AURORA ACADEMIES TRUST	
Policy Title:	Data Protection Policy
Policy Reference:	AAT - Data Protection Policy Nov 2016
Function:	For Information and Guidance/Statutory
Audience:	Prospective parents, Trustees, Governors, Regional Directors, Executive Headteachers, Heads, Teachers, Support Staff, as necessary
Ownership/ Implementation:	The Trustees/LAB Governing Body (as required) have overall responsibility for ensuring that this policy is implemented
Version:	001
Approved by Trust Board:	November 2016
Next Date for Review:	November 2018

DATA PROTECTION POLICY

1. POLICY STATEMENT AND OBJECTIVES

1.1 The objectives of this Data Protection Policy are to ensure that Aurora Academies Trust (the "Trust") and its trustees, employees and governors on the Local Governing Bodies are informed about, and comply with, their obligations under the Data Protection Act 1998 ("the Act"). References to "school" in this policy include any academy or school within the Trust.

1.2 Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information about a number of different groups of people and we recognise the need to treat it in an appropriate and lawful manner.

1.3 The types of information that we may be required to handle include details of current, past and prospective employees and pupils, parents, trustees, governors, suppliers and other individuals that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Act and other regulations. The Act imposes restrictions on how we may use that information.

1.4 This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action and serious breaches may result in dismissal. Breach of the Act may expose the Trust to enforcement action by the Information Commissioner or fines. Furthermore, certain breaches of the Act can give rise to personal criminal liability for the Trust's employees. At the very least, a breach of the Act could damage our reputation and have serious consequences for the Trust.

1.5 The Trust has notified the Information Commissioner that it processes personal information, and is on the register of data controllers, registration number Z3349370. It is the responsibility of the Trust Financial Director to confirm or amend the entry when the entry becomes inaccurate, incomplete or requires renewal each year.

1.6 This policy does not form part of any employee's contract of employment. It may be amended at any time.

2. STATUS OF THE POLICY

2.1 This policy has been approved by the Trust Board. It sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

2.2 The Trust Financial Director is responsible for ensuring compliance with the Act and with this policy. The Trust Data Protection Compliance Manager is David Baron, Financial Director, who can be contacted on 07443 430331 and the Headteacher/Head of School will be the Compliance Manager for the individual academies/schools within the Trust. Any questions or concerns about the operation of this policy should be referred in the first instance to the relevant Data Protection Compliance Manager.

2.3 If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with the relevant Data Protection Compliance Manager.

3. DEFINITION OF TERMS

3.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a school report) and can include telephone numbers, photographs and CCTV images.

3.4 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used in our business.

3.5 **Data users** include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

3.6 **Data processors** include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on our behalf.

3.7 **Parent has the meaning given in the Education Act 1996 and includes any person having parental responsibility or care of a child.**

3.8 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.9 **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

4. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

a) Processed fairly and lawfully.

b) Processed for limited purposes and in an appropriate way.

c) Adequate, relevant and not excessive for the purpose.

d) Accurate.

e) Not kept longer than necessary for the purpose.

f) Processed in line with data subjects' rights.

g) Secure.

h) Not transferred to people or organisations situated in countries without adequate protection.

5. FAIR AND LAWFUL PROCESSING

5.1 The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case the Trust), who the data controller's representative is (in this case the Data Protection Compliance Manager), the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

5.2 For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the

data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

6. PROCESSING FOR LIMITED PURPOSES

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected, or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

7. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

7.1 Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

7.2 In order to ensure compliance with this principle, the Trust will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data. Decisions on data to be deleted must come from the Data Protection Compliance Manager, after taking appropriate guidance.

8. ACCURATE DATA

8.1 Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

8.2 If a data subject informs the Trust (or a school within the Trust) of a change of circumstances their computer record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects periodically so they can check its accuracy and make any amendments.

8.3 Where a data subject challenges the accuracy of their data, the Trust will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the relevant Local Governing Body, or the Trust Board where appropriate, for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged'

marker will remain and all disclosures of the affected information will contain both versions of the information.

8.4 Notwithstanding paragraph 8.3, a data subject continues to have rights under the Act and may refer a complaint to the Information Commissioner's Office regardless of whether the procedure set out in paragraph 8.3 has been followed.

9. TIMELY PROCESSING

9.1 Personal data should not be kept longer than is necessary for the purpose for which it is held. This means that data should be destroyed or erased from our systems when it is no longer required.

9.2 It is the duty of the Data Protection Compliance Manager, after taking appropriate guidance for legal considerations, to ensure that obsolete data are properly erased. The Trust has a retention schedule for all data.

10. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

Data must be processed in line with data subjects' rights. Data subjects have a right to:

a) Request access to any data held about them by a data controller.

b) Prevent the processing of their data for direct-marketing purposes.

c) Ask to have inaccurate data amended.

d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

11. DATA SECURITY[1]

11.1 The Trust has taken steps to ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

11.2 The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

11.3 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

a) **Confidentiality** means that only people who are authorised to use the data can access it.

b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the school computer system instead of individual employee devices.

11.4 Security procedures include:[2]

Physical Security

Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the computer rooms. Disks, tapes and printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied. Any stranger seen in entry-controlled areas should be reported.

Computer Security

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (i.e. security copies are taken) regularly. Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC/laptop/handheld device when it is left unattended.

Procedural Security

In order to be given authorised access to the school ICT equipment, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded and/or subject to confidential waste disposal.

Paper documents should be shredded and CD-ROMs/USB sticks or other remote data storage devices should be given to the IT Technician to be physically destroyed when they are no longer required.

[2] Paragraph 11.4 is an example of some of the security procedures that schools may put in place. This section will need tailoring according to the practice of each school as it must reflect what each school does to keep data secure. If there are no data security practices in place at your school then you must address this and consider whether training is necessary.

12. DEALING WITH SUBJECT ACCESS REQUESTS

12.1 The Act extends to all data subjects a right of access to their own personal data. A formal request from a data subject for information that we hold about them must be made in writing. A fee may be[3] payable by the data subject for provision of this information. Any member of staff who receives a written request should forward it to their line manager or the Data Protection Compliance Manager **IMMEDIATELY** as there are statutory time limits for responding (currently 40 calendar days)[4].

12.2 In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place.

Where a request for subject access is received from a pupil, the Trust's policy is that:

a) Requests from pupils who are considered mature enough to understand their rights under the Act will be processed as any subject access request as outlined below and the copy will be given directly to the pupil. The Information Commissioner's guidance is that it may be reasonable to adopt a presumption that by the age of 12 a child has sufficient maturity to understand their rights and to make an access request themselves if they wish. In every case it will be for the school to assess on behalf of the Trust whether the child is capable of understanding their rights under the Act and the implications of their actions, and so decide whether the parent needs to make the request on the child's behalf. A parent would normally be expected to make a request on a child's behalf if the child is younger than 12 years of age.

b) Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.

c) Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent unless the school considers the child to be mature enough to understand their rights under the Act, in which case the school shall ask the child for their consent to disclosure of the personal data (subject to any enactment which permits the School to disclose the personal data to a parent without the child's consent). Subject to paragraph 14, if consent is not given to disclosure, the school shall not disclose the personal data if to do so would breach any of the eight data protection principles.

[3] The £10 fee is dependent on the amount of administrative effort required to collate the requested information.

[4] The timescale of 40 calendar days cannot be extended and will continue regardless of whether the school is closed for holidays (unlike the Freedom of Information Act 2000). It is therefore advisable that subject access requests are dealt with as soon as possible.

All subject access requests

Following receipt of a subject access request, and provided that there is sufficient information to process the request, an entry will be made in the school's Subject Access log book, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date for supplying the information (not more than 40 days from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

13. PROVIDING INFORMATION OVER THE TELEPHONE

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by the Trust. In particular they should:

a) Check the caller's identity to make sure that information is only given to a person who is entitled to it.

b) Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

c) Refer to their line manager or the Data Protection Compliance Manager for assistance in difficult situations. No-one should be bullied into disclosing personal information.

14. AUTHORISED DISCLOSURES

14.1 The Trust will, in general, only disclose data about individuals with their consent or unless the law requires or allows us to. There are circumstances under which the Trust may need to disclose data without explicit consent for that occasion including (but not limited to) the following:

a) Pupil data disclosed to authorised recipients related to education and administration necessary for the Trust to perform its statutory duties and obligations.

b) Pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare.

c) Pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school.

d) Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.

e) Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the Trust.

f) Disclosures required as a result of a court order or pursuant to an act of Parliament.

g) Disclosures to the Police where the Trust is satisfied that the information is needed to prevent or detect a crime or to catch and prosecute a suspect.

14.2 Only authorised and trained staff are allowed to make external disclosures of personal data in accordance with the Act. Data used within the schools by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the Trust who needs to know the information in order to do their work.

15. CCTV

The Trust schools use CCTV in locations around each academy site including (but not limited to) the following: [LIST PARTS OF THE SITE WHERE CCTV IS LOCATED]. [This is to:

a) protect the school buildings and their assets;
b) increase personal safety and reduce the fear of crime;
c) support the Police in a bid to deter and detect crime;
d) assist in identifying, apprehending and prosecuting offenders;
e) protect members of the public and private property; and
f) assist in managing the schools.

Images from the CCTV are stored for [period] and then deleted. [Please refer to the Trust's CCTV policy for more information.]

16. POLICY REVIEW

16.1 It is the responsibility of the Trust Board to facilitate the review of this policy on a regular basis. Recommendations for any amendments should be reported to the Data Protection Compliance Manager.

16.2 We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

17. ENQUIRIES

Further information about the Trust's Data Protection Policy is available from the Trust Financial Director.

General information about the Act can be obtained from the Information Commissioner's Office: www.ico.gov.uk.

Useful References

The Data Protection Act (1998)

http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1

The Information Commissioner's Office

HTTP://WWW.ICO.GOV.UK/