DATA RECORD MANAGEMENT AND RETENTION

POLICY

Last Updated: 10/03/2019

Contents

1. Scope of the Policy 2

2. Responsibilities 2

3. Information Security & Business Continuity 2

4. Disclosure / Confidentiality 3

5. Safe Disposal of Records 4

6. Security Breach 4

7. Retention Guidelines 4

Section 1: Management of the School 6

Section 2: HR Management of the School 11

Section 3: Financial Management of the School 15

Section 4: Property Management 18

Section 5: Pupil Management 20

Section 6: Curriculum Management **Error! Bookmark not defined.**

Section 7: Extra Curricular Activities **Error! Bookmark not defined.**

Section 8: Central Government & Local Authority 23

REACH recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Records provide evidence for protecting the legal rights and interests of the school, and provide evidence for demonstrating performance and accountability. This document provides the policy framework through which this effective management can be achieved and audited.

1. Scope of the Policy

This policy applies to all records created, received or maintained by staff of REACH in the course of carrying out its functions.

Records are defined as all those documents that facilitate the business carried out by REACH and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.

2. Responsibilities

REACH has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Alternative Education Director.

The person responsible for records management in the school will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way.

The Data Protection Officer will monitor compliance with this policy by carrying out an annual audit to check if records are stored securely and can be accessed appropriately.

Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with REACH's retention guidelines.

3. Information Security & Business Continuity

In order to protect the data and records the school is responsible for, the following security measures will be implemented.

The Storage & Security of Digital Data

Back Up System: REACH will undertake regular back ups of all information held electronically to enable restoration of the data in the event of an environmental or data corruption incident. A back-up takes place every night to the backup server.

REACH checks that the backup has run overnight the following day, on a daily basis. Any errors are logged and looked into.

Controlling the Storage of Digital Data: Personal information is not stored on the hard drive of any laptop or PC.

Password Control: REACH will ensure that data is subject to a robust password protection regime. The network passwords must be a minimum of 8 characters which must include capitals and lower case, numbers and symbols and are changed every 3 months. Password sharing is not encouraged. Staff are required to lock their PCs when they are away from their desks to prevent unauthorised use. In any event, PC's will automatically lock after 4 minutes.

The Storage & Security of Hard Copy Data

Storage of Physical Records: REACH recommends that all physical records are stored in filing cabinets, drawers or cupboards. Sensitive physical records should be kept in a lockable storage area. This is to prevent unauthorised access but also to protect against the risk of fire and flooding.

Unauthorised Access, Theft or Loss: Staff are encouraged not to take personal data on staff or students out of REACH unless there is no alternative. Records held within the REACH should be in lockable cabinets.

Clear Desk Policy: In order to avoid unauthorised access to physical records which contain sensitive or personal information and will protect physical records from fire and/or flood dame, REACH operates a clear desk policy. This involves the removal of the physical records to a cupboard or drawer (lockable where appropriate). It does not mean that the desk has to be cleared of all contents.

4. Disclosure / Confidentiality

Staff are made aware of the importance of ensuring that personal information is only disclosed to people who are entitled to receive it and that consideration has been given

to the General Data Protection Regulations. This is outlined in the Staff Handbook.

If REACH receives a request for information from a third party, then the process outlined in the Third Party Requests for Information Process should be followed.

5. Safe Disposal of Records

The General Data Protection Regulations give individuals the Right to Erasure which means that records should not be kept for any longer than is necessary in relation to the purpose for which it was originally collected/processed (see Section 7 Retention Guidelines).

All records containing personal information or sensitive policy information should be made either unreadable or not reconstructable.

- Paper records should be shredded using a cross-cutting shredder
- CDs/DVDs/Floppy Discs should be cut into pieces
- Audio/Video Tapes and Fax Rolls should be dismantled and shredded
- Hard discs should be dismantled and sanded

All records must be shredded on site in the presence of an employee. The disposal company must provide a Certificate of Destruction.

6. Security Breach

In the event of an incident involving the loss of information or records held by REACH, the Data Breach Policy should be followed.

7. Retention Guidelines

This retention schedule is based upon the schedule provided by the Information and Records Management Society (v5 01.02.16).

This retention schedule contains recommended retention periods for the different records created and maintained by REACH in the course of their business. The schedule refers to all information regardless of the media in which it is stored.

Some of the retention periods are governed by statute. Others are guidelines following best practice. Every effort has been made to ensure that these retention periods are

compliant with the requirements of the Data Protection Act (DPA).

Managing record series using these retention guidelines will be deemed to be ‘normal processing’ under the legislation mentioned above. If records are to be kept for longer or shorter periods than laid out in this document the reasons for this need to be documented.

The schedule should be reviewed on an annual basis.

Section 1: Management of REACH

1.1 Directors					
	Record Type	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the records life**
1.1.1	**Agendas form directors meetings**	**There may be data protection issues if the meeting is dealing with confidential issues relating to staff**		**One copy should be retained with the master set of minutes. All other copies can be disposed of.**	**SECURE DISPOSAL**
1.1.2	**Minutes of directors Meetings**	**There may be data protection issues if the meeting is dealing with confidential issues relating to staff**			
	Principal Set (signed)			**PERMANENT**	**If the school is unable to store these then they should be offered to the County Archives Service.**
	Inspection Copies			**Date of meeting + 3 years**	**If the minutes contain any sensitive, personal information they must be shredded**
1.1.3	**Reports presented to the directors**	**There may be data protection issues if the report is dealing with confidential issues relating to staff**		**Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports then the reports should be kept permanently.**	**SECURE DISPOSAL or retain with the signed set of minutes**

1.1.4	Meeting papers relating to annual parents' meeting held under section 33 of the Education Act 2002	No	Education Act 2002, Section 33	Date of the meeting + a minimum of 6 years	SECURE DIPOSAL

1.2 Senior Leadership Team					
	Record Type	Data Protection Issues	Statutory Provisions	Retention Period	Action at the end of the records life
1.2.1	Log books of activity in REACH maintained by the Director of Alternative Educaton	There may be data protection issues if the log book refers to individual members of staff		Date of last entry in the book + a minimum of 6 years then review	These could be of permanent historical value and should be offered to the County Archives Service if appropriate.
1.2.2	Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies	There may be data protection issues if the minutes refers to individual pupils or members of staff		Date of the meeting + 3 years then review	SECURE DISPOSAL
1.2.3	Reports created by the director of alternative education or the Management Team	There may be data protection issues if the report refers to individual pupils or members of staff		Date of the report + 3 years then review	SECURE DISPOSAL
1.2.4	Records created by the director of alternative education and other members of staff with administrative responsibilities	There may be data protection issues if the report refers to individual pupils or members of staff		Current academic year + 6 years then review	SECURE DISPOSAL

1.2.5	Correspondence created by director of education and other members of staff with administrative responsibilities	There may be data protection issues if the report refers to individual pupils or members of staff		Date of correspondence + 3years then review	SECURE DISPOSAL
1.2.6	Professional Development Plans	Yes		Life of then plan + 6 years	SECURE DISPOSAL
1.2.7	REACH Development Plans	No		Life of the plan + 3 years	SECURE DISPOSAL

1.3 Admissions					
	Record Type	Data Protection Issues	Statutory Provisions	Retention Period	Action at the end of the records life
1.3.1	All records relating to the creation and implementation of the School Admissions Policy	No	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, school adjudicators and admission appeals panels December 2014	Life of the policy + 3 years then review	SECURE DISPOSAL
1.3.2	Admissions – if the admission is successful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, school adjudicators and admission appeals panels December 2014	Date of admission + 1 year	SECURE DISPOSAL
1.3.3	Admissions – if the appeal is unsuccessful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, school adjudicators and admission appeals panels December 2014	Resolution of case + 1 year	SECURE DISPOSAL

1.3.4	Register of Admissions	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made	REVIEW Schools may wish to consider keeping the admission register permanently as often schools receive enquiries from past pupils to confirm the dates they attended the school.
1.3.5	Admissions – Secondary Schools – Casual	Yes		Current year + 1 year	SECURE DISPOSAL
1.3.6	Proofs of address supplied by parents as part of the admissions process	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, school adjudicators and admission appeals panels December 2014	Current year + 1 year	SECURE DISPOSAL
1.3.7	Supplementary Information form including additional information such as religion, medical conditions etc.	Yes			
	For successful admissions			The information should be added to the pupil file	SECURE DISPOSAL
	For unsuccessful admissions			Until appeals process completed	SECURE DISPOSAL

1.4 Operational Administration					
	Record Type	Data Protection Issues	Statutory Provisions	Retention Period	Action at the end of the records life
1.4.1	General file series	No		Current year + 5 years then REVIEW	SECURE DISPOSAL

1.4.2	**Records relating to the creation and publication of REACH brochure or prospectus**	**No**		**Current year + 3 years**	**SECURE DISPOSAL**
1.4.3	**Records relating to the creation and distribution of circulars to staff, parents or pupils**	**No**		**Current year + 1 year**	**SECURE DISPOSAL**
1.4.4	**Newsletters and other items with a short operational use**	**No**		**Current year + 1 year**	**SECURE DISPOSAL**
1.4.5	**Visitors' Books and Signing in Sheets**	**Yes**		**Current year + 6 years then REVIEW**	**SECURE DISPOSAL**
1.4.6	**Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations**	**No**		**Current year + 6 years then REVIEW**	**SECURE DISPOSAL**

Section 2: HR Management of REACH

2.1 Recruitment					
	Record Type	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the records life**
2.1.1	**All records leading up to the appointment of a new member of staff – unsuccessful candidates**	**Yes**		**Date of appointment of successful candidate + 6 months**	**SECURE DISPOSAL**
2.1.2	**All records leading up to the appointment of a new member of staff – successful candidate**	**Yes**		**All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months**	**SECURE DISPOSAL**
2.1.3	**Pre-employment vetting information – DBS checks**	**No**	**DBS Update Service Employer Guide June 2014: keeping children safe in education. July 2015 (Statutory Guidance from Dept. of Education) Sections 73, 74**	**The school does not have to keep copies of DBS certificates. Only the reference number is required on file.**	
2.1.4	**Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure**	**Yes**		**Where possible these should be checked and a note kept of what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff's personal file**	

2.1.5	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom	Yes	An employer's guide to right to work checks [Home Office May 2015]	Where possible these documents should be added to the Staff Personal File [see below], but if they are kept separately the Home Office requires that the documents are kept for termination of Employment plus two years	

2.2 Operational Staff Management					
	Record Type	Data Protection Issues	Statutory Provisions	Retention Period	Action at the end of the records life
2.2.1	Staff Personal File	Yes	Limitation Act 1980 (section 2)	Termination of Employment + 6 years	SECURE DISPOSAL
2.2.2	Timesheets	Yes		Current year + 6 years	SECURE DISPOSAL
2.2.3	Annual appraisal/assessment records	Yes		Current year + 5 years	SECURE DISPOSAL

2.3 Management of Disciplinary & Grievance Process					
	Record Type	Data Protection Issues	Statutory Provisions	Retention Period	Action at the end of the records life

2.3.1	**Allegation of a child protection nature against a member of staff including where the allegation is unfounded**	**Yes**	**"Keeping children safe in education Statutory guidance for schools and colleges March 2015";"Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children July 2018"**	**Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned**	**SECURE DISPOSAL These records must be shredded**
2.3.3	**Disciplinary Proceedings**	**Yes**			
	Oral warning			**Date of warning + 6 months**	**SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]**
	Written warning – level 1			**Date of warning + 6 months**	
	Written warning – level 2			**Date of warning + 12 months**	
	Final warning			**Date of warning + 18 months**	
	Case not found			**If the incident is child protection related then see above otherwise dispose of at the conclusion of the case**	**SECURE DISPOSAL**

2.5 Payroll and Pensions

	Record Type	Data Protection Issues	Statutory Provisions	Retention Period	Action at the end of the records life
2.5.1	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year + 3 years	SECURE DISPOSAL
2.5.2	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL

Section 3: Financial Management of REACH

3.1 Risk Management & Insurance					
	Record Type	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the records life**
3.1.1	Employer's Liability Insurance Certificate	No		Closure of the school + 40 years	SECURE DISPOSAL

3.2 Asset Management					
	Record Type	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the records life**
3.2.1	Inventories of furniture and equipment	No		Current year + 6 years	SECURE DISPOSAL
3.2.2	Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL

3.3 Accounts & Statements including Budget Management					
	Record Type	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the records life**
3.3.1	Annual Accounts	No		Current year + 6 years	STANDARD DISPOSAL
3.3.2	Loans and grants managed by REACH	No		Date of last payment on the loan + 12 years then REVIEW	SECURE DISPOSAL
3.3.3	Student Grant applications	Yes		Current year + 3 years	SECURE DISPOSAL

3.3.4	All records relating to the creation and management of budgets including the Annual Budget statements and background papers	No		Life of the budget + 3 years	SECURE DISPOSAL
3.3.5	Invoices, receipts, order books and requisitions, delivery notices	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.6	Records relating to the collection and banking of monies	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.7	Records relating to the identification and collection of debt	No		Current financial year + 6 years	SECURE DISPOSAL

3.4 Contract Management					
	Record Type	Data Protection Issues	Statutory Provisions	Retention Period	Action at the end of the records life
3.4.1	All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on contract + 12 years	SECURE DISPOSAL
3.4.2	All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on contract + 6 years	SECURE DISPOSAL
3.4.3	Records relating to the monitoring of contracts	No		Current year + 2 years	SECURE DISPOSAL

3.5 REACH Fund					
	Record Type	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the records life**
3.5.1	**REACH fund - Cheque books**	**No**		**Current year + 6 years**	**SECURE DISPOSAL**
3.5.2	**REACH fund - Paying in books**	**No**		**Current year + 6 years**	**SECURE DISPOSAL**
3.5.3	**REACH fund - Ledger**	**No**		**Current year + 6 years**	**SECURE DISPOSAL**
3.5.4	**REACH fund - Invoices**	**No**		**Current year + 6 years**	**SECURE DISPOSAL**
3.5.5	**REACH fund – Receipts**	**No**		**Current year + 6 years**	**SECURE DISPOSAL**
3.5.6	**REACH fund – Bank statements**	**No**		**Current year + 6 years**	**SECURE DISPOSAL**
3.5.7	**REACH fund – Journey Books**	**No**		**Current year + 6 years**	**SECURE DISPOSAL**

Section 4: Property Management

4.1 Health & Safety					
	Record Type	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the records life**
4.1.1	Health and Safety Policy Statements	No		Life of policy + 3 years	SECURE DISPOSAL
4.1.2	Health and Safety Risk Assessments	No		Life of Risk assessment + 3 years	SECURE DISPOSAL
4.1.3	Records relating to accident/ injury at work	Yes		Date of incident + 12 years. In the case of serious accidents a further retention period will need to be applied	SECURE DISPOSAL
4.1.4	Accident Reporting		Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
	Adults			Date of the incident + 6 years	SECURE DISPOSAL
	Children			DOB of the child + 25 years	SECURE DISPOSAL

4.1.5	Control of Substances Hazardous to Health (COSHH)	No	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677 Regulation 11; Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18(2)	Current year + 40 years	SECURE DISPOSAL
4.1.6	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	Last action + 40 years	SECURE DISPOSAL
4.1.7	Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	No		Last action + 50 years	SECURE DISPOSAL
4.1.8	Fire precautions log books			Current year + 6 years	SECURE DISPOSAL

4.2 Property Management					
	Record Type	Data Protection Issues	Statutory Provisions	Retention Period	Action at the end of the records life
4.2.1	Leases of property leased by or to the school	No		Expiry of lease + 6 years	SECURE DISPOSAL

4.2.2	**Records relating to the letting of school premises**	**No**		**Current financial year + 6 years**	**SECURE DISPOSAL**

4.3 Maintenance					
	Record Type	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the records life**
4.3.1	**All records relating to the maintenance of REACH carried out by contractors**	**No**		**Current year + 6 years**	**SECURE DISPOSAL**
4.3.2	**All records relating to the maintenance of REACH carried out by school employees including maintenance log books**	**No**		**Current year + 6 years**	**SECURE DISPOSAL**

Section 5: Service user Management

5.1 Pupil's Educational Record					
	Record Type	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the records life**
5.1	Service users details	yes		whilst with REACH + 1 yr	information will be permanently deleted from google suite

5.1.3	**Child Protection information held on file**	**Yes**	**"Keeping children safe in education Statutory guidance for schools and colleges March 2019"; "Working together to safeguard and promote the welfare of children July 2018**	All Child protection information is passed to referring agencies. REACH keeps a record until work finishes with service users and then all information is passed to the referring agency to store.	**Permanently deleted from google Suite**

7.3 Safeguarding Lead and Team					
	Record Type	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the records life**
7.3.1	**Day Books**	**Yes**		**Current year + 2 years then review**	
7.3.2	**Reports for outside agencies – where the report has been included on the case file created by the outside agency**	**Yes**		**Whilst child is attending school and then destroy**	
7.3.3	**Referral Forms**	**Yes**		**While the referral is current**	
7.3.4	**Contact data sheets**	**Yes**		**Current year then review, if contact is no longer active then destroy**	
7.3.5	**Contact database entries**	**Yes**		**Current year then review, if contact is no longer active then destroy**	