GDPR Records Management Policy

Policy Author	Principal Business Manager/CFO
Date Last Reviewed	September 2020
Trust Key Reader	MS
Approved by Trust Board	22.10.20
Review Date	September 2022

Statement of Intent

LEAP Multi-Academy Trust is committed to maintaining the confidentiality of its data and ensuring that all records within the Trust/its Academies are only accessible by the appropriate individuals. In line with the requirements of GDPR, the Trust's Academies also have a responsibility to ensure that all records are only kept for as long as it necessary to fulfil the purpose(s) for which they were intended.

The Trust has created this policy to outline how records are stored, accessed, monitored, retained and disposed of in order to meet LEAP Trust/its Academies statutory requirements.

1. Legal Framework

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

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

1.2 This policy also has due regard to the following guidance:

- Information Records Management Society (2019) 'Information Management Toolkit for Schools'
- DfE (2018) 'Data Protection: A Toolkit for Schools'

1.3 This policy will be implemented in accordance with the following Trust policies and procedures:

- Data Protection Policy
- Freedom of Information Policy
- e-Security Policy
- Security Breach Prevention & Management Plan
- Disposal of Records Log
- Data Register

2. Responsibilities

2.1 LEAP MAT has the responsibility for maintaining its records and record-keeping systems in line with statutory requirements.

2.2 LEAP Trustees/the Board is responsible for ensuring appropriate resources are made available, on the advice of the Chief Executive and DPO to comply with the GDPR.

2.2 The Chief Executive and others, as delegated, are responsible for implementation of LEAP GDPR Policies.

2.2 Each Principal holds overall responsibility for the policy and for ensuring it is implemented correctly.

2.3 The Data Protection Officer role is to:

- assist the controller or the processor in all issues relating to the protection of personal data
- inform and advise the Board, as well as their employees, of their obligations under data protection law
- monitor compliance of LEAP MAT with all legislation in relation to data protection, including in audits, awareness-raising activities as well as training of staff involved in processing operations
- provide advice where a DPIA has been carried out and monitor its performance
- act as a contact point for requests from individuals regarding the processing of their personal data and the exercise of their rights
- cooperate with the ICO and act as a contact point for the ICO on issues relating to processing
- The organisation must involve the DPO in a timely manner. The DPO must not receive any instructions from LEAP MAT for the exercise of her/his tasks. The DPO reports directly to the Chief Executive and ELT.

2.4 The DPO is responsible for promoting compliance with this policy and reviewing the policy on an annual basis, in conjunction with each Principal.

2.5 The Chief Executive and Academy Principals are responsible for ensuring that all records are stored securely, in accordance with the retention periods outlined in this policy and are disposed of correctly.

2.6 All staff members are responsible for ensuring that any records for which they are responsible for are accurate, maintained securely and disposed of correctly, in line with the provisions of this policy.

3. Management of Student Records

3.1 Student records are specific documents that are used throughout a student's time in the education system – they are passed to each School/Academy that a student attends and includes all personal information relating to them, eg date of birth, home address, as well as their progress and achievement.

3.2 The following information is stored on the front of a student record, and will be easily accessible by key staff:

- **Forename, Surname**

3.3 An electronic student management system (SIMS) is used to store other student data and is accessible to staff; data stored includes:

- **Ethnic origin, religion and first language (if not English)**
- **Any preferred names**
- **Siblings in the Academy**
- **Emergency contact details**
- **Any allergies or other medical conditions that are important to be aware of**
- **Names of parents/carers, including their home address(es) and telephone number(s)**
- **Name of the Academy, admission number, the date of admission and the date of leaving, where appropriate**
- **Any other agency involvement, eg speech and language therapist**

3.4 The following information is also stored on SIMs and will be easily accessible to staff:

- **Admissions form (paper copies kept with data office)**
- **Details of any SEND**
- **If the student has attended a primary/other secondary school, the record of transfer**
- **Privacy notice/Fair Processing notice – only the most recent notice will be included**
- **Assessment Point reports to parents/carers**
- **Notes relating to major incidents and accidents involving the student**
- **Any information about an education, health and care (EHC) plan and support offered in relation to the EHC plan**
- **Any information relating to exclusions**
- **Any correspondence with parents/carers or external agencies relating to major issues**
- **Notes indicating that records of complaints made by parents/carers or the student are held**

3.5 The following information is subject to shorter retention periods and therefore, will be stored separately:

- **Absence notes**
- **Parental and, where appropriate, student consent forms for educational visits, photographs and videos, etc.**

3.6 For security purposes safeguarding information including disclosures and reports relating to child protection are stored on CPOMs which has restricted access; if any paper copies are held then they are kept in a securely locked filing cabinet.

3.7 Hard copies of complaints made by parents/carers or students are stored in a file centrally – a note indicating this is marked on the student's file.

3.8 Actual copies of accident and incident information are stored separately on the Academy's secure file server which has restricted access and held in line with the retention periods outlined in this policy. An additional copy may be placed in the student's file in the event of a major accident or incident.

3.9 The Academy will ensure that no student records are altered or amended before transferring them to the next School/Academy that the student will attend. (NB records will be anonymised to remove other student names and also staff names as appropriate)

3.10 The only exception to the above is if any records placed on the student's file have a shorter retention period and may need to be removed. In such cases, the Academy Principal responsible for disposing records, will remove these records.

3.11 Electronic records relating to a student's record will also be transferred to the student's next School/Academy. Section 11 of this policy outlines how electronic records will be transferred.

3.12 <u>If any student attends the Academy until statutory school leaving age, the Academy will keep the student's records until the student reaches the age of 25 years.</u>

3.13 The Academy will, wherever possible, avoid sending a student record by post. Where a student record must be sent by post, it will be sent by **<u>registered post</u>** with an accompany list of the files included. **The School/Academy 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 relevant LEAP Academy.**

4. Retention of Student Records and Other Student Related Information

4.1 The table overleaf outlines the Trust's retention periods for individual student records and the action that will be taken after the retention period, in line with any requirements.

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

4.3 Before deletion, it must be determined that all legal and business requirements have expired, and that there is no related litigation or investigation. Records must be securely deleted in accordance with the school's security policy. Processes must be in place to ensure that all backups and copies are included in the deletion process.

Type of file	Retention period	Action taken after retention period ends
Personal Identifiers, Contacts and Personal Characteristics		
Images used in displays in schools	Whilst the student is at school + 1 year	Securely disposed of
Images used for marketing purposes, or other	Current year + 1 year	Securely disposed of
Biometric data	Whilst the student remains at school, plus one month	Securely disposed of
Admissions		
Register of admissions	Whilst the student remains at the school, plus one year	Information is reviewed and the register may be kept permanently
Admissions appeals	Whilst the student remains at school, plus five years	Securely disposed of
Secondary school admissions	Whilst the student remains at the school, plus one year	Securely disposed of
Proof of address (supplied as part of the admissions process)	Whilst the student remains at the school, plus one year	Securely disposed of
Supplementary information submitted, including religious and medical information etc. (where the admission was successful)	Whilst the student remains at the school, plus one year	Securely disposed of
Supplementary information submitted, including religious and medical information etc. (where the admission was not successful)	Whilst the student remains at the school, plus five years	Securely disposed of
Students' Educational Records		
Students' educational records	25 years after the student's date of birth, with their personal data removed	Securely disposed of
Public examination results	Added to the student's record and transferred to next school Certificates are held whilst the student is at school, plus five years	Returned to the examination board
Child protection records held in a separate file	25 years after the student's date of birth	Securely disposed of – shredded

Type of File	Retention period	Action taken after retention period ends
Medical Information and Administration		
Permission slips	For the duration of the period that medication is given, plus one month	Securely disposed of
Medical incidents that have a behavioural or safeguarding influence	Added to the student's record and transferred to the next school 25 years after the student's date of birth	Securely disposed of
SEND		
SEND files, reviews and individual education plans	25 years after the student's date of birth (as stated on the student's record)	Information is reviewed and the file may be kept for longer than necessary if it is required for the school to defend themselves in a 'failure to provide sufficient education' case
An EHC plan maintained under section 37 of the Children and Families Act 2014 (and any amendments to the statement or plan)	25 years after the student's date of birth (as stated on the student's record)	Securely disposed of, unless it is subject to a legal hold
Information and advice provided to parents regarding SEND	25 years after the student's date of birth (as stated on the student's record)	Securely disposed of, unless it is subject to a legal hold
Accessibility strategy	25 years after the student's date of birth (as stated on the student's record)	Securely disposed of, unless it is subject to a legal hold
Curriculum Management		
External examination papers	Until the appeals/validation process has been completed	Securely disposed of
Published Admission Number (PAN) reports	Current academic year, plus six years	Securely disposed of
Valued added and contextual data	Current academic year, plus six years	Securely disposed of
Self-evaluation forms	Current academic year, plus six years	Securely disposed of
Student's work	Returned to student s at the end of the academic year, or retained for the current academic year, plus one year	Securely disposed of

Type of File	Retention period	Action taken after retention period ends
Visits/Extra-Curricular Activities		
Field file – information taken on school trips	Until the conclusion of the trip, plus one month Where a minor incident occurs, field files are added to the core system as appropriate	Securely disposed of
Financial information relating to school trips	Whilst the student remains at school, plus one year	Securely disposed of
Parental consent forms for school trips where no major incident occurred	Until the conclusion of the trip +1 month	Securely disposed of
Parental consent forms for school trips where a major incident occurred	25 years after the student's date of birth on the student's record (permission slips of all students on the trip will also be held to show that the rules had been followed for all students)	Securely disposed of
Catering and Free School Meal Management		
Meal administration (Catering company)	Whilst the student is at school, plus one year	Securely disposed of
Meal eligibility	25 years after the student's date of birth on the student's record	Securely disposed of

5. Retention of Staff Records

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

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

Type of File	Retention period	Action taken after retention period ends
Operational		
Staff members' personal file	Termination of employment, plus six years	Securely disposed of
Timesheets	Current academic year, plus six years	Securely disposed of
Annual appraisal and assessment records	Current academic year, plus five years	Securely disposed of

Type of File	Retention period	Action taken after retention period ends
Recruitment		
Records relating to the appointment of a new Principal	Date of appointment, plus six years	Securely disposed of
Records relating to the appointment of new members of staff (unsuccessful candidates)	Date of appointment of successful candidate, plus six months	Securely disposed of
Records relating to the appointment of new members of staff (successful candidates)	Relevant information added to the member of staff's personal file and other information retained for six months	Securely disposed of
DBS certificates	Up to six months	Securely disposed of
Proof of identify as part of the enhanced DBS check	After identity has been proven	Reviewed and a note kept of what was seen and what has been checked – if it is necessary to keep a copy this will be placed on the staff member's personal file, if not, securely disposed of
Evidence of right to work in the UK	Added to staff personal file or, if kept separately, termination of employment, plus no longer than two years	Securely disposed of
Disciplinary and Grievance Procedures		
Child protection allegations, including where the allegation is unproven	Added to staff personal file, and until the individual's normal retirement age, or 10 years from the date of the allegation – whichever is longer. If allegations are malicious, they are removed from personal files	Reviewed and securely disposed of – shredded
Oral warnings	Date of warning, plus six months	Securely disposed of – if placed on staff personal file, removed from file
Written warning – level 1	Date of warning, plus six months	Securely disposed of – if placed on staff personal file, removed from file
Written warning – level 2	Date of warning, plus 12 months	Securely disposed of – if placed on staff personal file, removed from file
Final warning	Date of warning, plus 18 months	Securely disposed of – if placed on staff personal file, removed from file
Records relating to unproven incidents	Conclusion of the case, unless the incident is child protection related and is disposed of as above	Securely disposed of

6. Retention of Senior Leadership and Management Records

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

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

Type of File	Retention period	Action taken after retention period ends
Governing Board		
Agendas for governing board meetings	One copy alongside the original set of minutes – all others disposed of without retention	Securely disposed of
Original, signed copies of the minutes of governing board meetings	Permanent	
Inspection copies of the minutes of governing board meetings	Date of meeting, plus three years	Shredded if they contain any sensitive and personal information
Reports presented to the governing board	Minimum of six years, unless they refer to individual reports – these are kept permanently	Securely disposed of or, if they refer to individual reports, retained with the signed, original copy of minutes
Instruments of government, including articles of association	Permanent	
Trusts and endowments managed by the governing board	Permanent	
Action plans created and administered by the governing board	Duration of the action plan, plus three years	Securely disposed of
Policy documents created and administered by the governing board	Duration of the policy, plus three years	Securely disposed of
Records relating to complaints dealt with by the governing board	Date of the resolution of the complaint, plus a minimum of six years	Reviewed for further retention in case of contentious disputes, then securely disposed of
Annual reports created under the requirements of The Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002	Date of report, plus 10 years	Securely disposed of
Proposals concerning changing the status of the school	Date proposal accepted or declined, plus three years	Securely disposed of

Type of File	Retention period	Action taken after retention period ends
Principal and Senior Leadership Team (SLT)		
Minutes of SLT meetings and the meetings of other internal administrative bodies	Date of the meeting, plus three years	Reviewed and securely disposed of
Reports created by the Principal or SLT	Date of the report, plus a minimum of three years	Reviewed and securely disposed of
Records created by the Principal, Vice Principal, heads of year and other members of staff with administrative responsibilities	Current academic year, plus six years	Reviewed and securely disposed of
Correspondence created by the Principal, Vice Principal, heads of year and other members of staff with administrative responsibilities	Date of correspondence, plus three years	Reviewed and securely disposed of
Professional development plan	Duration of the plan, plus six years	Securely disposed of
School development plan	Duration of the plan, plus three years	Securely disposed of

7. Retention of Health and Safety Records

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

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

Type of File	Retention period	Action taken after retention period ends
Health & Safety		
Health and safety policy statements	Duration of policy, plus three years	Securely disposed of
Health and safety risk assessments	Duration of risk assessment, plus three years	Securely disposed of
Records relating to accidents and injuries at work	Date of incident, plus 12 years. In the case of serious accidents, a retention period of 15 years is applied	Securely disposed of
Accident reporting – adults	Date of the incident, plus six years	Securely disposed of

Type of File	Retention period	Action taken after retention period ends
Health & Safety		
Accident reporting – students	25 years after the student's date of birth, on the student's record	Securely disposed of
Control of substances hazardous to health	Current academic year, plus 40 years	Securely disposed of
Information relating to areas where employees and persons are likely to come into contact with asbestos	Date of last action, plus 40 years	Securely disposed of
Information relating to areas where employees and persons are likely to come into contact with radiation	Date of last action, plus 50 years	Securely disposed of
Fire precautions logbooks	Current academic year, plus six years	Securely disposed of

8. Retention of Financial Records

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

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

Type of File	Retention period	Action taken after retention period ends
Payroll Pensions		
Maternity pay records	Current academic year, plus three years	Securely disposed of
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Current academic year, plus six years	Securely disposed of
Risk Management and Insurance		
Employer's liability insurance certificate	Closure of the school, plus 40 years	Securely disposed of
Asset Management		
Inventories of furniture and equipment	Current academic year, plus six years	Securely disposed of
Burglary, theft and vandalism report forms	Current academic year, plus six years	Securely disposed of

Type of File	Retention period	Action taken after retention period ends
Accounts and Statements Including Budget Management		
Annual accounts	Current academic year, plus six years	Disposed of against common standards
Loans and grants managed by the school	Date of last payment, plus 12 years	Information is reviewed then securely disposed of
All records relating to the creation and management of budgets	Duration of the budget, plus three years	Securely disposed of
Invoices, receipts, order books, requisitions and delivery notices	Current financial year, plus six years	Securely disposed of
Records relating to the collection and banking of monies	Current financial year, plus six years	Securely disposed of
Records relating to the identification and collection of debt	Current financial year, plus six years	Securely disposed of
Contract Management		
All records relating to the management of contracts under seal	Last payment on the contract, plus 12 years	Securely disposed of
All records relating to the management of contracts under signature	Last payment on the contract, plus six years	Securely disposed of
All records relating to the monitoring of contracts	Current academic year, plus two years	Securely disposed of
School Fund		
Cheque books, paying in books, ledgers, invoices, receipts, bank statements and journey books	Current academic year, plus six years	Securely disposed of
School Meals		
Free school meals registers	Current academic year, plus six years	Securely disposed of
School meals registers	Current academic year, plus three years	Securely disposed of
School meals summary sheets	Current academic year, plus three years	Securely disposed of

9. Retention of Other Academy Records

9.1 The table below outlines the Trust's retention periods for any other records held by its Academies, and the action that will be taken after the retention period, in line with any requirements.

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

Type of File	Retention period	Action taken after retention period ends
Property Management		
Title deeds of properties belonging to the school	Permanent	Transferred to new owners if the building is leased or sold
Plans of property belonging to the school	For as long as the building belongs to the school	Transferred to new owners if the building is leased or sold
Leases of property leased by or to the school	Expiry of lease, plus six years	Securely disposed of
Records relating to the letting of school premises	Current financial year, plus six years	Securely disposed of
Maintenance		
All records relating to the maintenance of the school carried out by contractors	Current academic year, plus six years	Securely disposed of
All records relating to the maintenance of the school carried out by school employees	Current academic year, plus six years	Securely disposed of
Operational administration		
General file series	Current academic year, plus five years	Reviewed and securely disposed of
Records relating to the creation and publication of the school brochure and/or prospectus	Current academic year, plus three years	Disposed of against common standards
Records relating to the creation and distribution of circulars to staff, parents or students	Current academic year, plus one year	Disposed of against common standards
Newsletters and other items with short operational use	Current academic year plus one year	Disposed of against common standards
Visitors' books and signing-in sheets	Current academic year, plus six years	Reviewed then securely disposed of
Records relating to the creation and management of parent-teacher associations and/or old student associations	Current academic year, plus six years	Reviewed then securely disposed of
CCTV records	Maximum Six months	Securely disposed of

10. Identifying Information

10.1 Under the GDPR, all individuals have the right to data minimisation and data protection by design and default – as the Data Controller, the Academy ensures appropriate measures are in place in order for individuals to exercise this right.

10.2 Wherever possible, the Academy uses pseudonymisation, also known as the 'blurring technique' to reduce risk of identification.

10.3 Once an individual has left the Academy, if identifiers such as names and dates of birth are no longer required, these are removed or less specific personal data is used, eg the month of birth rather than specific date – the data is blurred slightly.

10.4 Where data is required to be retained over time, eg attendance data, the Academy removes any personal data not required and keeps only the data needed – in this example, the statistics of attendance rather than personal information.

11. Storing and Protecting Information

11.1 The DPO will undertake a risk analysis to identify which records are vital to Academy management and these records will be stored in the most secure manner.

11.2 The ICT Managers shall maintain a disaster recovery protocol for the restoration of data and services.

11.3 Where possible, backed-up information will be stored off the Academy premises.

11.4 **Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access.**

11.5 **Confidential paper records are not left unattended or in clear view when held in a location with general access.**

11.6 Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed-up off-site.

11.7 USBs/portable hard drives are not used to hold personal information unless they are password-protected and fully encrypted and staff have specific permission from the Chief Executive to have such a device.

11.8 **All electronic devices are password-protected** to protect the information on the device in case of theft.

11.9 Where possible, the Academy enables electronic devices to allow the remote blocking or deletion of data in case of theft.

11.10 When working off-site, **staff should log in via the virtual desktop/Academy Office 365 account** to ensure no student/staffs' personal data is held on personal computers/laptops/tablets etc.

11.11 All members of staff are provided with their **own secure login and password**, and every computer regularly prompts users to change their password.

11.12 **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.

11.13 **Circular emails to parents/carers are sent blind carbon copy (bcc)**, so email addresses are not disclosed to other recipients. This should also be the case for circular emails to a variety of organisations where recipients do not know each other/have not shared email contacts.

11.14 When sending confidential information by fax, members of staff always check that the recipient is correct before sending.

11.15 **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, eg keeping devices under lock and key. **The person taking the information from Academy premises accepts full responsibility for the security of the data.**

11.16 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.**

11.17 **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.

11.18 Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the Academy containing sensitive information are supervised at all times.

11.19 **The physical security of Trust buildings and storage systems, and access to them, is reviewed termly by the site manager in conjunction with the DPO**.

11.20 The Trust takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

11.21 The DPO is responsible for continuity and making sure recovery measures are in place to ensure the security of protected data.

11.22 Any damage to, or theft of, data will be managed in accordance with the Trust's Security Breach Management Plan.

12. Assessing Information

12.1 All Trust Academies are transparent with data subjects, the information held and how it can be processed.

12.2 All members of staff, parents/carers of registered students and other users of each Academy, eg visitors and third-party clubs, are entitled to:

- **Know what information the Academy 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 Academy is doing to comply with its obligations under the GDPR.**

12.3 All members of staff, parents/carers of registered students and other users of the Academy and its facilities have the right, under the GDPR, to access certain personal data being held about them or their child.

12.4 Personal information can be shared with students 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/carers.

12.5 Students 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.

12.6 Each Academy will adhere to the provisions outlined in the Trust's Data Protection Policy when responding to requests seeking access to personal information.

13. Digital Continuity Statement

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

13.2 The DPO will identify any digital data that will need to be named as part of a digital continuity statement.

13.3 The data will be archived to dedicated files on the Academy's server, which are password-protected – this will be backed-up in accordance with Section 11 of this policy.

13.4 Memory sticks will never be used to store digital data, subject to a digital continuity statement.

13.5 The IT department will review new and existing storage methods annually and, where appropriate, add them to the digital continuity statement.

13.6 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.

14. Information Audit

14.1 The Trust conducts information audits on an annual basis against all information held by each Academy to evaluate the information each Academy is holding, receiving and using, and to ensure that this is correctly managed in accordance with the GDPR. This includes the following information:

- Paper documents and records
- Electronic documents and records
- Databases
- Microfilm or microfiche
- Sound recordings
- Video and photographic records
- Hybrid files containing both paper and electronic information.

14.2 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.

14.3 The DPO is responsible for completing the information audit. The information audit will include the following:

- The Academy's data needs
- The information needed to meet those needs
- The format in which data is stored
- How long data needs to be kept for
- Vital records status and any protective marking
- Who is responsible for maintaining the original document

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

14.5 Once it has been confirmed that the information is accurate, the DPO will record all details on the Academy's Data Register.

14.6 The information displayed on the Data Register will be shared with each Principal to gain their approval.

15. Disposal of Data

15.1 Where disposal of information is outlined as standard disposal, this will be re-cycled appropriate to the form of the information, eg paper re-cycling, electronic re-cycling.

15.2 Where disposal of information is outlined as secure disposal, this will be shredded or pulped and electronic information will be scrubbed clean and, where possible, cut. The DPO will keep a record of all files that have been destroyed.

15.3 Where the disposal action is indicated as reviewed before it is disposed, the DPO will review the information against its administrative value – if the information should be kept for administrative value the DPO will keep a record of this.

15.4 If, after the review, it is determined that the data should be disposed of it will be destroyed in accordance with the disposal action outlined in this policy.

15.5 Where information has been kept for administrative purposes, the DPO will review the information again after three years and conduct the same process. If it needs to be destroyed, it will be destroyed in accordance with the disposal action outlined in this policy. If any information is kept, the information will be reviewed every three subsequent years.

15.6 Where information must be kept permanently, this information is exempt from the normal review procedures.

16. Monitoring and Review

16.1 This policy will be reviewed on an annual basis by the DPO in conjunction with each Principal – the next scheduled review date for this policy is September 2022.

16.2 Any changes made to this policy will be communicated to all members of staff and the Board of Trustees.