:

- [ATT Website](#)
- Our Local Authority at <https://www.suffolk.gov.uk/about/privacy-and-data-protection>
- [DfE Website](#)

## Appendix 2 - Suggested wording for the Privacy Notice for pupil data to be displayed in individual academy websites – Secondary academies

### Data Protection Act 1998: How we use pupil information

We collect and hold personal information relating to our pupils and may also receive information about them from their previous school, Local Authority and/or Department for Education (DfE). We use personal data to:

- Support our pupils' learning
- Monitor and report on their progress
- Provide appropriate pastoral care
- Assess the quality of our services.

This information will include their contact details, national curriculum assessment results, attendance information, any exclusion information, where they go after they leave us and personal characteristics (e.g. ethnic group, any special educational needs and relevant medical information). *For pupils enrolling for post-14 qualifications, the Learning Records Service will give us the Unique Learner Number (ULN) and may also give us details about your learning or qualifications.*

#### [For institutions with students aged 13+]

*Once our pupils reach the age of 13, the law requires us to pass on certain information to [Insert Name of Local Authority or provider of Youth Support Services in your area] who have responsibilities in relation to the education and training of 13-19 year olds. We may also share certain personal data relating to children aged 16 years and older with post-16 education and training providers in order to secure appropriate services for them. A parent/guardian can request that only their child's name, address and date of birth be passed to [Insert Name of Local Authority or provider of Youth Support Services in your area] by informing [Insert Name of academy Administrator]. The right is transferred to the child once he/she reaches the age of 16. For more information about services for young people, please go to our Local Authority website [Insert Link].*

*[Careers guidance – academies that pass young people's information to careers guidance services or the National Careers Service may wish to set out details here]*

We will not give information about our pupils to anyone without your consent unless the law and our policies allows us to do so. If you want to receive a copy of the information about your son/daughter that we hold, please contact [Insert Name and Contact Details of your academy Administrator]. *We are required, by law, to pass some information about our pupils to the Department for Education (DfE). This information will, in turn, then be made available for use by the Local Authority.*

DfE may also share pupil level personal data that we supply to them, with third parties. This will only take place where legislation allows it to do so and it is in compliance with the Data Protection Act 1998.

Decisions on whether DfE releases this personal data to third parties are subject to a robust approval process and are based on a detailed assessment of who is requesting the data, the

purpose for which it is required, the level of sensitivity of data requested and the arrangements in place to store and handle this data. To be granted access to pupil level data, requestors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of data. For more information on how this sharing process works, please visit <https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract>

For information on which third party organisations (and for which project) pupil level data has been provided to, please visit <https://www.gov.uk/government/publications/national-pupil-database-requests-received>

If you need more information about how ATT, our Local Authority and/or DfE collect and use your information please visit:

- [ATT Website](#)
- Our Local Authority at [\[Insert relevant LA website link\]](#)
- [DfE Website](#)

## Appendix 3 - Suggested wording for the Privacy Notice for pupil data to be displayed in individual academy websites

### Data Protection Act 1998: How we use your information

We process personal data relating to those we employ to work at, or otherwise engage to work at ATT. This is for employment purposes to assist in the running of ATT and/or to enable individuals to be paid for. The collection of this information will benefit both national and local users by:

- Improving the management of workforce data across the sector
- Enabling development of a comprehensive picture of the workforce and how it is deployed
- Informing the development of recruitment and retention policies
- Allowing better financial modelling and planning
- Enabling ethnicity and disability monitoring
- Supporting the work of the School Teachers' Review Body.

The personal data includes identifiers such as names and National Insurance Numbers and characteristics such as ethnic group, employment contracts and remuneration details, qualifications and absence information.

We will not share information about you with third parties without your consent unless the law allows us to. We are required, by law, to pass on some of this personal data to:

- Our Local Authority
- Department for Education (DfE)
- Office for National Statistics.

If you require more information about how we use and/or DfE store and use your personal data please visit:

- Our website <http://www.greatheathacademy.attrust.org.uk/>
- [DfE Website](#)

If you want to see a copy of information about your child that we hold, please contact the principal, Mr. S Vincent – 01638713430.