The Auriga Academy Trust
DATA PROTECTION POLICY AND PRIVACY NOTICE

Key Document Links:

Key Contacts:
Chief Executive Officer: John Kipps (jkipps@clarendon.richmond.sch.uk)
Trust HR Manager & Data Protection Officer: Annushka St Paul (astpaul@strathmore.richmond.sch.uk)
Finance Director: Susie Connor (sconnor@strathmore.richmond.sch.uk)

AURIGA Academy Trust Document Control System	
Name of document	Data Protection Policy and Privacy Notice
Status	Approved
Date Approved	01/09/2018
Approver	
Owner	MAT Finance
Author	Data Protection Officer
Anticipated Review date	23/05/2019
Location	

Contents Page

1. Aims

Our Trust aims to ensure that all personal data collected about staff, pupils, parents/ carers, Governors, Trustees, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Scope

Personal information is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

The Trust collects a large amount of personal data every year including:

- Staff records
- Pupil records
- Names, addresses and other contact details of those requesting to visit a School
- Examination and assessment marks
- References
- Fee collection

As well as the many different types of research data used by the Trust. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

3. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

In addition, this policy complies with our funding agreement and articles of association.

4. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership

	• Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

5. The data controller

Our Trust processes personal data relating to parents, pupils, staff, Trustees, Governors, visitors and others, and therefore is a data controller.

The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

6. Roles and responsibilities

This policy applies to all staff employed by our Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

6.1 Board of Trustees

The Board of Trustees has overall responsibility for ensuring that our Trust complies with all relevant data protection obligations.

6.2 Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Board of Trustees and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Annushka St Paul and is contactable via astpaul@strathmore.richmond.sch.uk.

6.3 Executive Headteachers

The Executive Headteachers act as the representative of the data controller on a day-to-day basis.

6.4 All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Trust of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed

- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

7. Data protection principles

The GDPR is based on data protection principles that our Trust must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the Trust aims to comply with these principles.

8. Collecting personal data

8.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

1. The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract
2. The data needs to be processed so that the Trust can **comply with a legal obligation**
3. The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
4. The data needs to be processed so that the Trust, as a public authority, can perform a task **in the public interest,** and carry out its official functions
5. The data needs to be processed for the **legitimate interests** of the Trust or a third party (provided the individual's rights and freedoms are not overridden)
6. The individual (or their parent/ carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13* (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

**Due to the nature of the schools within the Trust, a pupil's ability to provide consent will be assessed on a case-by-case basis.*

8.2 Limitation, Minimisation and Accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This

will be done in accordance with the Trust's record retention schedule (appendix 2).

9. Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/ carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

10. Subject Access Requests and Other Rights of Individuals

10.1 Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

10.2 Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from parents or carers of pupils below the age of 12 at our Trust may be granted without the express permission of the pupil.

Due to the nature of the schools within the Trust, pupils aged 12 and above will always be judged on a case-by-case basis on their ability to understand their rights and the implications of a subject access request. Therefore, there may be some subject access requests from parents or carers of pupils at our Trust that may not be granted without the express permission of the pupil.

10.3 Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the pupil is at risk of abuse, where the disclosure of that information would not be in the pupil's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the pupil

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

10.4 Other Data Protection Rights of the Individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 8), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

11. Parental Requests to See the Educational Record

Parents, or those with parental responsibility, are able to have free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

12. CCTV

We use CCTV in various locations around the different school sites to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the relevant school office.

13. Photographs and Videos

As part of school activities, we may take photographs and record images of individuals within our Trust.

We will obtain written consent from parents/ carers, or pupils aged 18* and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to the parent/ carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, prospectus, newspapers, campaigns
- Online on the school or Trust website social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

**Due to the nature of the schools within the Trust, a pupil's ability to provide consent will be assessed on a case-by-case basis.*

14. Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 7)
- Completing privacy impact assessments where a school or the Trust's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our Trust and DPO and all information we are required to share about how we use and process their

personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/ display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the relevant school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils, Trustees or Governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 9)

16. Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal Data Breaches

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on a school or Trust website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school or Trust laptop containing non-encrypted personal data about pupils or staff

18. Training

All staff, Trustees and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust's processes make it necessary.

19. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent

and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our Trust's practice. Otherwise, or from then on, this policy will be reviewed every year and shared with the full Board of Trustees and School Governing Boards.

20. Links with Other Policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Code of conduct (for staff)
- Child protection policy

Personal Data Breach Procedure

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

1. On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
2. 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

3. The DPO will alert the relevant Executive Headteacher and Chair of Governors
4. 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.
5. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
6. 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 or financial loss), including through:

    a. Loss of control over their data
    b. Discrimination
    c. Identify theft or fraud
    d. Financial loss
    e. Unauthorised reversal of pseudonymisation (for example, key-coding)
    f. Damage to reputation
    g. Loss of confidentiality
    h. 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.

7. 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 on a computer system within the Trust
8. 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. A description of the nature of the personal data breach including, where possible:
        i. The categories and approximate number of individuals concerned
        ii. The categories and approximate number of personal data records concerned
    b. The name and contact details of the DPO
    c. A description of the likely consequences of the personal data breach
    d. 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

9. 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
10. 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:

a. The name and contact details of the DPO
b. A description of the likely consequences of the personal data breach
c. 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

11. 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

12. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

a. Facts and cause
b. Effects
c. 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 a computer system within the Trust

13. The DPO and the relevant Executive 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

Below are examples of data breaches:

- Sensitive information being disclosed via email (including safeguarding records)
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- Non-anonymised pupil exam results or staff pay information being shared with governors
- Details of pupil premium interventions for named children being published on the school website
- The school's cashless payment provider being hacked and parents' financial details stolen

Below there are listed examples of the actions we will take 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.

– 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 DPO 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 DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police or insurers
– The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with any requests to delete or remove the information
– The DPO will 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
– The DPO will notify the relevant individuals that their financial details have been stolen or hacked and provide them with a description of the likely consequences of the breach. The individuals will also be given information on the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects.

Retention Schedule					
1. Pupil's Education Record					
Ref Nº	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437		
	Primary			Retain whilst the child remains at the school	The file should follow the pupil when he/she leaves primary education. This will include: • To another primary school • To a secondary school • To a pupil referral unit • If the pupil dies whilst school the file should be returned to the Local Authority to be retained for the statutory retention period. If the pupil transfers to home schooling or leaves the country the file should be returned to the Local Authority to be retained for the statutory retention period.

	Secondary		Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	SECURE DISPOSAL
1.2	Examination Results – Pupil Copies	Yes			
	Public			This information should be added to the pupil file	All uncollected certificates should be returned to the examination board.
	Internal			This information should be added to the pupil file	
1.3	Child Protection information held on a pupil	Yes	"Keeping children safe in education Statutory guidance for schools and colleges September 2016"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children"	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.	SECURE DISPOSAL these records MUST be shredded
1.4	Child protection information held in separate files	Yes	"Keeping children safe in education Statutory guidance for schools and colleges September 2016"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children"	DOB of the child + 25 years then review This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record.	SECURE DISPOSAL these records MUST be shredded

2. Attendance

Ref N°	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the End of the Administrative Life of the Record
2.1	Attendance Registers	Yes	Academy attendance: Departmental advice for	Every entry in the attendance register must be preserved for a	SECURE DISPOSAL

			maintained schools, academies, independent schools and local authorities October 2014	period of three years after the date on which the entry was made.	
2.2	Correspondence relating to authorised absence	Yes	Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL
3. Special Educational Needs					
Ref Nº	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	NOTE: This retention period is the minimum retention period that any pupil file should be kept.
3.2	Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	Date of birth of the pupil + 25 years [This is retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
3.3	Advice and information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Date of birth of the pupil + 25 years [This is retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
3.4	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Date of birth of the pupil + 25 years [This is retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
4. Statistics and Management Information					
Ref Nº	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
4.1	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL

4.2	Examination Results (Schools Copy)	Yes		Current year + 6 years	SECURE DISPOSAL
	SATS records	Yes			
	Results			The SATS results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years. The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year + 6 years to allow suitable comparison	SECURE DISPOSAL
	Examination Papers			The examination papers should be kept until any appeals/ validation process is complete	SECURE DISPOSAL
4.3	Published Admission Number (PAN) Reports	Yes		Current year + 6 years	SECURE DISPOSAL
4.4	Value Added and Contextual Data	Yes		Current year + 6 years	SECURE DISPOSAL
4.5	Self-Evaluation Forms	Yes		Current year + 6 years	SECURE DISPOSAL
5. Implementation of Curriculum					
Ref N°	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
5.1	Schemes of Work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further
5.2	Timetable	No		Current year + 1 year	
5.3	Class Record Books	No		Current year + 1 year	

5.4	Mark Books	No		Current year + 1 year	retention period or SECURE DISPOSAL
5.5	Record of homework set	No		Current year + 1 year	
5.6	Pupils' Work	No		Where possible pupils' work should be returned to the pupil at the end of the academic year if this is not the school's policy then current year + 1 year	SECURE DISPOSAL
6. Board of Trustees and Governing Board					
Ref Nº	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
6.1	Agendas for Board of Trustees or Governing Body Meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff		One copy should be retained with the master set of minutes. All other copies can be disposed of.	SECURE DISPOSAL
6.2	Minutes of Board of Trustees or Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff			
	Principal Set (signed)			PERMANENT	
	Inspection Copies			Date of meeting + 3 years	If these minutes contain any sensitive, personal information they must be shredded.

6.3	Reports presented to the Board of Trustees or Governing Body	There may be data protection issues if the report deals with confidential issues relating to staff.		Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports then the reports should be kept permanently.	SECURE DISPOSAL or retain with the signed set of the minutes.
6.4	Meeting papers relating to the annual parents' meeting held under section 33 of the Education Act 2002	No	Education Act 2002, Section 33	Date of the meeting + a minimum of 6 years	SECURE DISPOSAL
6.5	Instruments of Government including Articles of Association	No		PERMANENT	These should be retained at the Trust Head Office
6.6	Trusts and Endowments managed by the Governing Body	No		PERMANENT	These should be retained at the Trust Head Office
6.7	Action plans created and administered by the Governing Body	No		Life of the action plan + 3 years	SECURE DISPOSAL
6.8	Policy documents created and administered by the Governing Body	No		Life of the policy + 3 years	SECURE DISPOSAL
6.9	Records relating to complaints dealt with by the Governing Body	Yes		Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes	SECURE DISPOSAL
6.10	Annual Reports created under the requirements of the Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002	No	Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002 SI 2002 No 1171	Date of report + 10 years	SECURE DISPOSAL

6.11	Proposals concerning the change of status of a maintained school including Specialist Status Schools and Academies	No		Date proposal accepted or declined + 3 years	SECURE DISPOSAL
7. Executive Headteacher and Senior Management Team					
Ref Nº	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
7.1	Log books of activity in the Academy maintained by the Executive Headteachers	There may be data protection issues if the log book refers to individual pupils or members of staff		Date of last entry in the book + a minimum of 6 years then review	These could be of permanent historical value and should be stored securely
7.2	Minutes of Senior Management Team meetings and meetings of other internal administrative bodies	There may be data protection issues if the minutes refers to individual pupils or members of staff		Date of the meeting + 3 years then review	SECURE DISPOSAL
7.3	Reports created by an Executive Headteacher, Senior Leadership Team or the Management Team	There may be data protection issues if the report refers to individual pupils or members of staff		Date of the report + a minimum of 3 years then review	SECURE DISPOSAL
7.4	Records created by an Executive Headteacher, Senior Leadership Team and other members of staff with administrative responsibilities	There may be data protection issues if the records refer to individual pupils or members of staff		Current academic year + 6 years then review	SECURE DISPOSAL

7.5	Correspondence created by an Executive Headteacher, Senior Leadership Team and other members of staff with administrative	There may be data protection issues if the correspondence refers to individual pupils or members of staff		Date of correspondence + 3 years then review	SECURE DISPOSAL
7.6	Professional Development Plans	Yes		Life of the plan + 6 years	SECURE DISPOSAL
7.7	Academy and School Development Plans	No		Life of the plan + 3 years	SECURE DISPOSAL
8. Admissions Process					
Ref N°	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
8.1	All records relating to the creation and implementation of the Trust or School Admissions' Policy	No	Academy Admissions Code and School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Life of the policy + 3 years then review	SECURE DISPOSAL
8.2	Admissions – if the admission is successful	Yes	Academy Admissions Code and School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December	Date of admission + 1 year	SECURE DISPOSAL

			2014		
8.3	Admissions – if the appeal is unsuccessful	Yes	Academy Admissions Code and School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Resolution of case + 1 year	SECURE DISPOSAL
8.4	Register of Admissions	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the admission register must be preserved for a period of 3 years after the date on which the entry was made.	Schools may wish to consider keeping the admission register permanently as often schools receive enquiries from past pupils to confirm the dates they attended the school.
8.5	Admissions – Secondary Schools – Casual	Yes		Current year + 1 year	SECURE DISPOSAL
8.6	Proofs of address supplied by parents as part of the admissions process	Yes	Academy Admissions Code and School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Current year + 1 year	SECURE DISPOSAL

8.7	Supplementary Information form including additional information such as religion, medical conditions etc.	Yes			
	For successful admissions			This information should be added to the pupil file	SECURE DISPOSAL
	For unsuccessful admissions			Until appeals process completed	SECURE DISPOSAL
9. Operational Administration					
Ref Nº	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
9.1	General file series	No		Current year + 5 years then REVIEW	SECURE DISPOSAL
9.2	Records relating to the creation and publication of the Trust or School brochure or prospectus	No		Current year + 3 years	STANDARD DISPOSAL
9.3	Records relating to the creation and distribution of circulars to staff, parents or pupils	No		Current year + 1 year	STANDARD DISPOSAL
9.4	Newsletters and other items with a short operational use	No		Current year + 1 year	STANDARD DISPOSAL
9.5	Visitors' Books and Signing in Sheets	Yes		Current year + 6 years then REVIEW	SECURE DISPOSAL
9.16	Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	No		Current year + 6 years then REVIEW	SECURE DISPOSAL

10. Recruitment					
Ref N°	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
10.1	All records leading up to the appointment of a new Executive Headteacher or Headteacher	Yes		Date of appointment + 6 years	SECURE DISPOSAL
10.2	All records leading up to the appointment of a new member of staff– unsuccessful candidates	Yes		Date of appointment of successful candidate + 6 months	SECURE DISPOSAL
10.3	All records leading up to the appointment of a new member of staff–successful candidate	Yes		All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months	SECURE DISPOSAL
10.4	Pre-employment vetting information- DBS Checks	No	DBS Update Service Employer Guide June 2014: Keeping children safe in education. September 2016	The Trust does not have to keep copies of DBS certificates. If the Trust does so the copy must NOT be retained for more than 6 months	
10.5	Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure	Yes		Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff's personal file	
10.6	Pre-employment vetting information – Evidence	Yes	An employer's guide to right to work checks (Home	These documents should be added to the Staff Personal File	

	proving the right to work in the United Kingdom		Office May 2015)	(see below)	
11. Operational Staff Management					
Ref Nº	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
11.1	Staff Personal File	Yes	Limitation Act 1980 (Section 2)	Termination of Employment + 6 years	SECURE DISPOSAL
11.2	Timesheets	Yes		Current year + 6 years	SECURE DISPOSAL
11.3	Annual appraisal/ assessment records	Yes		Current year + 5 years	SECURE DISPOSAL
12. Management of Disciplinary and Grievance Processes					
Ref Nº	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
12.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded	Yes	"Keeping children safe in education Statutory guidance for schools and colleges September 2016"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children"	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	SECURE DISPOSAL
12.1	Disciplinary Proceedings	Yes			
	Verbal warning			Date of warning + 6 months	SECURE DISPOSAL (If warnings are placed on personal files then
	Written warning – level 1			Date of warning + 6 months	
	Written warning – level 2			Date of warning + 12 months	

	Final Written warning			Date of warning + 18 months	they must be weeded from the file)
	Unfounded case			If the incident is child protection related then see above otherwise dispose of at the conclusion of the case	SECURE DISPOSAL
13. Health and Safety					
Ref N°	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
13.1	Health and Safety Policy Statements	No		Life of policy + 3 years	SECURE DISPOSAL
13.2	Health and Safety Risk Assessments	No		Life of risk assessment + 3 years	SECURE DISPOSAL
13.3	Records relating to accident/ injury at work	Yes		Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied	SECURE DISPOSAL
13.4	Accident Reporting	Yes	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
	Adults			Date of the incident + 6 years	SECURE DISPOSAL
	Children			DOB of the child + 25 years	SECURE DISPOSAL
13.5	Control of Substances Hazardous to Health (COSHH)	No	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677 Regulation 11; Records kept under	Current year + 40 years	SECURE DISPOSAL

			the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18 (2)		
13.6	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	Last action + 40 years	SECURE DISPOSAL
13.7	Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	No		Last action + 50 years	SECURE DISPOSAL
13.8	Fire Precautions log books	No		Current year + 6 years	SECURE DISPOSAL
14. Educational Visits outside the Classroom					
Ref Nº	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
14.1	Records created by schools or the Trust to obtain approval to run an Educational Visit outside the Classroom – Primary	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 14 years	SECURE DISPOSAL
14.2	Records created by schools or the Trust to obtain approval to run an Educational Visit outside the Classroom – Secondary	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal	Date of visit + 10 years	SECURE DISPOSAL

			Framework and Employer Systems" and Section 4 - "Good Practice".		
14.3	Parental consent forms for school trips where there has been no major incident	Yes		Conclusion of the trip	Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low.
14.4	Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980 (Section 2)	DOB of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils	
15. Payroll and Pensions					
Ref N°	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
15.1	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year + 3 years	SECURE DISPOSAL
15.2	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL
16. Risk Management and Insurance					
Ref N°	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**

16.1	Employer's Liability Insurance Certificate	No		Closure of the Trust + 40 years	SECURE DISPOSAL
17. Asset Management					
Ref Nº	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
17.1	Inventories of furniture and equipment	No		Current year + 6 years	SECURE DISPOSAL
17.2	Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL
18. Accounts and Statements including Budget Management					
Ref Nº	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
18.1	Annual Accounts	No		Current year + 6 years	STANDARD DISPOSAL
18.2	Loans and grants managed by the Trust	No		Date of last payment on the loan + 12 years then REVIEW	SECURE DISPOSAL
18.3	Student Grant applications	Yes		Current year + 3 years	SECURE DISPOSAL
18.4	All records relating to the creation and management of budgets including the Annual Budget statement and background papers	No		Life of the budget + 3 years	SECURE DISPOSAL
18.5	Invoices, receipts, order books and requisitions, delivery notices	No		Current financial year + 6 years	SECURE DISPOSAL
18.6	Records relating to the collection and banking of monies	No		Current financial year + 6 years	SECURE DISPOSAL
18.7	Records relating to the	No		Current financial year + 6 years	SECURE DISPOSAL

	identification and collection of debt				
19. Contract Management					
Ref Nº	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
19.1	All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
19.2	All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL
19.3	Records relating to the monitoring of contracts	No		Current year + 2 years	SECURE DISPOSAL
20. School Fund					
Ref Nº	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
20.1	School Fund - Cheque books	No		Current year + 6 years	SECURE DISPOSAL
20.2	School Fund - Paying in books	No		Current year + 6 years	SECURE DISPOSAL
20.3	School Fund – Ledger	No		Current year + 6 years	SECURE DISPOSAL
20.4	School Fund – Invoices	No		Current year + 6 years	SECURE DISPOSAL
20.5	School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL
20.6	School Fund - Bank statements	No		Current year + 6 years	SECURE DISPOSAL
20.7	School Fund – Journey Books	No		Current year + 6 years	SECURE DISPOSAL
21. School Meals Management					
Ref Nº	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
21.1	Free School Meals Registers	Yes		Current year + 6 years	SECURE DISPOSAL

21.2	School Meals Registers	Yes		Current year + 3 years	SECURE DISPOSAL
21.3	School Meals Summary Sheets	No		Current year + 3 years	SECURE DISPOSAL
22. Property Management					
Ref Nº	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
22.1	Title deeds of properties belonging to the Trust	No		PERMANENT These should follow the property unless the property has been registered with the Land Registry	
22.2	Plans of property belong to the Trust	No		These should be retained whilst the building belongs to the Trust and should be passed onto any new owners if the building is leased or sold.	
22.3	Leases of property leased by or to the Trust	No		Expiry of lease + 6 years	SECURE DISPOSAL
22.4	Records relating to the letting of Trust premises	No		Current financial year + 6 years	SECURE DISPOSAL
23. Maintenance					
Ref Nº	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
23.1	All records relating to the maintenance of the Schools carried out by contractors	No		Current year + 6 years	SECURE DISPOSAL
23.2	All records relating to the maintenance of the School carried out by	No		Current year + 6 years	SECURE DISPOSAL

	Trust employees including maintenance log books				
24. Family Liaison Officers, Family Support Workers and School-Based Family Workers					
Ref Nº	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
24.1	Day Books	Yes		Current year + 2 years then review	
24.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes		Whilst child is attending school and then destroy	
24.3	Referral forms	Yes		While the referral is current	
24.4	Contact data sheets	Yes		Current year then review, if contact is no longer active then destroy	
24.5	Contact database entries	Yes		Current year then review, if contact is no longer active then destroy	
24.6	Group Registers	Yes		Current year + 2 years	
25. Local Authority					
Ref Nº	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
25.1	Secondary Transfer Sheets (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL
25.2	Attendance Returns	Yes		Current year + 1 year	SECURE DISPOSAL
25.3	School Census Returns	No		Current year + 5 years	SECURE DISPOSAL

25.3	Circulars and other information sent from the Local Authority	No		Operational use	SECURE DISPOSAL
26. Central Government					
Ref Nº	**Basic File Description**	**Data Protection Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the End of the Administrative Life of the Record**
26.1	OFSTED reports and papers	No		Life of the report then REVIEW	SECURE DISPOSAL
26.2	Returns made to central government	No		Current year + 6 years	SECURE DISPOSAL
26.3	Circulars and other information sent from central government	No		Operational use	SECURE DISPOSAL