Policy document control box	
Policy title	**Data Retention and Schedule**
Policy owner	Brooke Hornby RBET HR and Operations Lead Maddy Smart RBAir GDPR Lead
Version	1.00
Approving body	
Date of meeting when version approved	November 2023
Date of next review	November 2024

Policy contents:

1. Introduction 3
2. Scope 3
3. Legislation and Guidance 4
4. Responsibilities 4
   4.1 The Trust 4
   4.2 Data Protection Officer 4
   4.3 Centre GDPR Lead 4
   4.4 The Head of Centre 4
   4.5 The Department GDPR Advisor 5
   4.6 All Staff 5
   4.7 Record Management Process 5
5. Management of pupil records 6
6. Document Retention 8
   6.1 Section 1- RBET Trustees 8
   6.2 Management of the Centre 13
   6.3 Human Resources 15

6.4 Pensions and Payroll 20
6.5 Health and Safety 21
6.6 Financial Management 24
6.7 Property Management 29
6.8 Pupil Management 30
6.9 Central Government and Local Authority 36
6.10 Central Government and Local Authority 39
7. Storing and protecting information 40
8. Accessing Information 41
9. Digital continuity statement 41
10. Information Audit 42
11. Disposal of data 43
12. Monitor and review 44
13. FREEDOM OF INFORMATION ACT 2000 44
APPENDIX 1 45
APPENDIX 2 46

Data Retention

1. Introduction

The Red Balloon Educational Trust (RBET) and its Centres recognise that by efficiently managing our records, we will be able to comply with our legal and regulatory obligations and contribute to the effective overall management of our Centre. Maintaining good records helps us to provide the evidence needed to protect the legal rights and interests of our Trust/Centres, and for us to demonstrate our performance and accountability.

Red Balloon Educational Trust (RBET) 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 fulfill the purpose(s) for which they were originally intended.
The Trust has created this policy to outline how records are stored, accessed, monitored, retained and disposed of, in order to meet the Trust's statutory requirements.

Legal framework

This policy has due regard to legislation including, but not limited to, the following:

- General Data Protection Regulation
- Freedom of Information Act 2000
- Limitation Act 1980 (as amended by the

Limitation Amendment Act 1980) This policy also has
due regard to the following guidance:

- Information Records Management Society 'Information Management Toolkit for Schools 2019'

2. Scope

This policy applies to all records created, received or maintained by permanent and temporary staff of the Trust and its Centres in the course of carrying out its functions. Also, by any agents, contractors, consultants or third parties acting on behalf of the Trust and its Centres.

Records are defined as all documents which facilitate the business carried out by the Centres and which are thereafter retained to provide evidence of transactions or activities. These records may be created, received or maintained in hard copy or electrical format e.g. paper documents, scanned documents, e-mails, audio and video recordings, text messages, notes of telephone and spreadsheets, Word Documents, Google Documents presentations, etc.

3. Legislation and Guidance

This policy meets the requirements of the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA 2018) and the Freedom of Information Act 2000(FOIA 2000). It is based on the IRMS Toolkit For Schools, the Department of Education – Data Protection Toolkit for Schools, Department of Education – Annual Review of Centre Records and Safe Destruction Checklist, and guidance published by the Information Commissioner's Office (ICO) on the GDPR.

4. Responsibilities

4.1 The Trust

The Trust has a statutory responsibility to maintain the Trust/Centre's records and record keeping systems in accordance with the regulatory framework of the Centre. Each Centre has a responsibility for maintaining its records and record-keeping systems in line with statutory requirements and this policy.

4.2 Data Protection Officer

The Red Balloon Educational Trust Data Protection Officer (DPO) is responsible for promoting compliance with this policy.

4.3 Centre GDPR Lead

The Centre GDPR Lead will be responsible for the day-to-day management of records at the their Centre and reviewing the policy on an annual basis, in conjunction with the Red Balloon Education Trust DPO and Local Governance. The Centre GDPR Lead will guide the GDPR Department Advisors to encourage compliance and best practice across the organisation.

4.4 The Head of Centre

The Head of Centre is responsible for ensuring this policy is implemented correctly at their own Centre.

4.5 The Department GDPR Advisor

The GDPR Department Advisors will work in collaboration with the Centre GDPR Lead and Red Balloon Educational Trust DPO to ensure compliance and best practice are followed. The role of the GDPR Department Advisor is as follows:

- A GDPR Department Advisor has an expert understanding of the data and processes within each department.
- They are an accessible point of contact for specific departments in relation to the data and systems that their team uses to ensure compliance with RBET policies.
- They maintain and support best practice across the department regarding collection, management, and retention of data.
- They signpost staff to the correct processes and resources and escalate to the GDPR Lead for their Centre or RBET DPO accordingly.
- They participate in an annual review of data, systems and processes with the RBET DPO and the external DPO Centre.

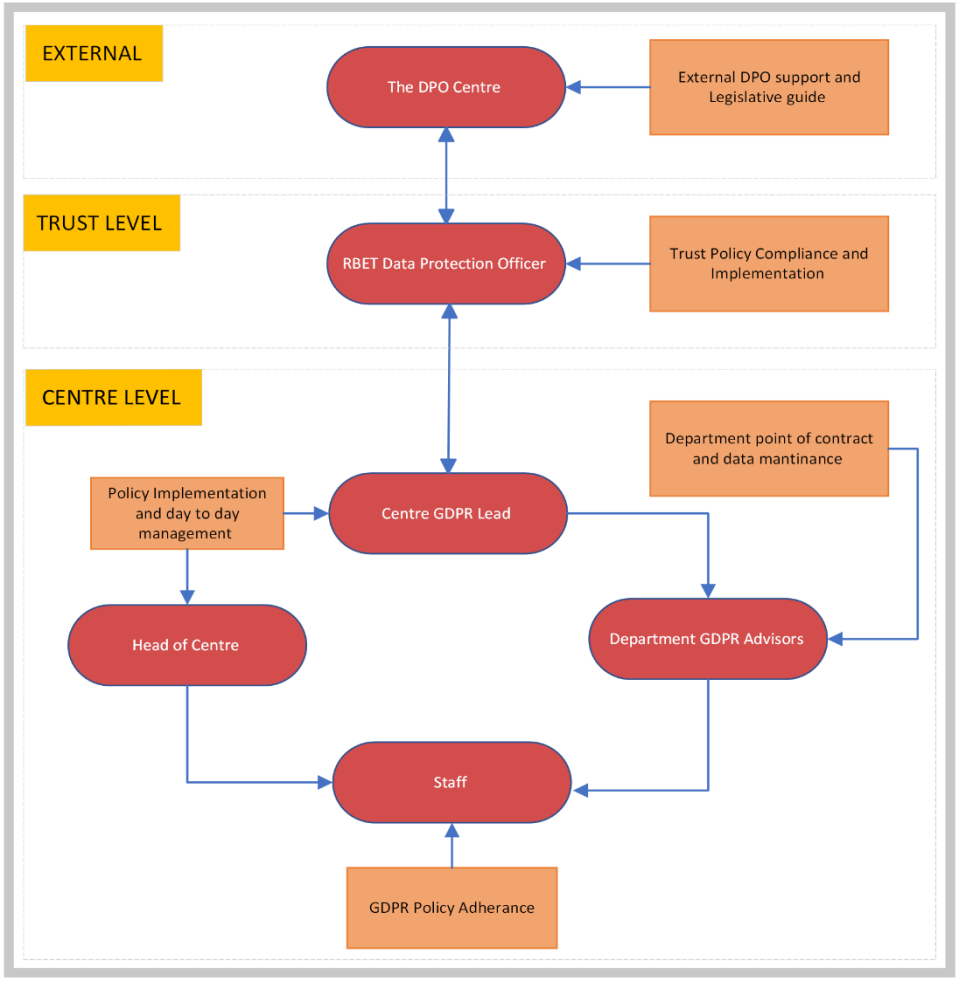
4.6 All Staff

It is the responsibility for all members of staff to ensure that our Centres do not keep personal information for longer than is necessary for the purpose or purposes for which it was collected.

It is the responsibility of all members of the Centres to ensure that they:

- Manage Trust/Centre records consistently in accordance with the Trust's and Centre policies and procedures;
- Properly document their actions and decisions;
- Hold personal information securely;
- Only share personal information appropriately and do not disclose it to an unauthorised third party;
- Dispose of records securely in accordance with the guidance set out in the Information and Records Management Society's toolkit for Schools Records Retention Schedule which can be found in Appendix 1
- Staff who do not comply with this policy may face disciplinary action.
- This policy does not form part of any employee's contract of employment and may be amended at any time.

4.7 Record Management Process



5. Management of pupil records

Pupil records are specific documents that are used throughout a pupil's time in the education system – they are passed to each Centre 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.

Where possible, all student information will be stored in the approved Management Information System however working documents and additional resources may be stored in Microsoft SharePoint or other secure storage facilities. The following information is stored on the front of a pupil record within the relevant database, and will be easily accessible:

- Forename, surname, gender, pronouns 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

The following lists common and potential record types that form part of the Pupil

Record:

- Admissions form
- Details of any SEND
- If the pupil has attended a previous educational setting, the record of transfer of any previous data
- Fair processing notice – only the most recent notice will be included
- Annual written reports to parents
- National curriculum and agreed syllabus record sheets
- Notes relating to major incidents and accidents involving the pupil
- Any information about an education and healthcare (EHC) plan and support offered in relation to the EHCP plan
- Any notes indicating child protection disclosures and reports are held
- Any information relating to exclusions
- Any correspondence with parents or external agencies relating to major issues, e.g. mental health
- Notes indicating that records of complaints made by parents or the pupil are held
- Examination results – pupil copy

The following information is subject to shorter retention periods and, therefore, will be stored separately in a personal file for the pupil in an appropriate secure location: they should not be forwarded to the pupils' next school or provision:

- Attendance Registers and Information
- Absence notes and correspondence
- Parental and, where appropriate, pupil consent forms for educational visits, photographs and videos, etc.
- Accident forms (a copy can be placed on the pupil record if it is a major incident)
- Medicine consent and administering records
- Copies of birth certificates, passports, etc.
- Correspondence with parents about minor issues, e.g. behaviour
- Pupil work and drawings
- Previous data collection forms which have been supersededChild protection records are kept in the approved safeguarding software, or, if received as paper copies, a lockable cabinet only accessible by the Head of Safeguarding DSL (Designated Safeguarding Lead) or other person trained to that level. Once a student leaves, those files are passed on via secure email or via physical media (in person or recorded delivery) to the 'receiving' educational provider (a signed receipt is required) or returned to the relevant local authority.

Actual copies of accident and incident information are stored separately on the individual Centres' 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.

Each Centre will ensure that no pupil records are altered or amended before transferring them to the next school or provision that the pupil will attend.

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, a named individual will be responsible for disposing records and will remove these records.

Electronic records relating to a pupil's record will also be transferred to the pupils' next Centre. Secondary academies including sixth forms.

If any pupil attends the Centre until the statutory Centre leaving age, the Centre will keep the pupil's records until the pupil reaches the age of 25 years.

Each Centre 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 provision 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 Centre.

6. Document Retention

6.1 Section 1- RBET Trustees

This section contains retention periods connected to the work and responsibilities of the Trustee board.

1.1 RBET Trustees - Operational Management				
Ref	Basic file description	Personal Information	Retention Period	Action at the end of the administrative life of the record
1.1.1	Instruments of government		For the life of the Centre	Consult local archives before disposal
1.1.2	Trusts and endowments		For the life of the Centre	Consult local archives before disposal
1.1.3	Records relating to the election of chair and vice chair	YES	Once the decision has been recorded in the minutes, the records relating to the election can be destroyed	SECURE DISPOSAL
1.1.4	Reports created for submission to the Charity Commission			SECURE DISPOSAL
1.1.5	Annual Reports required by the DfE	POSSIBLY	Date of report + 10 years	SECURE DISPOSAL
1.1.6	Action plans created and administered by the Trustees		Until superseded or whilst relevant	SECURE DISPOSAL

1.2 RBET Trustees – Meetings				
Ref	Basic file description	Personal Information	Retention Period	Action at the end of the administrative life of the record
1.2.1	Meetings schedule		Current year	STANDARD DISPOSAL
1.2.2	Agendas – principal copy		Where possible the agenda should be stored with the principal set of the minutes	Consult local archives before disposal
1.2.3	Minutes – principal set (signed)	YES	Although generally kept for the life of the Organisation, RBET is only required to make these available for 10 years from the date of the meeting	Consult local archives before disposal
1.2.4	Reports made to the trustees' meeting which are referred to in the minutes		Although generally kept for the life of the Organisation, RBET is only required to make these available for 10 years from the date of the meeting	Consult local archives before disposal
1.2.5	Register of attendance at full board meetings	YES	Date of meeting + 6 years	SECURE DISPOSAL

1.4 Trustee records – HR Management				
Ref	Basic file description	Personal Information	Retention Period	Action at the end of the administrative life of the record
1.4.1	Records relating to the appointment of a clerk to the Trustees	YES	Date on which clerk appointment ceases + 6 years	SECURE DISPOSAL
1.4.2	Records relating to appointment of Trustees	YES	Date appointment ceases + 6 years	SECURE DISPOSAL
1.4.3	Records relating to Trustee declaration against disqualification criteria	YES	Date appointment ceases + 6 years	SECURE DISPOSAL
1.4.4	Register of business interests	YES	Date appointment ceases + 6 years	SECURE DISPOSAL
1.4.5	Trustee code of conduct		This is expected to be a dynamic document; one copy of each version should be kept for the life of the organisation	
1.4.6	Records relating to the training safeguarding required and received by Trustees	YES	Except in cases where there has been an allegation of child protection, including if the allegation is unfounded. If so, until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	SECURE DISPOSAL

1.4.7	Records relating to the induction programme for new Trustees	YES	Date appointment ceases + 6 years	SECURE DISPOSAL
1.4.8	Records relating to DBS checks carried out on clerk and Trustees	YES	Date appointment ceases + 6 years	SECURE DISPOSAL
1.4.9	Trustee personnel files	YES	Date appointment ceases + 6 years Except in cases where there has been an allegation of child protection, including if the allegation is unfounded. If so, until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	SECURE DISPOSAL

6.2 Management of the Centre

This section contains retention periods connected to the processes involved in managing the Centre, including Human Resources, Financial Management, Payroll and Property Management.

2.1 Head of Centre and Senior Management Team Created Records				
Ref	Basic file description	Personal Information	Retention Period	Action at the end of the administrative life of the record
2.1.1	Reports created by the Head of Centre or the management team	POTENTIAL	Date of the report + a minimum of 3 years then review annually or as required if not destroyed	SECURE DISPOSAL
2.1.2	Correspondence created Heads of Centre, Senior Management Team or members of staff with administrative responsibilities	POTENTIAL	Current year + 3 years	SECURE DISPOSAL
2.1.3	Professional development plans	POTENTIAL	These should be held on the individual's personnel record. If not, then termination of employment + 6 years	SECURE DISPOSAL

2.2 Operational Administration				
Ref	Basic file description	Personal Information	Retention Period	Action at the end of the administrative life of the record
2.2.1	General file series which do not fit under any other category	POSSIBLY	Current year + 5 years, then review	SECURE DISPOSAL
2.2.2	Records relating to the creation and publication of the Centre brochure or prospectus	POSSIBLY	Current academic year + 3 years	The Centre could preserve a copy for their archive otherwise SECURE DISPOSAL
2.2.3	Records relating to the creation and distribution of circulars to staff, parents or pupils	POSSIBLY	Current academic year + 1 year	STANDARD DISPOSAL
2.2.4	Centre Privacy Notices which are published as part of UK GDPR compliance		Until superseded + 6 years	STANDARD DISPOSAL
2.2.5	Consents relating to Centre activities as part of UK GDPR compliance (for example, consent for use of images)	YES	Consent will last whilst the pupil attends the Centre, it can therefore be destroyed when the pupil leaves	SECURE DISPOSAL
2.2.6	Newsletters and other items with a short operational use	YES	Current academic year + 1 year [Centres may decide to archive a copy]	STANDARD DISPOSAL

2.2.7	Visitor management systems (including electronic systems, visitors books and signing-in sheets)	YES	Last entry in the visitors book + 12 months (unless report of serious incident or allegation)	SECURE DISPOSAL
2.2.8	CCTV Images (currently only in use at Milton)	YES	Images retained for 30 days and are then overwritten	SECURE DISPOSAL

6.3 Human Resources

3.1 Recruitment				
Ref	Basic file description	Personal Information	Retention Period	Action at the end of the administrative life of the record
3.1.1	All records created leading up to the appointment of an employee	YES	Add to personnel file	SECURE DISPOSAL
3.1.2	Records of unsuccessful job applicants	YES	Date of appointment of successful candidate + 6 months	SECURE DISPOSAL

3.1.3	Pre-employment vetting information + DBS Checks	YES	Duration of the employee's employment + 6 years as these are part of the personnel file. You are not required to retain a copy of the DBS Certificate through a DBS check sheet that must be completed and uploaded to the employees file. DBS should be carried out every 3 years therefore when completing a DBS Check form set an alert within the system with an expiry date being set 2.5 years from the date of the DBS check date	SECURE DISPOSAL
3.1.4	Forms of proof of identity collected as part of the process of checking "portable" enhanced DBS disclosure	YES	Where possible this process should be carried out using the on-line system. If it is necessary to take a copy of documentation then it should be retained on the staff personal file. You are not required to retain a copy of the DBS Certificate through a DBS check sheet that must be completed and uploaded to the employees file. DBS should be carried out every 3 years therefore when completing a DBS Check form set an alert within the system with an expiry date being set 2.5 years from the date of the DBS check date	SECURE DISPOSAL

3.1.5	Pre employment vetting information – Evidence proving the right to work in the United Kingdom	YES	These documents should be stored securely in the personnel file, however the Home Office requires that copies of the documents are securely destroyed 2 years following the termination of employment.	SECURE DISPOSAL

3.2 Operational Staff Management				
Ref	Basic file description	Personal Information	Retention Period	Action at the end of the administrative life of the record
3.2.1	Staff personnel file ● Application Form ● Offer Letter ● Qualification Certificate(s) ● Signed Contract ● Job Description ● References ● Details of Enhanced DBS ● Right to Work Check ● Training Certificates, including Safeguarding ● Probation Review ● GDPR Form ● Medical Form ● Any other documents i.e Disiplinary,	YES	Termination of Employment + 6 years. Except in cases where there has been an allegation of child protection, including if the allegation is unfounded. If so, until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	SECURE DISPOSAL

	grievance etc			
3.2.2	Annual appraisal /assessment records	YES	Current year + 6 years	SECURE DISPOSAL
3.2.3	Staff training – where the training leads to continuing professional development	YES	Length of time required by the professional body	SECURE DISPOSAL
3.2.4	Staff training – except where dealing with children, e.g. first aid or health and safety	YES	This should be retained on the personnel file	SECURE DISPOSAL
3.2.5	Staff training where the training relates to children (e.g. safeguarding or other child related training)	YES	Termination of Employment + 6 years. Except in cases where there has been an allegation of child protection, including if the allegation is unfounded. If so, until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	SECURE DISPOSAL

3.2.6	Sickness absence monitoring	YES	Current year + 3 years .	SECURE DISPOSAL

3.3 Disciplinary and Grievance Processes				
Ref	Basic file description	Personal Information	Retention Period	Action at the end of the administrative life of the record
3.3.1	Records relating to any allegation of a child protection nature against a member of staff	YES	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 the allegations are found, they should be kept on the individual's personnel file and a copy provided to the person concerned.	SECURE DISPOSAL
3.3.2	Verbal warning	YES	Date of warning + 6 months	SECURE DISPOSAL
3.3.3	Written warning – level 1	YES	Date of warning + 6 months	SECURE DISPOSAL
3.3.4	Written warning – level 2	YES	Date of warning + 12 months	SECURE DISPOSAL
3.3.5	Final warning	YES	Date of warning + 18 months	SECURE DISPOSAL
3.3.6	Case not found – not related to child protection		Dispose of at the conclusion of the case	SECURE DISPOSAL

3.3.7	Case not found – related to child protection		If the incident is related to child protection then see 3.3.1, otherwise dispose of at the conclusion of the case.	SECURE DISPOSAL

6.4 Pensions and Payroll

4.1 Payroll and Pensions				
Ref	Basic file description	Personal Information	Retention Period	Action at the end of the administrative life of the record
4.1.1	Absence record	YES	Current year + 3 years	SECURE DISPOSAL
4.1.2	Payroll Batches	YES	Current year + 6 years	SECURE DISPOSAL
4.1.3	Car mileage claims	YES	Current year + 6 years	SECURE DISPOSAL
4.1.4	Insurance	YES	Current year + 6 years	SECURE DISPOSAL
4.1.5	Maternity payment	YES	Current year + 3 years	SECURE DISPOSAL
4.1.6	Overtime	YES	Current year + 6 years	SECURE DISPOSAL
4.1.7	Payroll awards	YES	Current year + 6 years	SECURE DISPOSAL
4.1.8	Payroll – gross/net weekly or monthly	YES	Current year + 6 years	SECURE DISPOSAL
4.1.9	Payroll reports	YES	Current year + 6 years	SECURE DISPOSAL
4.1.10	Payslips – copies	YES	Current year + 6 years	SECURE DISPOSAL
4.1.11	Pension payroll	YES	Current year + 6 years	SECURE DISPOSAL

4.1.12	Personal bank details	YES	Until superseded + 3 years	SECURE DISPOSAL
4.1.13	Sickness records	YES	Current year + 3 years	SECURE DISPOSAL
4.1.14	Superannuation adjustments	YES	Current year + 6 years	SECURE DISPOSAL
4.1.15	Superannuation reports	YES	Current year + 6 years	SECURE DISPOSAL
4.1.16	Tax forms P6/P11/ P11D/P35/P45/ P46/ P48	YES	Current year + 6 years	SECURE DISPOSAL

6.5 Health and Safety

5.1 Health and Safety				
Ref	Basic file description	Personal Informatio n	Retention Period	Action at the end of the administrative life of the record
5.1.1	Health and safety policy statements		Life of policy + 3 years	SECURE DISPOSAL
5.1.2	Health and safety risk assessments		Life of risk assessment + 3 years provided that a copy of the risk assessment is stored with the accident report if an incident has occurred	SECURE DISPOSAL

5.1.3	Accident reporting records relating to individuals who are over 18 years of age at the time of the incident	YES	Date of incident + 3 years	SECURE DISPOSAL

5.1.4	Accident reporting records relating to individuals who are under 18 years of age at the time of the incident	YES	Date of incident + 3 years	SECURE DISPOSAL
5.1.5	Records relating to any reportable death, injury, disease or dangerous occurrence (RIDDOR).	YES	Date of incident + 3 years provided that all records relating to the incident are held on personnel file [see 2.4.2 above]	SECURE DISPOSAL
5.1.6	Control of Substances Hazardous to Health (COSHH)	POSSIBLY	Date of incident + 40 years	SECURE DISPOSAL
5.1.7	Process of monitoring of areas where employees and persons are likely to have come into contact with asbestos		Last action + 40 years	SECURE DISPOSAL
5.1.8	Fire precautions log books		Current year + 3 years	SECURE DISPOSAL
5.1.19	Health and safety file to show current state of building, including all Alterations (wiring, plumbing, building works, etc.), to be passed on in the case of change of ownership		Pass to new owner on sale or transfer of building	

6.6 Financial Management

6.1 - Financial Management				
Ref	Basic file description	Statutory Provisions	Retention Period	Action at the end of the administrative life of the record
6.1.1	Employer's liability insurance certificate		Closure of the Centre + 40 years	SECURE DISPOSAL Consult Local Authority if the Centre closes

6.2 Asset Management				
Ref	Basic file description	Statutory Provisions	Retention Period	Action at the end of the administrative life of the record
6.2.1	Inventories of furniture and equipment		Current year + 6 years	SECURE DISPOSAL
6.2.2	Burglary, theft and vandalism report forms		Current year + 6 years	SECURE DISPOSAL

6.3 Accounts and Statements				
Ref	Basic file description	Statutory Provisions	Retention Period	Action at the end of the administrative life of the record
6.3.1	Annual accounts		Current year + 6 years	STANDARD DISPOSAL
6.3.2	Loans and grants managed by the Trust		Date of last payment on the loan + 12 years then review	SECURE DISPOSAL
6.3.3	All records relating to the creation and management of budgets, including the annual budget statement and back-ground papers		Life of the budget + 3 years	SECURE DISPOSAL
6.3.4	Invoices, receipts, order books and requisitions, delivery notices		Current financial year + 6 years	SECURE DISPOSAL
6.3.5	Records relating to the collection and banking of monies		Current financial year + 6 years	SECURE DISPOSAL
6.3.6	Records relating to the identification and collection of debt		Final payment of debt + 6 years	SECURE DISPOSAL

6.4 Pupil Finance				
Ref	Basic file description	Personal Information	Retention Period	Action at the end of the administrative life of the record
6.4.1	Student Invoices	YES	Current financial year + 6 years	SECURE DISPOSAL

6.5 Contract Management				
Ref	Basic file description	Statutory Provisions	Retention Period	Action at the end of the administrative life of the record
6.5.1	All records relating to the management of contracts under seal	Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL
6.5.2	All records relating to the management of contracts under signature	Limitation Act 1980	Life of contract + 6 years	SECURE DISPOSAL
6.5.3	Records relating to the monitoring of contracts		Life of contract + 6 years	SECURE DISPOSAL

6.6 Centre Funds				
Ref	Basic file description	Statutory Provisions	Retention Period	Action at the end of the administrative life of the record
6.6.1	Centre Fund – Cheque books		Current year + 6 years	SECURE DISPOSAL
6.6.2	Centre Fund – Paying in books		Current year + 6 years	SECURE DISPOSAL
6.6.3	Centre Fund – Ledger		Current year + 6 years	SECURE DISPOSAL
6.6.4	Centre Fund – Invoices		Current year + 6 years	SECURE DISPOSAL
6.6.5	Centre Fund – Receipts		Current year + 6 years	SECURE DISPOSAL
6.6.6	Centre Fund – Bank statements		Current year + 6 years	SECURE DISPOSAL

6.7 Fundraising & Donations				
Ref	Basic file description	Statutory Provisions	Retention Period	Action at the end of the administrative life of the record
6.7.1	Gift Aid declaration forms and returns	HMRC	Current year + 6 years	SECURE DISPOSAL
6.7.2	Donations received from third party donation platforms	HMRC	Current year + 6 years	SECURE DISPOSAL
6.7.3	Website donation information	HMRC	Current year + 6 years	SECURE DISPOSAL

6.7 Property Management

7.1 Property Management				
Ref	Basic file description	Statutory Provisions	Retention Period	Action at the end of the administrative life of the record
7.1.1	Title deeds of properties belonging to the Centre		These should be retained by the property's owner unless the property has been registered with the Land Registry	
7.1.2	Plans of properties belonging to the Centre		These should be retained whilst the building belongs to the Centre and should be passed on to any new owners if the building is leased or sold.	
7.1.3	Leases of property leased by or to the Centre		Expiry of lease + 6 years	SECURE DISPOSAL
7.1.4	Records relating to the letting of Centre premises		Current financial year + 6 years	SECURE DISPOSAL

7.2 Property Management – Maintenance				
Ref	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
7.2.1	All records relating to the maintenance of the Centre carried out by contractors		These should be retained whilst the building belongs to the Trust and should be passed on to any new owners if the building is leased or sold.	SECURE DISPOSAL
7.2.2	All records relating to the maintenance of the Centre carried out by Centre employees, including maintenance log books		These should be retained whilst the building belongs to the Trust and should be passed on to any new owners if the building is leased or sold.	SECURE DISPOSAL

6.8 Pupil Management

This section contains retention periods connected to the processes involved in managing a pupil's journey through their time at the Centre, including the admissions process.

8.1 Admissions Process				
Ref	Basic file description	Personal Information	Retention Period [Operational]	Action at the end of the administrative life of the record
8.1.1	All records relating to the creation and implementation of the Centre Admissions Policy		Life of the policy + 3 years then review	SECURE DISPOSAL
8.1.2	Admissions records – if the admission is successful	YES	This information is used to create the pupil record on the MIS.	SECURE DISPOSAL
8.1.3	Admissions records – if the admission is unsuccessful	YES	6 months following notification of outcome	SECURE DISPOSAL
8.1.4	Register of Admissions	YES	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made	SECURE DISPOSAL
8.1.5	Supplementary information provided as part of admissions process such as medical conditions, previous assessments, wellbeing reviews – if the admission is successful	YES	This information should be added to the pupil file.	SECURE DISPOSAL

8.1.6	Supplementary information provided as part of admissions process such as medical conditions, previous assessments, wellbeing reviews – if the admission is unsuccessful	Yes	6 months following notification of unsuccessful admission then destroyed	
8.1.7	Panel meeting minutes	Yes	Current academic year + 1	Secure disposal

8.2 Pupils Educational Record				
Ref	Basic file description	Personal Information	Retention Period	Action at the end of the administrative life of the record
8.2.1	Pupil's Educational Record	YES	Retain whilst the student remains in the Centre, then archive until the following threshold: Date of birth of the pupil + 25 years	The record should follow the pupil when he/she leaves the primary Centre. This will include: To another Centre To an alternative provision
8.2.2	Individual student SharePoint folders	Yes	Retain whilst the student remains in the Centre, then archive until the following threshold: Date of birth of the pupil + 25 years	SECURE DISPOSAL

8.2.3	Public Examination Results	YES	This information should be added to the pupil file	Centre must securely destroy any unclaimed certificates after retaining them for a minimum of 12 months. Centres that do not have a means of destroying certificates confidentially may return them to the respective awarding body.
8.2.4	Internal Examination Results	YES	This information should be added to the pupil file	
8.2.5	Child protection information held on pupil file	YES	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
8.2.6	Child protection information held separate from pupil file (eg. Online safeguarding software)	YES	DOB of the child + 25 years then review.	SECURE DISPOSAL

8.2.7	Examination records generated as part of JCQ inspections	YES	Until closure of examination appeals process	SECURE DISPOSAL

8.3 Attendance				
Ref	Basic file description	Personal Information	Retention Period	Action at the end of the administrative life of the record
8.3.1	Attendance Registers	YES	Every entry in the attendance register must be preserved for a period of 3 years after the date on which the last entry was made.	SECURE DISPOSAL
8.3.2	Correspondence relating to any absence (authorised or unauthorised)	YES	Current academic year + 2 years	SECURE DISPOSAL

8.4 Special Educational Needs Information				
Ref	Basic file description	Personal Information	Retention Period	Action at the end of the administrative life of the record
8.4	Special Educational Needs files, reviews and EHCPs. Including advice and information provided to parents regarding educational needs and accessibility strategy	YES	Date of birth of the pupil + 31 years then REVIEW. If no legal action pending, then destroy.	SECURE DISPOSAL

6.9 Central Government and Local Authority

9.1 Statistics and Management Information				
Ref	Basic file description	Personal Information	Retention Period [Operational]	Action at the end of the administrative life of the record
9.1.1	Curriculum returns		Current year + 3 years	SECURE DISPOSAL
9.1.2	Examination Results (Centre's copy)	YES	Current year + 6 years	SECURE DISPOSAL
9.1.3	Exam Results	YES	Exam results should be recorded on the pupil's educational file and will therefore be	SECURE DISPOSAL

			retained until the pupil reaches the age of 25 years. The Centre may wish to keep a composite record of all of the whole year's exam results. These could be kept for current year + 6 years to allow suitable comparison	
9.1.5	Published Admission Number (PAN) Reports		Current year + 6 years	SECURE DISPOSAL
9.1.6	Value added and contextual data		Current year + 6 years	SECURE DISPOSAL
9.1.7	Self-evaluation forms - internal moderation	YES	Academic year plus 1 academic year	SECURE DISPOSAL
9.1.8	Self-evaluation forms - external moderation	YES	Until superseded	SECURE DISPOSAL

9.2 Implementation of the Curriculum				
Ref	Basic file description	Personal Information	Retention Period	Action at the end of the administrative life of the record
9.2.1	Schemes of work		Current year + 1 year	SECURE DISPOSAL
9.2.2	Timetable		Current year + 1 year	SECURE DISPOSAL

9.2.3	Group records	YES	Current year + 1 year	SECURE DISPOSAL
9.2.4	Mark books	YES	Current year + 1 year	SECURE DISPOSAL
9.2.5	Pupil's work	POSSIBLY	Where possible, the pupil's work should be returned to the pupil at the end of the academic year. If this is not the Centre's policy then current year + 1 year The Centre may also elect to retain some copies of pupil work for a reasonable length of time, to allow for inspection from external agencies (e.g. OFSTED)	SECURE DISPOSAL

9.3 Centre Trips				
Ref	Basic file description	Personal Informatio n	Retention Period	Action at the end of the administrative life of the record
9.3.1	Parental consent forms for Centre trips – where there has been no major incident	YES	The Centre should complete a risk assessment to assess whether the forms are likely to be required and could make a decision to dispose of the consent forms at the end of the trip (or at the end of the academic year).	SECURE DISPOSAL

9.3.2	Parental permission slips for Centre trips – where there has been a major incident	YES	Date of birth 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	SECURE DISPOSAL

6.10 Central Government and Local Authority

10.1 Local Authority				
Ref	Basic file description	Personal Information	Retention Period	Action at the end of the administrative life of the record
10.1	Attendance returns	YES	Current year + 1 year	SECURE DISPOSAL
10.2	Centre census returns	YES	Current year + 5 years	SECURE DISPOSAL

7. Storing and protecting information

The GDPR Lead will undertake a risk analysis to identify which records are vital to Trust and individual Centres' management and these records will be stored in the most secure manner.

- Each Centre will have data backed-up with the support of the Central IT team 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.
- Where possible, backed-up information will be stored off the Centre premises, using a central back-up service operated.
- Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access.
- Confidential paper records are not left unattended or in clear view when held in a location with general access.
- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed-up.
- Where data is saved on removable storage or a portable device, the device is kept in a locked filing cabinet, drawer or safe when not in use.
- Memory sticks are not used to hold personal information unless they are password-protected and fully encrypted.
- All electronic devices are password-protected to protect the information on the device in case of theft.
- Where possible, the Trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- Staff and governors do not use their own personal email addresses for Centre purposes.
- All members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password in line with the current Password Policy.
- 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 in a separate email.
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- 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 Centre premises accepts full responsibility for the security of the data.
- 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.
- 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.
- Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of each Centre containing sensitive information are supervised at all times.

8. Accessing Information

RBET is transparent with data subjects, the information we hold and how it can be accessed.

All members of staff, parents of registered pupils and other users of the Trust, 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.
- All members of staff, parents of registered pupils and other users of the Trust, its academies and its facilities have the right, under the GDPR, to access certain personal data being held about them or their child.
- Personal information can be shared with pupils once they are considered to be at an appropriate age and responsible for their own affairs; although, this information can still be shared with parents.
- Pupils who are considered to be at an appropriate age to make decisions for themselves are entitled to have their personal information handled in accordance with their rights.

9. Digital continuity statement

Digital data that is retained for longer than six years will be named as part of a digital continuity statement.

- The GDPR Lead will identify any digital data that will need to be named as part of a digital continuity statement.
- The data will be archived to dedicated files on the Trust's servers, which are password-protected – this will be backed-up.
- Memory sticks will never be used to store digital data, subject to a digital continuity statement.
- The Central Services IT Manager will review new and existing storage methods annually and, where appropriate add them to the digital continuity statement.

The following information will be included within the digital continuity statement:

- A statement of purpose and requirements for keeping the records
- The names of the individuals responsible for long term data preservation
- A description of the information assets to be covered by the digital preservation statement

- A description of when the record needs to be captured into the approved file formats • A description of the appropriate supported file formats for long-term preservation
- A description of the retention of all software specification information and licence information
- A description of how access to the information asset register is to be managed in accordance with the GDPR

10. Information Audit

The Trust conducts information audits on an annual basis against all information held by each Centre to evaluate the information the Centre 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

The information 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

The GDPR Lead is responsible for completing the information audit. The information audit will include the following:

- The Trust's and individual Centres' 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?

The GDPR Lead will consult with staff members involved in the information audit process to ensure that the information is accurate.

Once it has been confirmed that the information is accurate, the GDPR Lead will record all details

on the Trust's Information Asset Register.

The information displayed on the Information Asset Register will be shared with the Board and each designated Centre leader to gain their approval.

11. Disposal of data

- All records containing personal information, or sensitive policy information will be made either unreadable or unreconstructable.
    - Digital files will be deleted and removed from the local bin or system bin
    - Paper records should be shredded using a cross-cutting shredder
    - CDs / DVDs should be cut into pieces
    - Audio / Video Tapes and Fax Rolls should be dismantled and shredded
    - Hard Disks should be dismantled and sanded
- 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 GDPR Champion will keep a record of all files that have been destroyed.
    - The shredding will be planned with specific dates and all records will be identified as to the date of destruction.
- 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.
- Where the disposal action is indicated as reviewed before it is disposed, the GDPR Champion will review the information against its administrative value – if the information should be kept for administrative value, the DP Lead will keep a record of this.
    - 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.
- Where an external provider is used, where possible, all records will be shredded on-site in the presence of an employee. The organisation must also be able to prove that the records have been destroyed by the company who should provide a Certificate of Destruction. Staff working for the external provider will be trained in the handling of confidential documents.
- Where information has been kept for administrative purposes, the GDPR Champion 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.
- Where information must be kept permanently, this information is exempt from the normal review procedures

NOTE 1: Do not put records containing personal information with the regular waste or a skip.
NOTE 2: if the records are recorded as 'to be destroyed' but have not yet been destroyed and a request for the records has been received they MUST still be provided.

12. Monitor and review

This policy will be reviewed on an annual basis by the GDPR Lead in conjunction with the DPO, Trustees and Centres Business Officers – the next scheduled review date for this policy is November 2024.

Any changes made to this policy will be communicated to all members of staff and trustees.

13. FREEDOM OF INFORMATION ACT 2000

The Freedom of Information Act 2000 requires us to maintain a list of records which have been destroyed and who authorised their destruction.
When destroying either a substantial amount of information or information which is of a particularly sensitive or important nature, members of staff should record at least:

- The information that has been destroyed
- The volume of the information that has been destroyed
- Who provided authorisation to destroy the information
- The date the information was destroyed

By following this guidance and completing the Annual Checklist, we will ensure that our Trust and Centres are compliant with the Data Protection rules and the Freedom of Information Act 2000.

APPENDIX 1

Template Records and Safe Destruction Log

Records and Data safely destroyed
The following sheet can be completed or alternatively documented in a spreadsheet.

Ref Number	File/Record Title	Description	Reference or Cataloguing Information	Number of Files Destroyed	Method of destruction	Confirm (i) Safely destroyed (ii) In accordance with Data Retention Guidelines (Date and INITIAL)
6.3.4	*Centre Invoices*	*Copies of purchase invoices dated 2011/12*	*Folders marked "Purchase Invoices 2011/12" 1 to 3*	*3 Folders*	*Shredding*	*BH – 27/08/2021*
2.2.7	*Visitor manageme n t systems*	*Copy of signing in book – dated 09/2010 – 09/2011*		*1 folder*	*Shredding*	*BH – 27/08/2021*

APPENDIX 2

Annual Review of Centre Records Checklist Annual Checklist to be completed by each Centre in the Trust

Checklist for Annual Review of Individual Centre Records and Safe Data Destruction

Completion page

Centre name: Review completed by:

Date: Approved by Head of Centre :

Date:

Note – The completion of this review should be shared at the board meeting and minuted. A. Summary of areas reviewed:

Ref	Area	Pages	Annual Review Completed Tick (√)	Reviewer Initials
1	The Governing Body			
2	Management of the Centre			
3	Human Resources			
4	Pensions and Payroll			
5	Health and Safety			
6	Financial Management			
7	Property Management			
8	Pupil Management			
9	Curriculum Management and Extra Curricular Activities			
10	Central Government and Local Authority			

RedBalloon
Educational Trust