GDPR-Document Retention Management Policy

Document Retention Management Policy

April 2018

Document Version: V6
Review Date: May 2026

Owner: Director of Operations

Version 6
Last updated: 10th May 2018
Next Review Date : May 2019

Document History

Date	Author	Version Number	Summary of changes
25 Mar 2018	Director of Operations	V1	New policy linked to Data Protection Strategy – Draft format
28th March 2018	Director or Operations	V2	Revised Policy and Process & amendments following comments from CEO
16th April 2018	Director or Operations	V3	Reviewed and updated with Director of IT
24TH April 2018	Director of Operations	V4	Tweaked following operational review
3rd May 2018	Director of Operations	V5	Removed signature requirement
10th May 2018	Director of Operations	V6	Removed sentence in section 3.12 which was not required and updated the Governance table to accurately reflect retention of governance documents.
September 2024			Policy Review – No updates Necessary

Contents:

Statement of intent

Discovery Schools Academies Trust (DSAT), further referred to as **DSAT** or **the organisation** is committed to maintaining the confidentiality of its information and ensuring that all records within the organisation are only accessible by the appropriate individuals. In line with the requirements of the General Data Protection Regulation (GDPR), DSAT also has a responsibility to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were intended.

DSAT has created this policy as part of the Data Protection Strategy to outline how records are stored, accessed, monitored, retained and disposed of, in order to meet the Organisations statutory requirements.

This document complies with the requirements set out in the GDPR, which will come into effect on 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

The retention periods outlined in this policy are good practice guidelines only, and schools should ensure that they consider requirements specific to their school when implementing these timeframes. The tables for retention periods are based on information provided by the Information Records Management Society (IRMS) and are not an exhaustive list of records that may be kept by schools. Where the IRMS has not provided guidance for disposal methods or retention periods, good practice recommendations have been provided in **yellow and bold**.

1. Legal framework

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

- General Data Protection Regulation (2016)
- 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 'Information Management Toolkit for Schools' 2016

1.3. This policy will be implemented in accordance with the Data Protection Strategy and following trust policies and procedures:

- **ICT Acceptable Use Policy**
- **Data Security Incident Management Policy**
- **Freedom of Information Policy**
- **CCTV Policy**
- **School Workforce Privacy Notice**
- **Parent/carer Privacy Notice**
- **Governor Privacy Notice**

2. Responsibilities

2.1. DSAT has a responsibility for maintaining its records and record-keeping systems in line with statutory requirements.

2.2. The **CEO** holds overall responsibility for this policy and for ensuring it is implemented correctly.

2.3. The **Director of Operations** is responsible for the management of records at **Discovery Schools Academies Trust** and **Local Data Protection Representatives** are responsible for the management of records in schools.

2.4. The **DPO** is responsible for promoting compliance with this policy and reviewing the policy on an **annual** basis, in conjunction with the **trust executive team**.

2.5. The **DPO** is responsible via carrying out termly audits, 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 pupil records

3.1. Pupil records are specific documents that are used throughout a pupil's time in the education system – they are passed to each school that a pupil attends and includes all personal information relating to them, e.g. date of birth, home address, as well as their progress and achievement.

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

- Forename, surname, gender and date of birth
- Unique pupil number - UPN
- Note of the date when the file was opened
- Note of the date when the file was closed, if appropriate

3.3. The following information is stored **inside the front cover** of a pupil record, and will be easily accessible. Where possible use your MIS to manage this data but use the inside cover for staff who don't have appropriate access to the MIS.

- Ethnic origin, religion and first language (if not English)
- Any preferred names
- Position in their family, e.g. eldest sibling
- Emergency contact details and the name of the pupil's doctor
- Any allergies or other medical conditions that are important to be aware of
- Names of parents, including their home address(es) and telephone number(s)
- Name of the school, admission number, the date of admission and the date of leaving, where appropriate
- Any other agency involvement, e.g. speech and language therapist.

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

- Admissions form
- Details of any SEND
- If the pupil has attended an early years setting, the record of transfer
- Privacy Notice – only the most recent notice will be included
- Annual written reports to parents
- Hard copy 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 EHC plan
- Any information relating to exclusions (fixed or permanent)secondary
- 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

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

- Absence notes

- Parental and, where appropriate, pupil consent forms for educational visits, photographs and videos, etc.
- Correspondence with parents about minor issues, e.g. behaviour

3.6. Hard copies of disclosures and reports relating to child protection are stored in a sealed envelope, in a securely locked filing cabinet in the **head teachers** office - a note indicating this, is marked on the pupil's file.

3.7. Actual copies of disclosures and reports are stored separately on the school's CPoms systems and held in line with the retention periods outlined in this policy – a note indicating this, is marked on the pupil's file. An additional copy may be placed in the pupil's file in the event of a major accident or incident.

3.8. Hard copies of complaints made by parents or pupils are stored in a secure file in the **school office** – a note indicating this, is marked on the pupil's file.

3.9. Actual copies of accident and incident information are stored separately on the school's management information system and held in line with the retention periods outlined in this policy – a note indicating this is marked on the pupil's file. An additional copy may be placed in the pupil's file in the event of a major accident or incident.

3.10. The school will ensure that no pupil records are altered or amended before transferring them to the next school that the pupil will attend.

3.11. 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, **the Local Data Protection Representative** (LDPR) responsible for disposing records, will remove these records.

3.12. Electronic records relating to a pupil's record will also be transferred to the pupils' next school.

3.13. The school will, wherever possible, avoid sending a pupil record by post. Where a pupil record must be sent by post, it will be sent by registered post, with an accompanying list of the files included. The school it is sent to is required to sign a copy of the list to indicate that they have received the files and return this to the school.

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

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

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

Type of file	Data Protection Issues	Retention period	Action taken after retention period ends
Admissions			
Register of admissions	Yes	Three years after the date on which the entry was made	Information is reviewed and the register may be kept open permanently
Proof of address (*supplied as part of the admissions process*)	Yes	The current academic year, plus one year	Securely disposed of
Supplementary information submitted, including religious and medical information etc. (where the admission was successful)	Yes	Added to the pupil's record	Securely disposed of
Supplementary information submitted, including religious and medical information etc. (where the admission was not successful)	Yes	Until the appeals process has been completed	Securely disposed of
Pupils' educational records			
Pupils' educational records	Yes	Whilst the pupil remains at the school	Transferred to the next destination – if this is an independent school, home-schooling or outside of the UK, the file will be kept by the LA and retained for the statutory period
Internal examination results (SAT's)	Yes	Added to the pupil's record	**Securely disposed of**
Child protection information held on a pupil's record	Yes	Stored in a sealed envelope for the same length of time as the pupil's record	Securely disposed of – MUST be shredded
Child protection records held in a separate file e.g. Safeguarding files	Yes	25 years after the pupil's date of birth	Securely disposed of – MUST be shredded
Attendance			
Attendance registers	Yes	Last date of entry on to the register, plus three years	Securely disposed of
Letters authorising absence	Yes – if it refers to individuals	Current academic year, plus two years	Securely disposed of
SEND			
SEND files, reviews and individual education plans	Yes	25 years after the pupil's date of birth (as stated on the pupil's record)	Information is reviewed and the file may be kept for longer than necessary if it is required for the school to defend themselves in a 'failure to provide sufficient education' case

Statement of SEN maintained under section 324 of the Education Act 1996 or an EHC plan maintained under section 37 of the Children and Families Act 2014 (and any amendments to the statement or plan)	Yes	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
Information and advice provided to parents regarding SEND	Yes	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
Accessibility strategy	Yes	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
Curriculum management			
SATs results	Yes	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of
Examination papers	Yes	Until the appeals/validation process has been completed	Securely disposed of
Published Admission Number (PAN) reports	Yes	Current academic year, plus six years	Securely disposed of
Valued added and contextual data	Yes	Current academic year, plus six years	Securely disposed of
Self-evaluation forms	Yes	Current academic year, plus six years	Securely disposed of
Pupils' work	No	Returned to pupils at the end of the academic year, or retained for the current academic year, plus one year	Securely disposed of
Extra-curricular activities			
Parental consent forms for school trips where ***no major*** incident occurred	Yes	Until the conclusion of the trip	Up to 22 years after the pupil's date of birth if storage not an issue.
Parental consent forms for school trips where a major incident occurred	Yes	25 years after the pupil's date of birth on the pupil's record (permission slips of all pupils on the trip will also be held to show that the rules had been followed for all pupils)	**Securely disposed of**

Walking bus registers	Yes	Three years from the date of the register being taken	Securely disposed of
Family liaison officers and home-school liaison assistants			
Day books	Yes	Current academic year, plus two years	Reviewed and destroyed if no longer required
Reports for outside agencies	Yes	Duration of the pupil's time at school	**Securely disposed of**
Referral forms	Yes	Whilst the referral is current	**Securely disposed of**
Contact data sheets	Yes	Current academic year	Reviewed and destroyed if no longer active
Contact database entries	Yes	Current academic year	Reviewed and destroyed if no longer required
Group registers	Yes	Current academic year, plus two years	**Securely disposed of**

5. Retention of staff records

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

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

Type of file	Data Protection Issues	Retention period	Action taken after retention period ends
Operational			
Staff members' personal file	Yes	Termination of employment, plus six full academic years	Securely disposed of
Timesheets	Yes	Current academic year, plus six years	Securely disposed of
Annual appraisal and assessment records	Yes	Current academic year, plus five years	Securely disposed of
Recruitment			
TRUST - Records relating to the appointment of a senior leader /management	Yes	Date of appointment, plus six years	Securely disposed of
TRUST - Records relating to the appointment of new members of staff (unsuccessful candidates)	Yes	Date of appointment of successful candidate, plus six months	Securely disposed of
TRUST - Records relating to the appointment of new members of staff (successful candidates)	Yes	Relevant information added to the member of staff's personal file and other information retained for six months	Securely disposed of
SCHOOLS - Records relating to the appointment of a new headteacher	Yes	Date of appointment, plus six years	Securely disposed of
SCHOOLS -Records relating to the appointment of new members of staff (unsuccessful candidates)	Yes	Date of appointment of successful candidate, plus six months	Securely disposed of
SCHOOLS - Records relating to the appointment of new members of staff (successful candidates)	Yes	Relevant information added to the member of staff's personal file and other information retained for six months	Securely disposed of
DBS certificates	Yes	DBS certificates DO NOT need to be retained on file. If they are they should not be retained for more than six months	**Securely disposed of**
Proof of identify as part of the enhanced DBS check	Yes	**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	Yes	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 – MUS be shredded
Oral warnings	Yes	Date of warning, plus six months	Securely disposed of – if placed on staff personal file, removed from file
Written warning – level 1	Yes	Date of warning, plus 6 months	Securely disposed of – if placed on staff personal file, removed from file
Written warning – level 2	Yes	Date of warning, plus 12 months	Securely disposed of – if placed on staff personal file, removed from file
Final warning	Yes	Date of warning, plus 18 months	Securely disposed of – if placed on staff personal file, removed from file
Records relating to unproven incidents	Yes	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 school's retention periods for senior leadership and management records, and the action that will be taken after the retention period, in line with any requirements.

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

Type of file	Data Protection Issues	Retention period	Action taken after retention period ends
Governing board			
Agendas for governing board meetings	Only if dealing with confidential matters relating to staff	**One copy Permanent**	Securely disposed of
Original, signed copies of the minutes of governing board meetings	Only if dealing with confidential matters relating to staff	**One copy permanent**	If unable to store, **local authority archive service should be investigated – refer matter to Trust**
Inspection copies of the minutes of governing board meetings	Only if dealing with confidential matters relating to staff	Date of meeting, plus three years	Shredded if they contain any sensitive and personal information
Reports presented to the governing board	Only if dealing with confidential matters relating to staff	**One copy permanent**	Securely disposed of or, if they refer to individual reports, retained with the signed, original copy of minutes
Trusts and endowments managed by the trustees	No	Permanent	Retained in the school whilst it remains open, If unable to store, **local authority archive service should be investigated – refer matter to Trust**
Action plans created and administered by the governing board	No	Duration of the action plan, plus three years	Securely disposed of
Records relating to complaints dealt with by the governing board	No	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
Principal and senior leadership team (SLT)			
Log books of activity in the school maintained by the Headteacher	May be issues if logs refer to individual staff or pupils	Date of last entry, plus a minimum of six years	Retained in the school whilst it remains open, If unable to store, **local authority archive service should be investigated – refer matter to Trust**
Minutes of SLT meetings and the meetings of other internal administrative bodies	May be issues if minutes refer to individual staff or pupils	Date of the meeting, plus three years	Reviewed and securely disposed of
Reports created by the headteacher or SLT	May be issues if minutes refer to individual staff or pupils	Date of the report, plus a minimum of three years	Reviewed and securely disposed of

Records created by the headteachers, deputy assistant heads and other members of staff with administrative responsibilities	May be issues if minutes refer to individual staff or pupils	Current academic year, plus six years	Reviewed and securely disposed of
Correspondence created by the headteacher, deputy/assistant heads and other members of staff with administrative responsibilities	May be issues if minutes refer to individual staff or pupils	Date of correspondence, plus three years	Reviewed and securely disposed of
Professional development plan	Yes	Duration of the plan, plus six years	Securely disposed of
School development plan	No	Duration of the plan, plus three years	Securely disposed of

7. Retention of health and safety records

7.1. The table below outlines the school'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	Data Protection Issues	Retention period	Action taken after retention period ends
Health and safety			
Health and safety policy statements	No	Duration of policy, plus three years	Securely disposed of
Health and safety risk assessments	No	Duration of risk assessment, plus three years	Securely disposed of
Records relating to accidents and injuries at work	Yes	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	Yes	Date of the incident, plus six years	Securely disposed of
Accident reporting – pupils	Yes	25 years after the pupil's date of birth, on the pupil's record	Securely disposed of

Control of substances hazardous to health	No	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	No	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	No	Date of last action, plus 50 years	Securely disposed of
Fire precautions log books	No	Current academic year, plus six years	Securely disposed of

8. Retention of financial records

8.1. The table below outlines the school'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	Data Protection Issues	Retention period	Action taken after retention period ends
Payroll pensions			
Maternity pay records	Yes	Current academic year, plus three years	Securely disposed of
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes	Current academic year, plus six years	Securely disposed of
Risk management and insurance			
Employer's liability insurance certificate	No	Closure of the school, plus 40 years	Securely disposed of
Asset management			
Inventories of furniture and equipment	No	Current academic year, plus six years	Securely disposed of
Burglary, theft and vandalism report forms	No	Current academic year, plus six years	Securely disposed of
Accounts and statements including budget management			
Annual accounts	No	Current academic year, plus six years	Disposed of against common standards

Loans and grants managed by the school	No	Date of last payment, plus 12 years	Information is reviewed then securely disposed of
All records relating to the creation and management of budgets	No	Duration of the budget, plus three years	Securely disposed of
Invoices, receipts, order books, requisitions and delivery notices	No	Current financial year, plus six years	Securely disposed of
Records relating to the collection and banking of monies	No	Current financial year, plus six years	Securely disposed of
Records relating to the identification and collection of debt	No	Current financial year, plus six years	Securely disposed of
Contract management			
All records relating to the management of contracts under seal	No	Last payment on the contract, plus 12 years	Securely disposed of
All records relating to the management of contracts under signature	No	Last payment on the contract, plus six years	Securely disposed of
All records relating to the monitoring of contracts	No	Current academic year, plus two years	Securely disposed of
School fund			
Cheque books, paying in books, ledgers, invoices, receipts, bank statements and journey books	No	Current academic year, plus six years	Securely disposed of
School meals			
Free school meals registers	Yes	Current academic year, plus six years	Securely disposed of
School meals registers	Yes	Current academic year, plus three years	Securely disposed of
School meals summary sheets	No	Current academic year, plus three years	Securely disposed of

9. Retention of other school records

9.1. The table below outlines the school's retention periods for any other records held by the school, 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	Data Protection Issues	Retention period	Action taken after retention period ends
Property management			
Title deeds of properties belonging to the school	No	Permanent	**Transferred to new owners if the building is leased or sold**
Plans of property belonging to the school	No	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	No	Expiry of lease, plus six years	Securely disposed of
Records relating to the letting of school premises	No	Current financial year, plus six years	Securely disposed of
Maintenance			
All records relating to the maintenance of the school carried out by contractors	No	Current academic year, plus six years	Securely disposed of
All records relating to the maintenance of the school carried out by school employees	No	Current academic year, plus six years	Securely disposed of
Operational administration			
General file series	No	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	No	Current academic year, plus three years	Disposed of against common standards
Records relating to the creation and distribution of circulars to staff, parents or pupils	No	Current academic year, plus one year	Disposed of against common standards
Newsletters and other items with short operational use	No	Current academic year plus one year	Disposed of against common standards
Visitors' books and signing-in sheets	Yes	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 pupil associations	No	Current academic year, plus six years	Reviewed then securely disposed of

CCTV recordings	Yes	Up to 30 days maximum unless	Over written by system

10. Storing and protecting information

10.1. The **Director of Operations** will undertake a risk analysis to identify which records are vital to school management and these records will be stored in the most secure manner.

10.2. The **IT team** will conduct a back-up of digital information on a regular basis to ensure that all data can still be accessed in the event of a security breach, e.g. a virus, and prevent any loss or theft of data.

10.3. Where possible, backed-up information will be stored off the school premises, using a central back-up service operated by the Trust.

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

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

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

10.7. Where data is saved on removable storage or a portable device, the device is kept in a locked and fireproof filing cabinet, drawer or safe when not in use.

10.8. Pen Drive (memory sticks) will not be used to hold personal information unless they are password-protected and fully encrypted

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

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

10.11. Staff and governors do not use their personal laptops or computers for school purposes.

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

10.13. 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.

10.14. Circular emails to parents are used they are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients OR 3rd party communication providers are used.

10.15. In the infrequent case of sending confidential information by fax, staff will always check that the recipient details are correct and that they are aware of incoming communication before it is sent.

10.16. 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 school premises accepts full responsibility for the security of the data.

10.17. Before sharing data, staff always ensure that:

- They have consent from data subjects to share it.
- Adequate security is in place to protect it.
- The data recipient has been outlined in a privacy notice.

10.18. All staff members will implement a 'clear desk policy' to avoid unauthorised access to physical records containing sensitive or personal information. All confidential information will be stored in a securely locked filing cabinet, drawer or safe with restricted access.

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

10.20. The physical security of the school's buildings and storage systems, and access to them, is reviewed **termly** by the **site manager** in conjunction with **the Estates and Admissions Manager**. If an increased risk in vandalism, burglary or theft is identified, this will be reported to the **Executive Team** and extra measures to secure data storage will be put in place.

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

10.22. The **Director of Operations and the Director of IT are** responsible for continuity and recovery measures are in place to ensure the security of protected data.

10.23. Any damage to or theft of data will be managed in accordance with the school's **Data Security Incident Management Policy**

11. Accessing information

11.1. **Discovery Schools Academies Trust** is transparent with data subjects, the information we hold and how it can be accessed.

11.2. All members of staff, parents of registered pupils and other users of the school, e.g. visitors and third-party clubs, are entitled to:

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

11.3. All members of staff, parents of registered pupils and other users of the school and its facilities have the right, under the GDPR, to access certain personal data being held about them or their child.

11.4. The trust/school will adhere to the provisions outlined in the trust's **GDPR Data Protection Policy** when responding to requests seeking access to personal information.

12. Disaster Recovery Plan

12.1. Digital data that is retained for longer than six years will be covered in the **Disaster Recovery Plan (DRP)**.

12.2. The **Director of IT** will identify any digital data that will need to be named as part of a DRP.

12.3. The data will be archived to dedicated files on the school's server, which is password-protected – this will be backed-up in accordance with section 10 of this policy.

12.4. Memory sticks will never be used to store digital data, subject to a DRP.

12.5. The Director of IT will review new and existing storage methods annually and, where appropriate add them to DRP.

12.6. 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

13. Information audit

13.1. The trust and all schools in the multi academy group conduct information audits on an **annual** basis against all information held by the school to evaluate the information the school 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

13.2. 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

13.3. The **Local Data Protection Representative** is responsible for completing the information audit following trust guidelines. The information audit will include the following:

- The school'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

13.4. The **DPO** will carry out a quality assurance audit and consult with staff members involved in the information audit process to ensure that the information is accurate.

13.5. Once it has been confirmed that the information is accurate, **the Director of Operations** will record all details on the trust's **Information Asset Register**.

13.6. The information displayed on the **Information Asset Register** will be shared with the **CEO** to gain their approval.

14. Disposal of data

14.1. Where disposal of information is outlined as standard disposal, this will be recycled appropriate to the form of the information, e.g. paper recycling, electronic recycling.

14.2. Where disposal of information is outlined as secure disposal, this will be shredded and electronic information will be scrubbed clean and, where possible, cut. The **Local Data Protection Representative** will keep a record of all files that have been destroyed which will be countersigned by the **DPO** on a termly basis.

14.3. 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.

14.4. 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.

14.5. 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.

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

15. Monitoring and review

15.1. This policy will be reviewed on an **annual** basis by the **Executive Team** with guidance from the DPO – the next scheduled review date for this policy is **May 2019**.

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