BRADFORD ACADEMY TRUST

Responsibility | Respect | Resilience

Our **Vision** **RESPONSIBILITY** **RESPECT** **RESILIENCE**	**A shining light in our community** You are the light of the world. A city on a hill cannot be hidden. - Matthew 5:14b

Records Management Policy

Approved by:	RMC	**Date:**	December 2025
Last reviewed on:	December 2025		
Next review due by:	December 2026		
Related Documents			
Guidance	General data protection policy		
Author	**Data Protection Team**		

TABLE OF CONTENTS

1 INTRODUCTION AND SCOPE

Bradford Academy recognises records management as a core corporate function that supports the effective management of the organisation. A records management programme improves accountability, transparency, continuity, decision-making, and compliance with relevant legislation and regulations

This policy provides a framework for ensuring that we comply with the requirements of the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 (DPA), and other relevant legislation, as well as associated guidance and codes of practice.

This policy, including its appendices, applies to our entire workforce. This includes employees, governors or trustees, contractors, agents and representatives, volunteers and temporary staff working for or on our behalf. Individuals found to knowingly or recklessly infringe this policy may face disciplinary action.

This is our main Records Management policy and applies to all personal data, whether paper or electronic. It should be read alongside the other policies within our information governance policy framework.

2 ROLES AND RESPONSIBILITIES

Overall responsibility for ensuring that we meet the statutory requirements of any data protection legislation lies with the Board of Governors or Trustees. The following roles will have day-to-day responsibility for compliance and providing the necessary assurance to the Board.

2.1 DATA PROTECTION OFFICER (DPO)

The role of the DPO is to assist us in monitoring compliance with data protection legislation and advise on data protection issues. Bradford Academy have appointed Veritau as our DPO. Veritau's contact details are:

Schools Data Protection Officer
Veritau
West Offices
Station Rise
York
North Yorkshire
YO1 6GA

The DPO service is an advisory role, and its duties include:

- Informing and advising us and our employees about our obligations to comply with the UK GDPR, the Data Protection Act 2018, and other data protection and information access laws;
- Monitoring compliance with data protection legislation and other information governance policies;

- Raising awareness of data protection issues; and
- Liaising with the Information Commissioner's Office (ICO).

2.2 SENIOR INFORMATION RISK OWNER (SIRO)

The SIRO is responsible for overseeing the implementation of this policy and ensuring that effective records management practices are in place across the organisation. The SIRO is also responsible for operational management and will ensure that staff are appropriately trained in records management, supported by the SPOC and IAOs. In our organisation, this role lies with Executive Principal

2.3 DATA PROTECTION TEAM (DPT)

The DPT take on the duties of what is also commonly referred as 'Single Point of Contact (SPOC)'. The DPT are a number of senior staff members who are ultimately responsible for information risk. The DPT will ensure that our information governance policies and procedures are effective and comply with legislation, promote best practice, and embed a culture of data protection compliance. In our organisation, this role lies with the IT Director, Data Manager and Finance Director.

The DPT will take operational responsibility for data protection compliance, including communicating with data subjects and the DPO service.

2.4 INFORMATION ASSET OWNER (IAO)

An IAO is an individual responsible for the security and maintenance of a particular information asset and for ensuring that other staff members use the information safely and responsibly. IAOs will be appointed based on sufficient seniority and level of responsibility and will be documented in our Information Asset Register (IAR).

2.5 ALL STAFF

All staff, including governors or trustees, contractors, agents and representatives, volunteers, and temporary staff working for or on our behalf, will be responsible for collecting, storing, and processing personal data in accordance with this policy.

3 RECORDS MANAGEMENT

A record is 'information created, received, and maintained as evidence and an asset by an organisation in pursuit of legal obligations or in the transaction of business.' Records are retained for a period determined by legal, regulatory, and functional requirements.

A programme will be developed to manage our records throughout their lifecycle. This will include using methods such as version control, naming conventions, and file plans to ensure that records can be easily searched and accessed in the event of an information request.

We will ensure that our records are authentic, reliable, useable and have integrity to fulfil and retain their evidentiary value. Regular reviews of the records management programme will be conducted to ensure compliance and check that records are stored securely and can be accessed appropriately.

4 PUPIL RECORDS

We are required to maintain records for each pupil. This record is the core evidence of an individual's progress through the education system and will accompany them throughout their school career.

Pupil records are held electronically within our management information system (MIS) whenever possible. Information not forming part of the core record may be held outside the MIS in either electronic or paper format. This includes information with shorter retention periods, such as attendance registers, consent forms, medical forms, accident forms, absence notes, and pupil work.

Records relating to pupils involved with child protection or safeguarding are held securely in a designated system accessible to the Designated Safeguarding Lead and designated staff members. These records are stored separately from the core pupil record to ensure confidentiality and restricted accessibility. They may be retained for longer than the core pupil file.

We will ensure that the information in the pupil file is accurate, objectively recorded, expressed in a professional manner, and kept up to date.

Pupil records will be transferred electronically to any new setting the pupil attends. Once securely transferred, we will not keep copies of the pupil record unless there is ongoing legal action. The setting the pupil attends until the statutory school leaving age is responsible for retaining the pupil record until the pupil reaches the age of 25.

5 STAFF RECORDS

Records relating to our workforce will be held securely electronically, wherever possible, or in paper format. Appropriate security measures are in place to ensure confidentiality and restricted access.

Information related to child protection allegations against staff will be held separately from the core employee record to ensure confidentiality and restricted accessibility. This information may be held for longer than the core employee file.

6 INFORMATION ASSET REGISTER (IAR)

In accordance with Article 30 of UK GDPR, we will have an Information Asset Register (IAR) that maintains a record of our processing activities. The IAR will document what records we hold, where they are stored, who has access to the information, and the retention periods in place. It will be reviewed, at least annually, to ensure it remains accurate.

7 EMAIL MANAGEMENT

We will have a process in place to ensure that emails are managed in accordance with this policy and our retention framework. Emails discussing business or reflecting significant actions or decisions concerning our pupils or staff will not be stored in personal email inboxes. These emails must be filed into an appropriate electronic filing system, and the original email deleted.

8 SECURITY AND ACCESS

All records, especially those containing personal data, will be stored securely to maintain confidentiality while keeping the information accessible to those authorised to see it. Electronic records will have appropriate security and access controls, and systems will have robust audit functionality wherever possible.

Paper records will be stored in secure, lockable storage areas with restricted access to key roles.

When sharing or transferring records containing personal information, we will ensure appropriate transmission security controls are in place and align with our Information Security Policy.

9 INFORMATION REQUESTS AND DATA SUBJECT RIGHTS

Requests for information under Data Protection, Freedom of Information, Environmental Information, or other legislation will be handled in line with our Data Protection Policy.

10 RETENTION AND DISPOSAL

Retention is the period a record is kept after it stops being actively used but before it is destroyed. It is a vital part of records management as it allows organisations to retain records only for as long as needed and discourages records being held for long periods ‘just in case’.

Legal, regulatory, or functional requirements determine the retention period for particular types of records. We have implemented a Retention Framework that outlines our specified retention periods. This framework will be reviewed at least annually to ensure accuracy.

We will ensure that any records containing personal or confidential information are disposed of appropriately and securely in line with our retention schedule.

Records held in databases or electronic management systems, with the functionality to automatically destroy records after a specified period, will be used wherever possible. A review of the records will be carried out before destruction, where practical.

Where automatic disposal is not in place, for example, for paper records, we will conduct a manual review annually to ensure they are destroyed in line with retention framework.

The disposal of all information is documented to ensure that we maintain a record of when it has been deleted and by whom. This allows us to evidence that a record no longer exists or has been transferred to another setting in the event of an information request being received.

11 ARCHIVING

Where records are likely to have a historical value, or are worthy of permanent preservation based on their 'enduring value', we may choose to archive them at the end of any retention period. Where information is to be archived or destroyed, the Academy must carry out such processing by no later than the August after the expiration of the retention period.

When archiving is in place, the following safeguards are also applied:

- Appropriate measures are taken to minimise any identifiable personal data in the records, such as anonymisation or pseudonymisation (if this can be achieved without seriously impairing the archiving process)
- Ensuring the archived material is not being retained for decision-making about an individual
- The process of archiving is not likely to cause substantial damage or distress to an individual.

11.1 WHAT RECORDS MAY BE CONSIDERED OF 'ARCHIVAL VALUE'?

UK GDPR allows for the permanent preservation of such records where it is in the public interest, such as where it facilitates historical or academic research. This can include but is not limited to:

- Register of admissions
- Logbooks of activity in the school
- Records and minutes relating to management meetings and board meetings
- Whole school photographs
- Programmes of school events and celebrations
- Records relating to the school curriculum
- Visitor books
- School brochures or prospectus'

APPENDIX ONE – RETENTION FRAMEWORK

1. INTRODUCTION

According to the UK General Data Protection Regulations (UK GDPR), the Academy is required to retain records only for the necessary duration. This framework outlines the retention periods for processed information or records and applies to all formats of information.

2. ROLES AND RESPONSIBILITIES

The Academy is legally obligated to maintain its records and record-keeping systems in compliance with applicable data protection regulations. The Data Protection Team holds overall responsibility for the implementation, oversight, and review of this policy.

The Data Protection Team will provide guidance and training to all staff on effective records management practices and will actively promote adherence to this policy across the Academy.

All employees are responsible for ensuring the accuracy and integrity of the records they manage. Upon the conclusion of the designated retention period, staff must ensure that records are securely disposed of in accordance with this policy. Furthermore, any data related to the ongoing operations of the Academy must be stored in a centrally managed, access-restricted location—such as a shared drive or approved system—and not within personal folders or email accounts.

3. RECORD RETENTION

Records must be retained for as long as necessary to fulfil the operational requirements of the Academy, as well as to comply with applicable legal and regulatory obligations. We have conducted an evaluation of our records in order to:

- Assess their value as information sources on the Academy, its operations, relationships, and environment.
- Evaluate their significance as documentation of Academy activities and decisions.
- Determine if any legal or regulatory retention obligations apply, including but not limited to the Public Records Act (1958), the Freedom of Information Act (2000), the Limitation Act (1980), and the Data Protection Act (2018).

Where records are likely to have a historical value, or are worthy of permanent preservation, we may choose to archive them at the end of any retention period. Where information is to be archived or destroyed, the Academy must carry out such processing by no later than the August after the expiration of the retention period.

4. RETENTION SCHEDULE

The retention schedule (below) has been developed in accordance with guidance from the UK Government and the Information and Records Management Society (IRMS), which is widely referenced by the Information Commissioner's Office (ICO). While this schedule covers the most common categories of data, it may not be exhaustive. Where staff are unsure about specific retention periods, they should seek advice from the Academy's Data Protection Team.

The schedule suggests several actions that can be taken to dispose of information once it has reached the end of its retention period:

- Regular disposal
  - Records may be disposed of in a standard rubbish bin or skip.
- Secure disposal
  - Data is considered securely disposed of only if it cannot be read or reconstructed; standard skips and general waste are not considered secure.
  - Paper records must be shredded or placed in a secure bin for third-party shredding.
  - CDs/DVDs and other media should be destroyed into particles smaller than 6mm.
  - Electronic data, including backups, should be deleted.
- Review
  - At the end of the retention period, a review may be necessary to ascertain whether a further retention period is required to the one advised. If a further retention period isn't necessary, the information must be securely disposed of.
- Transfer
  - At the conclusion of the retention period, information may be transferred to another company or establishment. In such cases, the information should be transmitted securely via encrypted email or other secure electronic methods, by recorded delivery, or delivered in person.

5. CHILD PROTECTION RECORDS

Notwithstanding the retention timescales outlined below, the Academy reserves the right to prolong the retention period for any information if, upon review, it is determined that destroying such records could potentially compromise a child's safety. Any such decision will be formally documented and subjected to regular review.

6. THIRD PARTY SERVICES

The Academy may, at its discretion, engage an external company to assist with secure record disposal. Comprehensive due diligence will be conducted on all third-party providers to ensure they are reputable and that records are destroyed securely.

- A formal contract and data processing agreement will be established with the company to ensure adherence to the Data Protection Act and UK GDPR requirements.
- Comprehensive records of disposal will be systematically maintained.

7. STAFF DOCUMENTS, ONEDRIVE AND EMAILS

Staff documents, OneDrive accounts, and mailboxes are classified as personal working areas and should be managed accordingly. All documents pertaining to staff, pupils, or the operational continuity of the Academy that fall within the scope of the retention schedules must be stored in a central location, with any personal copies removed. Central storage repositories include, but are not limited to: MStore, SharePoint work areas/document libraries, CPOMs, and shared mailboxes. Staff documents, OneDrive, and email accounts will be retained for one year following the date of departure. The Academy reserves the right to retain this information for a longer period if necessary to support ongoing operations or meet statutory requirements. Any retention that exceeds these timeframes will be appropriately documented, including a review date and rationale.

8. RECORD-KEEPING

A log will be kept outlining the disposal of records when this has been done in line with the records retention schedule below.

When equipment or confidential waste is sent off-site for disposal or destruction by a third party, a record should be maintained that includes the collection date, the company responsible, and a brief description of the files destroyed. Upon destruction the third party is required to provide the academy with a certificate of destruction, which will be recorded.

Where documents are retained in excess of our retention schedule for archiving purposes, this will be recorded and a log will be kept of the date the decision was made, the authorising officer, a brief description of the files involved and the reason for the decisions made.

These records will establish a comprehensive audit trail for any inspections carried out by the Information Commissioner’s Office and will facilitate the handling of Freedom of Information requests in cases where the requested information is no longer retained.

9. FRAMEWORK REVIEW

The Data Protection Team will review this framework on an annual basis, or more often if required.

10. RECORD DISPOSAL TIMELINE

Pupils, Curriculum and Outcomes		
Record Description	**Retention Period**	**End Of Retention Period Action Required**
All records relating to creation and implementation of the Admissions Policy	Life of the policy + 3 years	Review
Paperwork relating to successful admissions	Date of admission + 1 year	Secure disposal
Paperwork relating to unsuccessful admissions	Resolution of case + 1 year	Secure disposal
Register of admissions	For each entry - date of entry + 6 years	Secure disposal
Proof of address supplied by parents as part of the admissions process	Current year + 1 year	Secure disposal
Supplementary information supplied for admission process such as information regarding religion and medical conditions	Successful admissions add to pupil file Unsuccessful admission retain until appeal process complete	Successful admissions see retention period for pupil file Unsuccessful admissions secure disposal
Published Admission Number reports	Current year + 6 years	Secure disposal
Pupil File (Primary)	Retain whilst at primary school	Transfer - Follow the pupil when they leave the primary school to either: - Another primary - Secondary school - Pupil referral unit If the pupil leaves under any other circumstance, the file should be sent to the local authority to retain.

Pupil Education Record (Secondary)	Date of birth of pupil + 25 years	Secure disposal
Secondary transfer sheets	Current year + 2 years	Secure disposal
Records regarding exclusions	Date of birth of pupil + 25 years	Secure disposal
Attendance registers	Every entry in the register must be preserved for 6 years after the date of the entry	Secure disposal
Attendance returns to the local authority	Current year + 1 years	Secure disposal
School census returns	Current year + 5 years	Secure disposal
SEND information	Date of birth + 25 years	Secure disposal
Management of exam registrations	Each exam board will have their own retention period that should be followed	Refer to exam board for retention period
Public examination results (pupil copy)	Certificates given to pupils and outcomes recorded on their pupil file	See retention periods for pupil files. All uncollected certificates to be returned to the examination board after date of exam + 1 year
Internal examination results (pupil copy)	Added to pupil file	See retention period for pupil file
Examination results (Academy copy)	Current year + 6 years	Secure disposal
Curriculum returns	Current year + 3 years	Secure disposal
SATs exam papers	Retain until any appeal/validation process is complete	Secure disposal
Value added and contextual data	Current year + 6 years	Secure disposal
Schemes of work	Current year + 1 year	Secure disposal
Timetable	Current year + 1 year	Secure disposal

Class lists	Current year + 1 year	Secure disposal
Record of homework set	Current year + 1 year	Secure disposal
Pupil's work	Where possible all work should be returned to pupils at the end of the academic year. If not possible, retain up to a maximum of one academic year.	Secure disposal – where personal data is identifiable
Pupil's digital documents and emails	Date of leaving + 1 year	Secure disposal
Records created to obtain approval for educational trips	Secondary - Date of visit + 10 years	Secure disposal
Parental consent forms for non-residential trips where no major incident	Conclusion of the trip	Secure disposal
Parental consent forms for non-residential trips where major incident occurred	Consent forms for all pupils on the trip should be retained for - date of birth of pupil involved +25 years	Review
Parental consent for residential trips	Date of birth of youngest pupil involved + 25 years	Secure disposal
Safeguarding records where child is not looked after, and leaves and doesn't transfer to another school	Concerns were at low level / threshold for referral to social care not met / no inter-agency involvement - Date of	Secure disposal

Safeguarding		
Retention Period	**End Of Retention Period Action Required**	**End Of Retention Period Action Required**
Safeguarding records where child is not looked after, and leaves and doesn't transfer to another school	Concerns were at low level / threshold for referral to social care not met / no inter-agency involvement - Date of birth + 25 years. A referral was made / social care involved / other agencies involved date child left school + 35 years	Secure disposal

Safeguarding records where child who is not looked after, leaves school and moves to another school; or where the child is under 18 and leaves to attend college	Chronology of events should be retained as above. Where new school has CPOMS- no action required (other than to retain chronology) as new school can access this once child on roll. Where the new school doesn't have CPOMS, or where we hold other safeguarding records, these should be either sent via a secure email platform or hand delivered to the DSL of the new school. If it is necessary to post the file, this should be by recorded delivery and a copy of the entire file should be kept until the new setting confirms safe receipt.	Secure disposal.
Safeguarding records for child who is looked after	Date child leaves school + 75 years	Secure disposal
Allegation which is child protection in nature against a visitor/volunteer, including where the allegation is unfounded	Until the person's normal retirement age or 10 years from the date of the allegation (whichever is longer)	Review

Human Resources		
Basic File Description	**Retention Period**	**End Of Retention Period Action Required**
All records leading up to the appointment of a new Executive Principal or phase principal	All relevant information added to the personnel file (see below) and all other information retained from date of appointment + 6 years	Secure disposal
All records leading up to the appointment of a new member of staff successful candidate	All relevant information added to the personnel file (see below) and all other information retained for 6 months	Secure disposal
All records leading up to the appointment of a new member of staff unsuccessful candidates	Date of appointment of successful candidate + 6 months	Secure disposal

Pre-employment vetting information - DBS checks	Copies of DBS certificates should not be retained for the Single Central Record, instead records should be kept of date of check, subjects name, unique reference number and type of check. However, there may be circumstances where a copy of the DBS certificate may be kept for a period of time: • If there is a formal risk assessment (positive disclosure form) in place. DBS is kept for the duration of the risk assessment or until such time that the convictions would be filtered by DBS (whichever is sooner). • If the Academy is waiting for a new starter's DBS to arrive, we may keep a copy of a DBS from a previous employer (if one has been provided), until the new DBS has been received.	Secure disposal
Proof of ID collected for DBS check	Checked and a note made of what was seen. If felt necessary, copy of documents can be added to personnel file.	Secure disposal
Evidence of right to work in the UK	Where possible, these documents should be added to the personnel file, Home Office requires that they are kept for 2 years from termination of employment.	Secure disposal
Records relating to TUPE	Date last member of staff transfers or leaves the organisation + 6 years	Secure disposal
Staff personnel files, including contract and training records	Termination of employment + 6 years	Secure disposal
Time sheets	Current year + 6 years	Secure disposal

Performance management records	Current year + 6 years	Secure disposal
Records relating to the agreement of pay and conditions	Date pay and conditions superseded + 6 years	Secure disposal
Training needs analysis	Current year + 1	Secure disposal
Allegation which is child protection in nature against a member of staff, including where the allegation is unfounded	Until the person's normal retirement age or 10 years from the date of the allegation (whichever is longer)	Review
Other disciplinary records where case not found	If the incident is child protection related see above; otherwise dispose of at conclusion of the case	Secure disposal
Disciplinary sanctions	Remain on personnel File	See retention period for personnel file.

	Finance	
Basic File Description	**Retention Period**	**End Of Retention Period Action Required**
All records relating to the creation and management of budgets	Life of the budget + 3 years	Secure disposal
Trustees Annual Report and Financial Statements	Date of report + 10 years	Secure disposal
Independent auditors report on regularity and report on financial statements	Financial year report relates to + 6 years	Secure disposal
Funding agreements	Date of last payment of funding + 6 years	Secure disposal
Funding records (capital grants, EAG, GAG etc)	Date of last payment of funding + 6 years	Secure disposal

Gift aid and tax relief	Date of last payment + 6 years	Secure disposal
Loans and Grants	Date of last payment on loans + 12 years	Secure disposal
Pupil grant applications	Current year + 3 years	Secure disposal
School fund records	Current financial year + 6 years	Secure disposal
School meal registers, including evidence of successful FSM eligibility checks	FSM - current year + 6 years; Other - current year + 3 years	Secure disposal
All other financial records and documents	Current financial year + 6 years	Secure disposal

Payroll		
Basic File Description	**Retention Period**	**End Of Retention Period Action Required**
Maternity pay records	Current year + 3 years	Secure disposal
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	From the end of the year in which the accounts were signed + 6 years	Secure disposal
Records relating to pensions	Date of last payment on the pension + 6 years	Secure disposal
Payroll records	Date of payroll run + 6 years	Secure disposal

Contracts and Licences		
Basic File Description	**Retention Period**	**End Of Retention Period Action Required**
All records relating to the management of contracts under seal (executed as a deed, signed and witnessed)	Last payment on contract + 12 years	Secure disposal

All records relating to the management of any other contract	Last payment on contract + 6 years	Secure disposal
Records relating to the monitoring of contracts	Current year + 2 years	Secure disposal
Records relating to software licenses	Date licence expires + 6	Secure disposal

Risk Management and Insurance		
Basic File Description	**Retention Period**	**End Of Retention Period Action Required**
Visitor books and signing in records	Current year + 6 years	Secure disposal
Insurance policies	Date policy expires + 6 years	Secure disposal
Records relating to the settlement of insurance claims	Date claim settled + 6 years	Secure disposal
Employers' liability insurance certificate	Closure of the Trust + 40 years	Secure disposal
Risk and control framework/Risk Register	Life of framework + 6 years	Secure disposal
H&S risk assessments (not fire - see below)	Life of risk assessment + 3 years	Secure disposal
Records relating to accident/injury at work	Date of incident + 12 years	Review (in the case of serious accidents, a further retention period will need to be applied, if not - secure disposal)
Accident book	3 years after last entry	Secure disposal

Accident Reporting Forms	Adult - Date of incident + 6 years Child - Date of birth + 25 years	Secure disposal
Other incident reports	Current year + 20 years	
Control of substances hazardous to health	Current year + 10 years	Review
Asbestos monitoring / management	Last action + 40 years	Secure disposal
Radiation monitoring / management	Last action + 50 years	Secure disposal
Fire precaution logbooks	Current year + 6 years	Secure disposal
Fire risk assessments	Life of the risk assessment + 6 years	Secure disposal
Business Continuity Plans	Date the plan was superseded + 3 years	Secure disposal

Property and Asset Management		
Basic File Description	**Retention Period**	**End Of Retention Period Action Required**
Land and building valuations	Date valuation superseded + 6 years	Secure disposal
Leases for land and other property.	Date lease expires + 6 years	Secure disposal
Transfer of land	Life of land ownership	Transfer to new owner
Property plans	Life of land ownership	Transfer to new owner
Records relating to the letting of school premises	Current year + 6 years	Secure disposal
Inventories of furniture and equipment	Current year + 6 years	Secure disposal

Disposal of assets	Date asset disposed of + 6 years	Secure disposal
Burglary, theft and vandalism reports forms	Current year + 6 years	Secure disposal
Property maintenance records	Current year + 6 years	Secure disposal
Acquiring, disposing of and maintenance of vehicles	Disposal of the vehicle + 6 years	Secure disposal
Service logs for vehicles	Leased vehicle - return to lease company with vehicle Owned vehicle - Life of vehicle + 6 years	Return to lease company Secure disposal
GPS tracking data	Date of journey + 6 years	Secure disposal

Management and Policies		
Basic File Description	**Retention Period**	**End Of Retention Period Action Required**
Policy documents created and administered by the Governing Board	Life of the policy + 3 years Management	Secure disposal
Minutes of meetings	For governance meetings see governance retention periods. For all other meetings - date of meeting + 3 years	Review
Reports created by the academy	Date of report + 3 years	Secure disposal
Professional Development Plans	Life of the plan + 6 years	Secure disposal
Self-evaluation forms	Current year + 6 years	Secure disposal
Management of complaints	Date complaint resolved + 3 years.	Review + Secure disposal
Records relating to the creation and distribution of circulars and newsletters	Current year + 1 year	Secure disposal

Records relating to the creation and management of Parent Teacher Association and other parent forums	Current year + 6 years	Secure disposal
Ofsted reports and papers	Life of the report	Review
Returns made to central government	Current year + 6 years	Secure disposal

Governance		
Basic File Description	**Retention Period**	**End Of Retention Period Action Required**
Articles of Association	Life of the Academy Trust	Regular disposal
Memorandum of Association	Life of the Academy Trust	Secure disposal
Constitution	Life of the Academy Trust	Regular disposal
Special Resolutions	Life of the Academy Trust	Secure disposal
Written Scheme of Delegation (SoD)	Life of the SoD + 10 years	Secure disposal
Rules and Bylaws	Date rules/bylaws superseded + 6 years	Secure disposal
Statutory registers (including directors/trustees, members, secretaries, register of interests, registers of gifts and hospitality)	Life of the Trust + 6 years	Secure disposal
Appointment and removal of members, trustees and Community Council Members or equivalent	Life of appointment + 6 years	Secure disposal
Director/trustee disqualification	Date of disqualification + 15 years	Secure disposal

Trustees Annual Report and Financial Statements	Date of report + 10 years	Secure disposal
Annual return/confirmation statement	Date of report + 10 years	Secure disposal
Strategic plans and reviews	Life of plan + 6 years	Secure disposal
Agendas, Minutes and meeting papers	One copy to be retained for the life of the Trust	Secure disposal
Annual schedule of business/agenda planner	Current year	Secure disposal
Procedures for the conduct of meetings (governance document)	Date document superseded + 6 years	Secure disposal

	Other data	
Basic File Description	**Retention Period**	**End Of Retention Period Action Required**
Data retrieved as part of a subject access request or a freedom of information request	A log will be kept of all information requests within the GDPR management platform. All communications related to the request and its outcome, along with any relevant documented evidence, will be stored on the GDPR platform or an appropriate secure SharePoint folder for one year from the date of the outcome.	NA Review and then Secure disposal.

Record of breaches and any data collected as part of the investigation.	A log will be kept of all information requests within the GDPR management platform. Any notes, correspondence or data collated as a result of the investigation will be held for 1 year following the date the breach was realised.	N/A Review and then Secure disposal
Data Processing Agreements, Data Sharing Agreements.	Last payment on contract/date processing or sharing terminated (whichever is later) + 6 year	Secure disposal
Data Protection Impact Assessments.	Life of the DPIA + 6 years	Secure disposal
Photography	The date the data subject has left the academy + 3 years (unless the photograph is deemed worthy of permanent preservation due to their historical or social value (i.e. a significant event in the life of the school; class or yearbook photographs).	Secure disposal
CCTV and body worn Cameras	CCTV footage/images will be retained for a maximum of 30 days. On occasion footage may be retained for longer than 30 days, for example where a safeguarding concern is being investigated or where a law enforcement body is investigating a crime, to give them the opportunity to view the images as part of an active investigation. Footage that is no longer part of an active investigation or falls under any other aspect of the Bradford Academy data retention schedule will be deleted.	Review and then Secure disposal