

Horizons Specialist Academy Trust

Records Management Policy

Adopted by the Finance & General Purposes Committee : 9 July 2019
Date of next review: Summer term 2020
Responsible Officer: Data Protection Officer

Contents:

Statement of intent

1. Legal framework
2. Responsibilities
3. Management of pupil records
4. Retention of pupil records and other pupil-related information
5. Retention of staff records
6. Retention of senior leadership and management records
7. Retention of health and safety records
8. Retention of financial records
9. Retention of other school records
10. Storing and protecting information
11. Accessing information
12. Digital continuity statement
13. Information audit
14. Disposal of data
15. Monitoring and review

Statement of intent

Horizons Specialist Academy Trust ("The Trust") is committed to maintaining the confidentiality of its information and ensuring that all records within the Trust are only accessible by the appropriate individuals. In line with the requirements of the General Data Protection Regulation (GDPR), the Trust also has a responsibility to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were intended.

This policy has been created to outline how records are stored, accessed, monitored, retained and disposed of, in order to meet the statutory requirements.

This document complies with the requirements set out in the GDPR and Data Protection Act 2018.

1. Legal framework

- 1.1. This policy has due regard to legislation including, but not limited to, the following:
 - General Data Protection Regulation (2018)
 - Freedom of Information Act 2000
 - Limitation Act 1980 (as amended by the Limitation Amendment Act 1980)
 - Data Protection Act 2018
- 1.2. This policy also has due regard to the following guidance:
 - Information Records Management Society 'Information Management Toolkit for Schools' 2016
 - DfE (2018) 'Data Protection tool kit for schools'
 - DfE (2018) 'Careers guidance and access for education and training'
- 1.3. This policy will be implemented in accordance with the following Trust policies and procedures:
 - Data Protection Policy
 - Freedom of Information Policy
 - Information Security Policy

2. Responsibilities

- 2.1. The Trust as a whole has a responsibility for maintaining its records and record-keeping systems in line with statutory requirements.
- 2.2. The Data Protection Officer (DPO) is responsible for the management of records at Horizons Specialist Academy Trust.
- 2.3. The DPO is responsible for promoting compliance with this policy and reviewing the policy on an annual basis.
- 2.4. The DPO is responsible for ensuring that all records are stored securely, in accordance with the retention periods outlined in this policy, and are disposed of correctly.
- 2.5. All staff members are responsible for ensuring that any records for which they are responsible for are accurate, maintained securely and disposed of correctly, in line with the provisions of this policy.

3. Management of pupil records

- 3.1. Pupil records are specific documents that are used throughout a pupil's time in the education system – they are passed to each school that a pupil attends and

includes all personal information relating to them, e.g. date of birth, home address, as well as their progress and achievement.

3.2. The following information is stored on the front of a pupil record, and will be easily accessible:

- Legal name, preferred name, gender and date of birth
- Unique pupil number
- Note of the date when the file was opened
- Note of the date when the file was closed, if appropriate
- Ethnic origin, religion and first language (if not English)
- Emergency contact details, the name of the pupil's doctor's practice and contact information
- Any allergies, dietary requirements or other medical conditions that are important to be aware of
- Names of parents/carers, including their home address(es), telephone number(s) and any other contact information
- Admission number, the date of admission and the date of leaving, where appropriate
- Any other agency involvement, e.g. speech and language therapist
- Previous school information
- Identification if Child Protection/Child In Need

3.3. The following information is stored in a pupil record, and will be easily accessible:

- Admissions form
- Fair processing notice – only the most recent notice will be included
- Full year written report to parents
- End of year achievement report
- Notes relating to accidents involving the pupil
- Any information about an education and healthcare (EHC) plan and support offered in relation to the EHC plan
- Any information relating to exclusions
- Any correspondence with parents or external agencies relating to major issues, e.g. mental health, holiday requests, absence notes
- All information received from primary/previous school

3.4. The following information is subject to shorter retention periods and, therefore, will be stored separately in a personal file for the pupil:

- Parental and, where appropriate, pupil consent forms for residential visits, photographs and videos, etc.
 - Correspondence with parents about minor issues, e.g. behaviour
- 3.5. Hard copies of disclosures and reports relating to child protection/Child In Need /Early Help are stored in a separate pupil file stored in a securely locked filing cabinet in the Designated Safeguarding Officer's or Principal's office (CP/CIN) or in the Parent Support Advisor's Office (Early Help) – a note indicating this is marked on the pupil's file.

The following information will be stored at the front of the child protection/child in need/Early Help files:

- Name of Child
- DOB
- RAISE ID
- UPN NO
- School
- Entry date to school
- Date of CIN/CP
- Date discharged from CP/CIN

The following information will be stored in the CP/CIN files:

- Copy of CPOMS chronology and meeting chronology sheet
- Key contact sheet recording:
 1. Name of Child
 2. DOB
 3. UPN
 4. Name of School
 5. Current Year group
 6. Current Address
 7. Name and contact details of parents/carers with parental responsibility
 8. Name of anyone child is not allowed contact with
 9. Name and contact details of current social worker
 10. Name contact details of any other named professional

11. Names and DOBs of siblings and the Schools they attend

- Current Child Protection Plan/Child In Need Plan/Early Help Assessment
 - Initial Child Protection Report/Review Child Protection Report/Core Group minutes/Planning Meeting Minutes/TAC/TAF minutes. (Copy of official minutes and HSAT DSL minutes)
 - Cause for concern reports/Children's Hub (First Contact) response letter/Strategy minutes (Copy of official minutes and HSAT DSL minutes)
 - Pupil Risk Assessments
 - School Reports
 - Any other reports/letters relevant to Safeguarding
 - Receipt of acceptance (case transfer receipt)
- 3.6. Hard copies of complaints made by parents or pupils are stored in a file in the Principal's office – a note indicating this is marked on the pupil's file.
- 3.7. Actual copies of accident and incident information are stored separately on the Trust's management information system and held in line with the retention periods outlined in this policy – a note indicating this is marked on the pupil's file. An additional copy may be placed in the pupil's file in the event of a major accident or incident.
- 3.8. CPOMS – Any data stored electronically via CPOMS is transferred to the pupil's next school (if relevant). Data stored via CPOMS will be subject to the same retention schedules as hard copies.
- 3.9. The Trust will ensure that no pupil records are altered or amended before transferring them to the next school that the pupil will attend.
- 3.10. The only exception to the above is if any records placed on the pupil's file have a shorter retention period and may need to be removed. In such cases, pastoral lead, will remove these records.
- 3.11. Electronic records relating to a pupil's record will also be transferred to the pupils' next school. Section 10 of this policy outlines how electronic records will be transferred.
- 3.12. [Primary schools only] The Trust will not keep any copies of information stored within a pupil's record, unless there is ongoing legal action at the time during which the pupil leaves the academy. The responsibility for these records will then transfer to the next school that the pupil attends.
- 3.13. [Secondary schools and sixth form colleges only] If any pupil attends the academy until statutory school leaving age, the pupil's records will be kept until the pupil reaches the age of 25 years.
- 3.14. The Trust will, wherever possible, avoid sending a pupil record by post. Where a pupil record must be sent by post, it will be sent by registered post, with an

accompanying list of the files included. The school it is sent to is required to sign a copy of the list to indicate that they have received the files and return this to the Trust.

4. Retention of pupil records and other pupil-related information

- 4.1. The table below outlines the Trust's retention periods for individual pupil records and the action that will be taken after the retention period, in line with any requirements.
- 4.2. Electronic copies of any information and files will be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Admissions		
Register of admissions	Whilst the pupil remains at the school plus one year	Information is reviewed and the register may be kept permanently
[Secondary schools only] Secondary school admissions	Whilst the pupil remains at the school plus one year	Securely disposed of
Proof of address (supplied as part of the admissions process)	Whilst the pupil remains at the school plus one year	Securely disposed of
Supplementary information submitted, including religious and medical information etc (where the admission was successful)	Whilst the pupil remains at the school plus one year	Securely disposed of
Supplementary information submitted, including religious and medical information etc. (where the admission was not successful)	Until the appeals process has been completed	Securely disposed of
Pupils' educational records		
[Primary schools only] Pupils' educational records	Whilst the pupil remains at the school	Transferred to the next destination – if this is an independent school, home-schooling or outside of the UK, the file will be kept by the LA and retained for the statutory period
[Secondary schools only] Pupils' educational records	25 years after the pupil's date of birth	Securely disposed of

Type of file	Retention period	Action taken after retention period ends
Public examination results	<p>Added to the pupil's record and transferred to next school</p> <p>Copies with pupils' names are held whilst the pupil is at school, plus five years</p> <p>Copies with pupils' names removed are held for 25 years after the pupil's date of birth</p>	Returned to the examination board
Internal examination results	<p>Added to the pupil's record and transferred to next school</p> <p>Copies with pupils' names are held whilst the pupil is at school, plus five years</p> <p>Copies with pupils' names removed are held for 25 years after the pupil's date of birth</p>	Securely disposed of
Behaviour records	<p>Added to the pupil's record and transferred to the next school</p> <p>Copies are held whilst the pupil is at school, plus one year</p>	Securely disposed of
Exclusion records	<p>Added to the pupil's record and transferred to the next school</p> <p>Copies are held whilst the pupil is at school, plus one year</p>	Securely disposed of
Historic child protection information held on a pupil's record	Stored in a sealed envelope for 25 years after the pupil's date of birth	Securely disposed of – shredded
Child protection/Child In Need/Early Help records held in a separate file	25 years after the pupil's date of birth	Securely disposed of – shredded

Type of file	Retention period	Action taken after retention period ends
Education, training or employment destinations data	Whilst the pupil is at the school, plus three years or from the end of KS4, whichever is earliest	Securely disposed of
Attendance		
Attendance registers	Last date of entry onto the register, plus three years	Securely disposed of
Letters authorising absence	Current academic year, plus two years	Securely disposed of
Medical		
Permission slips	For the duration of the period that medication is given, plus one year	Securely disposed of
Medical conditions – ongoing management	Added to the pupil's record and transferred to the next school Copies held whilst the pupil is at school, plus one year	Securely disposed of
Medical incidents that have a behavioural or safeguarding influence	Added to the pupil's record and transferred to the next school Copies held whilst the pupil is at school, plus 25 years	Securely disposed of
SEND		
SEND files, reviews and individual education plans	25 years after the pupil's date of birth (as stated on the pupil's record)	Information is reviewed and the file may be kept for longer than necessary if it is required for the Trust to defend themselves in a 'failure to provide sufficient education' case
Statement of SEN maintained under section 324 of the Education Act 1996 or an EHC plan maintained under section 37 of the Children and Families Act 2014 (and any amendments to the statement or plan)	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
Information and advice provided to parents regarding SEND	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold

Type of file	Retention period	Action taken after retention period ends
Accessibility strategy	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
Curriculum management		
SATs results	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of
Examination papers	Until the appeals/validation process has been completed	Securely disposed of
Published Admission Number (PAN) reports	Current academic year, plus six years	Securely disposed of
Valued added and contextual data	Current academic year, plus six years	Securely disposed of
Self-evaluation forms	Current academic year, plus six years	Securely disposed of
Pupils' work	Returned to pupils at the end of the academic year, or retained for the current academic year, plus one year	Securely disposed of
Extra-curricular activities		
Parental consent forms for school trips where no major incident occurred	Until the conclusion of the trip	Securely disposed of
Field file – information taken on school trips	Until the conclusion of the trip Where a minor incident occurs, field files are added to the core systems as appropriate	Securely disposed of
Financial information relating to school trips	Whilst the pupil remains at school, plus one year	Securely disposed of

Type of file	Retention period	Action taken after retention period ends
Parental consent forms for school trips where a major incident occurred	25 years after the pupil's date of birth on the pupil's record (permission slips of all pupils on the trip will also be held to show that the rules had been followed for all pupils)	Securely disposed of
Parent Support Advisers		
Reports for outside agencies	Duration of the pupil's time at school	Securely disposed of
Parent Support Referral forms	Whilst the referral is current	Securely disposed of
Electronic Data base of case files	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
Catering and free school meal management		
Meal administration	Whilst the pupil is at school, plus one year	Securely disposed of
Meal eligibility	Whilst the pupil is at school, plus five years	Securely disposed of

5. Retention of staff records

- 5.1. The table below outlines the Trust's retention period for staff records and the action that will be taken after the retention period, in line with any requirements.
- 5.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Operational		
Staff members' personal file	Termination of employment, plus six years	Securely disposed of
Timesheets	Current academic year, plus six years	Securely disposed of

Annual appraisal and assessment records	Current academic year, plus five years	Securely disposed of
Recruitment		
Records relating to the appointment of a new Principal	Date of appointment, plus six years	Securely disposed of
Records relating to the appointment of new members of staff (unsuccessful candidates)	Date of appointment of successful candidate, plus six months	Securely disposed of
Records relating to the appointment of new members of staff (successful candidates)	Relevant information added to the member of staff's personal file and other information retained for six months	Securely disposed of
DBS Enhanced results snapshot	Added to the member of staff's personal file	Securely disposed of
DBS certificates	After information has been documented on Single Central Record	Securely disposed of
Proof of identify as part of the enhanced DBS check	After identity has been proven	Reviewed and a note kept of what was seen and what has been checked – if it is necessary to keep a copy this will be placed on the staff member's personal file, if not, securely disposed of
Evidence of right to work in the UK	Added to staff personal file or, if kept separately, termination of employment, plus no longer than two years	Securely disposed of
Disciplinary and grievance procedures		
Child protection allegations, including where the allegation is unproven	Added to staff personal file, and until the individual's normal retirement age, or 10 years from the date of the allegation – whichever is longer If allegations are malicious, they are removed from personal files	Reviewed and securely disposed of – shredded

Informal management guidance	Placed in staff's personal file indefinitely	Securely disposed of
Written warning	Date of warning, plus 12 months. A valid record will be kept in staff's personal file	Securely disposed of
Final warning	Date of warning, plus 18 months. A valid record will be kept in staff's personal file	Securely disposed of
Records relating to unproven incidents	Conclusion of the case, unless the incident is child protection related and is disposed of as <u>above</u>	Securely disposed of

6. Retention of senior leadership and management records

- 6.1. The table below outlines the Trust's retention periods for senior leadership and management records, and the action that will be taken after the retention period, in line with any requirements.

Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Governing board		
Agendas for governing board meetings	One copy alongside the original set of minutes – all others disposed of without retention	Securely disposed of
Original, signed copies of the minutes of governing board meetings	Permanent	If unable to store, these will be provided to the county archives service
Inspection copies of the minutes of governing board meetings	Date of meeting, plus three years	Shredded if they contain any sensitive and personal information
Instruments of government, including articles of association	Permanent	If unable to store, these will be provided to the county archives service
Trusts and endowments managed by the governing board	Permanent	Retained in the school whilst it remains open, then provided to the county archives service when the school closes

Action plans created and administered by the governing board	Duration of the action plan, plus three years	Securely disposed of
Policy documents created and administered by the governing board	Duration of the policy, plus three years	Securely disposed of
Records relating to complaints dealt with by the governing board	Date of the resolution of the complaint, plus a minimum of six years	Reviewed for further retention in case of contentious disputes, then securely disposed of
Proposals concerning changing the status of an academy	Date proposal accepted or declined, plus three years	Securely disposed of
CEO, Executive Principal, Principals and senior leadership teams (SLTs)		
Log books of activity in the academies maintained by the Principals	Date of last entry, plus a minimum of six years	Reviewed and offered to the county archives service if appropriate
Minutes of Executive leadership team, SLT meetings and the meetings of other internal administrative bodies	Date of the meeting, plus three years	Reviewed and securely disposed of
Reports created by the CEO, Executive Principal, Principals or SLTs	Date of the report, plus a minimum of three years	Reviewed and securely disposed of
Records created by the CEO, Executive Principal, Principals, SLTs, and other members of staff with administrative responsibilities	Current academic year, plus six years	Reviewed and securely disposed of
Correspondence created by the CEO, Executive Principal, Principals, SLTs, and other members of staff with administrative responsibilities	Date of correspondence, plus three years	Reviewed and securely disposed of
Professional development plan	Duration of the plan, plus six years	Securely disposed of
Academy Improvement plan	Duration of the plan, plus three years	Securely disposed of
Trust's Strategic Plan	Duration of plan, plus three years	Securely disposed of

7. Retention of health and safety records

- 7.1. The table below outlines the Trust's retention periods for health and safety records, and the action that will be taken after the retention period, in line with any requirements.
- 7.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Health and safety		
Health and safety policy statements	Duration of policy, plus three years	Securely disposed of
Health and safety risk assessments	Duration of risk assessment, plus three years	Securely disposed of
Records relating to accidents and injuries at work	Date of incident, plus 12 years. In the case of serious accidents, a retention period of 15 years is applied	Securely disposed of
Accident reporting – adults	Date of the incident, plus six years	Securely disposed of
Accident reporting – pupils	25 years after the pupil's date of birth, on the pupil's record	Securely disposed of
Control of substances hazardous to health	Current academic year, plus 40 years	Securely disposed of
Information relating to areas where employees and persons are likely to come into contact with asbestos	Date of last action, plus 40 years	Securely disposed of
Information relating to areas where employees and persons are likely to come into contact with radiation	Date of last action, plus 50 years	Securely disposed of
Fire precautions log books	Current academic year, plus six years	Securely disposed of

8. Retention of financial records

- 8.1. The table below outlines the Trust's retention periods for financial records and the action that will be taken after the retention period, in line with any requirements.

8.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Payroll pensions		
Maternity pay records	Current academic year, plus three years	Securely disposed of
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Current academic year, plus six years	Securely disposed of
Risk management and insurance		
Employer's liability insurance certificate	Closure of the school, plus 40 years	Securely disposed of
Asset management		
Inventories of furniture and equipment	Current academic year, plus six years	Securely disposed of
Burglary, theft and vandalism report forms	Current academic year, plus six years	Securely disposed of
Accounts and statements including budget management		
Annual accounts	Current academic year, plus six years	Disposed of against common standards
Loans and grants managed by the school	Date of last payment, plus 12 years	Information is reviewed then securely disposed of
All records relating to the creation and management of budgets	Duration of the budget, plus three years	Securely disposed of
Invoices, receipts, order books, requisitions and delivery notices	Current financial year, plus six years	Securely disposed of
Records relating to the collection and banking of monies	Current financial year, plus six years	Securely disposed of
Records relating to the identification and collection of debt	Current financial year, plus six years	Securely disposed of
Contract management		
All records relating to the management of contracts under seal	Last payment on the contract, plus 12 years	Securely disposed of

All records relating to the management of contracts under signature	Last payment on the contract, plus six years	Securely disposed of
All records relating to the monitoring of contracts	Current academic year, plus two years	Securely disposed of
School fund		
Cheque books, paying in books, ledgers, invoices, receipts, bank statements and journey books	Current academic year, plus six years	Securely disposed of
School meals		
Free school meals registers	Current academic year, plus six years	Securely disposed of
School meals registers	Current academic year, plus three years	Securely disposed of
School meals summary sheets	Current academic year, plus three years	Securely disposed of

9. Retention of other school records

- 9.1. The table below outlines the Trust's retention periods for any other records held by the Trust, and the action that will be taken after the retention period, in line with any requirements.
- 9.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Property management		
Title deeds of properties belonging to the Trust	Permanent	Transferred to new owners if the building is leased or sold
Plans of property belonging to the Trust	For as long as the building belongs to the school	Transferred to new owners if the building is leased or sold
Leases of property leased by or to the Trust	Expiry of lease, plus six years	Securely disposed of
Records relating to the letting of Trust premises	Current financial year, plus six years	Securely disposed of
Maintenance		
All records relating to the maintenance of the academies carried out by contractors	Current academic year, plus six years	Securely disposed of

All records relating to the maintenance of the academies carried out by Trust employees	Current academic year, plus six years	Securely disposed of
Operational administration		
General file series	Current academic year, plus five years	Reviewed and securely disposed of
Records relating to the creation and publication of the Trust/academy brochures	Current academic year, plus three years	Disposed of against common standards
Records relating to the creation and distribution of circulars to staff, parents or pupils	Current academic year, plus one year	Disposed of against common standards
Newsletters and other items with short operational use	Current academic year plus one year	Disposed of against common standards
Visitors' books and signing-in sheets	Current academic year, plus one year	Reviewed then securely disposed of
Records relating to the creation and management of parent-teacher associations and/or old pupil associations	Current academic year, plus six years	Reviewed then securely disposed of

10. Storing and protecting information

- 10.1. The ICT Manager will ensure back-up of information is conducted on a weekly basis to ensure that all data can still be accessed in the event of a security breach, e.g. a virus, and prevent any loss or theft of data.
- 10.2. Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access.
- 10.3. Confidential paper records are not left unattended or in clear view when held in a location with general access.
- 10.4. Digital data is coded, encrypted or password-protected when being sent off site.
- 10.5. Memory sticks are not used to hold personal information.
- 10.6. All electronic devices are password-protected to protect the information on the device in case of theft.
- 10.7. Where possible, the Trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- 10.8. All members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

- 10.9. Emails containing sensitive or confidential information are password-protected to ensure that only the recipient is able to access the information. The password will be shared with the recipient separately.
- 10.10. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- 10.11. When sending confidential information by fax, members of staff always check that the recipient is correct before sending.
- 10.12. Where personal information that could be considered private or confidential is taken off the premises, to fulfil the purpose of the data in line with the GDPR, either in an electronic or paper format, staff take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the premises accepts full responsibility for the security of the data.
- 10.13. Before sharing data, staff always ensure that:
- They have consent from data subjects to share it.
 - Adequate security is in place to protect it.
 - The data recipient has been outlined in a privacy notice.
- 10.14. All staff members will implement a 'clear desk policy' to avoid unauthorised access to physical records containing sensitive or personal information. All confidential information will be stored in a securely locked filing cabinet, drawer or safe with restricted access.
- 10.15. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas containing sensitive information are supervised at all times.
- 10.16. The physical security of the Trust's buildings and storage systems, and access to them, is reviewed termly by the Premises & Facilities Manager. If an increased risk in vandalism, burglary or theft is identified, this will be reported to the Principal and extra measures to secure data storage will be put in place.
- 10.17. The Trust takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.
- 10.18. The IT Manager is responsible for continuity and recovery measures are in place to ensure the security of protected data.
- 10.19. Any damage to or theft of data will be managed in accordance with the Trust's Security Breach Management Plan.

11. Accessing information

- 11.1. Horizons Specialist Academy Trust is transparent with data subjects, the information we hold and how it can be accessed.

- 11.2. All members of staff, parents of registered pupils and other users of the Trust's academies, e.g. visitors and third-party clubs, are entitled to:
- Know what information the Trust holds and processes about them or their child and why.
 - Understand how to gain access to it.
 - Understand how to provide and withdraw consent to information being held.
 - Understand what the Trust is doing to comply with its obligations under the GDPR.
- 11.3. All members of staff, parents of registered pupils and other users of the Trust's academies and its facilities have the right, under the GDPR, to access certain personal data being held about them or their child.
- 11.4. Personal information can be shared with pupils once they are considered to be at an appropriate age (13 years), responsible for their own affairs, and have capacity to make decisions; although, this information can still be shared with parents.
- 11.5. Pupils who are considered to be at an appropriate age (13 years) to make decisions for themselves, and have capacity to make decisions, are entitled to have their personal information handled in accordance with their rights.
- 11.6. The Trust will adhere to the provisions outlined in the Trust's GDPR Data Protection Policy when responding to requests seeking access to personal information.

12. Personal Data audit

- 12.1. The Trust conducts personal data audits on an annual basis against all information held by the Trust to evaluate the information the academy is holding, receiving and using, and to ensure that this is correctly managed in accordance with the GDPR. This includes the following information:
- Paper documents and records
 - Electronic documents and records
 - Databases
 - Microfilm or microfiche
 - Sound recordings
 - Video and photographic records
 - Hybrid files, containing both paper and electronic information
- 12.2. The audit may be completed in a number of ways, including, but not limited to:
- Interviews with staff members with key responsibilities – to identify information and information flows, etc.
 - Questionnaires to key staff members to identify information and information flows, etc.
 - A mixture of the above

- 12.3. The DPO is responsible for completing the audit. The audit will include the following:
- The Trust's data needs
 - The information needed to meet those needs
 - The format in which data is stored
 - How long data needs to be kept for
 - Vital records status and any protective marking
 - Who is responsible for maintaining the original document
- 12.4. The DPO will consult with staff members involved in the information audit process to ensure that the information is accurate.
- 12.5. Once it has been confirmed that the information is accurate, the DPO will record all details on the Trust's Personal Data Audit Register.
- 12.6. This information will be shared with the CEO to gain their approval.

13. Disposal of data

- 13.1. Where disposal of information is outlined as standard disposal, this will be recycled appropriate to the form of the information, e.g. paper recycling, electronic recycling.
- 13.2. Where disposal of information is outlined as secure disposal, this will be shredded or pulped and electronic information will be scrubbed clean and, where possible, cut. The DPO will keep a record of all files that have been destroyed.
- 13.3. Where the disposal action is indicated as reviewed before it is disposed, the DPO will review the information against its administrative value – if the information should be kept for administrative value, the DPO will keep a record of this.
- 13.4. If, after the review, it is determined that the data should be disposed of, it will be destroyed in accordance with the disposal action outlined in this policy.
- 13.5. Where information has been kept for administrative purposes, the DPO will review the information again after three years and conduct the same process. If it needs to be destroyed, it will be destroyed in accordance with the disposal action outlined in this policy. If any information is kept, the information will be reviewed every three subsequent years.
- 13.6. Where information must be kept permanently, this information is exempt from the normal review procedures

14. Monitoring and review

- 14.1. Any changes made to this policy will be communicated to all members of staff and the governing board.