

Data Retention Policy

V1.11

This document applies to all academies and operations of Cambrian Learning Trust.

www.cambrianlearningtrust.org

Document Control			
Author	Operations Manager	Approved By	COO
Last Reviewed	March 2022	Next Review	September 2025
Review Cycle	3 years	Version	1.11

Contents

Policy Statement	3
Legal framework.....	3
Responsibilities	4
Management of pupil records	4
Primary School Pupil Records	4
Secondary School Pupil Records	7
Responsibility for the pupil record once the pupil leaves the school	8
Retention of pupil records and other pupil-related information	8
Retention of staff records	12
Retention of management records	14
Retention of health and safety records.....	16
Retention of financial records	17
Retention of other school records	19
Storing and protecting information	20
Accessing Information	22
Digital continuity statement.....	22
Information audit	23
Disposal of data	24
Monitoring and review	25

Policy Statement

Cambrian Learning Trust (CLT) is committed to maintaining the confidentiality of its information and ensuring that all records within CLT or any of the CLT schools are only accessible by the appropriate individuals. In line with the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018, each school 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.

The Trust has created this policy to outline how records are stored, accessed, monitored, retained and disposed of, in order to meet the school's statutory requirements.

This document complies with the requirements set out in the Data Protection Act 2018 (DPA 2018), which is the UK's implementation of the General Data Protection Regulation.

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. Where the IRMS has not provided guidance for disposal methods or retention periods, good practice recommendations are shown.

Legal framework

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)
- Data Protection Act 2018
- Companies Act

This policy also has due regard to the following guidance:

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

This policy will be implemented in accordance with, and read alongside, the following school policies and procedures:

- Data Protection Policy

- Freedom of Information Policy
- E-security Policy

Responsibilities

CLT Board of Trustees has an accountability for ensuring the Trust meets its statutory requirements.

The Chief Executive Officer (CEO) holds overall responsibility for this policy and for ensuring it is implemented correctly.

The GDPR Trust Lead is accountable for promoting compliance with this policy and reviewing the policy on a 3 yearly basis, in conjunction with the CEO.

The Head Teacher is responsible for the compliance within their school.

The Data Champion at each school is responsible for ensuring that all records are stored securely, in accordance with the retention periods outlined in this policy and are disposed of correctly at their school.

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.

Management of pupil records

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

These guidelines apply to information created and stored both physically and electronically.

Primary School Pupil Records

The following information is stored on a pupil record, and will be easily accessible:

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

The following information is stored on a pupil record, and will be easily accessible:

- 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

The following information is retained in our pupil records:

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

The following information is subject to shorter retention periods and, therefore, will be stored separately in a personal file for the pupil in the in a way that is compliant with GDPR principles:

- 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
- Hard copies of disclosures and reports relating to child protection are stored in a sealed envelope, in a securely locked filing cabinet - a note indicating this is marked on the pupil's file.
- Hard copies of complaints made by parents or pupils are stored in a secure file – a note indicating this is marked on the pupil's file.
- Actual copies of accident and incident information are stored separately on RET'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.

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

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

Electronic records relating to a pupil's record will also be transferred to the pupils' next school. This policy outlines how electronic records will be transferred.

CLT 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 CLT.

Secondary School Pupil Records

Items which should be included on the pupil record:

- If the pupil has attended an early years setting, then the record of transfer should be included on the pupil file.
- Admission form (application form)
- Privacy Notice [if these are issued annually only the most recent need be on the file]
- Photography Consents
- Years Record
- Annual Written Report to Parents
- National Curriculum and Religious Education Locally Agreed Syllabus Record Sheets
- Any information relating to a major incident involving the child (either an accident or other incident)
- Any reports written about the child
- Any information about a statement and support offered in relation to the statement
- Any relevant medical information (should be stored in the file in a sealed envelope clearly marked as such)
- Child protection reports/disclosures (should be stored in the file in a sealed envelope clearly marked as such)
- Any information relating to exclusions (fixed or permanent)
- Any correspondence with parents or outside agencies relating to major issues
- Details of any complaints made by the parents or the pupil.

The following records should be stored separately to the pupil record as they are subject to shorter retention periods and if they are placed on the file then it will involve a lot of unnecessary weeding of the files once the pupil leaves the school.

- Absence notes
- Parental consent forms for trips/outings [in the event of a major incident all the parental consent forms should be retained with the incident report not in the pupil record]
- Correspondence with parents about minor issues

- Accident forms (these should be stored separately and retained on the school premises until their statutory retention period is reached. A copy could be placed on the pupil file in the event of a major incident)

Responsibility for the pupil record once the pupil leaves the school

The school which the pupil attended until statutory school leaving age is responsible for retaining the pupil record until the pupil reaches the age of 25 years.

Retention of pupil records and other pupil-related information

The table below outlines CLT's retention periods for individual pupil 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 be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after Retention period ends
Admissions		
Register of admissions from Local Authority	3 years after the date on which the entry was made	Information is reviewed and the register may be kept permanently as an archive
Secondary school admissions from Local Authority	The current academic year, plus 1 year	Secure Disposal
Proof of address (supplied as part of the enrolment process)	The current academic year, plus 1 year	Secure Disposal
Supplementary information submitted, including religious and medical information etc. (where the admission was successful)	Added to the pupil's file	Secure Disposal

Type of file	Retention period	Action taken after Retention period ends
Supplementary information submitted, including religious and medical information etc. (where the admission was not successful)	Until the appeals process has been completed	Secure Disposal
Pupils' educational records		
Primary Pupils' educational records	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
Secondary Pupils' educational records	25 years after the pupil's date of birth	Secure Disposal
Public examination results	Added to the pupil's record	Uncollected certificates returned to the examination board
Internal examination results	Added to the pupil's record	
Child protection information held on a pupil's record	Stored in a sealed envelope for the same length of time as the pupil's record	Secure Disposal – shredded
Child protection records held in a separate file	25 years after the pupil's date of birth	Secure Disposal – shredded
Attendance		
Attendance registers	Last date of entry on to the register, plus three years	Secure Disposal
Letters authorising absence	Current academic year, plus 2 years	Secure Disposal
SEND		
SEND files, reviews and individual education plans	31 years after the pupil's date of birth (as stated on the pupil's record)	Secure Disposal, unless it is subject to a legal hold
Statement of SEN maintained under section 324 of the Education Act 1996 or an EHC plan maintained under...	31 years after the pupil's date of birth (as stated on the pupil's record)	Secure Disposal, unless it is subject to a legal hold

Type of file	Retention period	Action taken after Retention period ends
...section 37 of the Children and Families Act 2014 (and any amendments to the statement or plan		
Information and advice provided to parents regarding SEND	31 years after the pupil's date of birth (as stated on the pupil's record)	Secure Disposal, unless it is subject to a legal hold
Accessibility strategy	31 years after the pupil's date of birth (as stated on the pupil's record)	Secure Disposal, unless it is subject to a legal hold
Curriculum management		
SATs results	25 years after the pupil's date of birth (as stated on the pupil's record) The School may keep a composite record of the whole year results- these could be kept for current year + 6 years	Secure Disposal
Examination papers	Until the appeals/validation process has been completed	Secure Disposal
Published Admission Number (PAN) reports	Current academic year, plus 6 years	Secure Disposal
Valued added and contextual data	Current academic year, plus 6 years	Secure Disposal
Self-evaluation forms	Current academic year, plus 6 years	Secure Disposal
Pupils' work	Returned to pupils at the end of the academic year, or retained for the current academic year, plus 1 year	Secure Disposal
Extra-curricular activities		
Primary Schools– Records created by schools to obtain approval to run an Educational Visit outside the Classroom	Date of visit + 14 years	Secure Disposal

Type of file	Retention period	Action taken after Retention period ends
Primary Schools– Records created by schools to obtain approval to run an Educational Visit outside the Classroom	Date of visit + 14 years	Secure Disposal
Secondary Schools– Records created by schools to obtain approval to run an Educational Visit outside the Classroom	Date of visit + 10 years	Secure Disposal
Parental consent forms for school trips where no major incident occurred	Should be held for 22 years after the pupil's date of birth. However a risk assessment can be carried out and a decision made to dispose at the end of the trip or at the end of the academic year.	Secure Disposal
Parental consent forms for school trips where a major incident occurred	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)	Secure Disposal
Walking bus registers	6 years from the date of the register being taken	Secure Disposal
Family liaison officers and home-school liaison assistants		
Day books	Current academic year, plus 2 years	Secure Disposal
Reports for outside agencies	Duration of the pupil's time at school	Secure Disposal
Referral forms	Whilst the referral is current	Secure Disposal
Contact data sheets	Current academic year	Reviewed and destroyed if no longer active
Group registers	Current academic year, plus 2 years	Secure Disposal
Contact database entries	Current academic year	Reviewed and destroyed if no longer required

Retention of staff records

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.

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
Operational		
Staff members' personal file	Termination of employment, plus 6 years Unless a staff member is part of any case which falls under the terms of reference of IICSA- if so the file will need to be retained until IICSA enquires are complete	Secure Disposal
Timesheets	Current academic year, plus 3 years	Secure Disposal
Annual appraisal and assessment and professional development records	Current academic year, plus 6 years	Secure Disposal
Recruitment		
Records relating to the appointment of new members of staff (unsuccessful candidates)	Date of appointment of successful candidate, plus 6 months	Secure Disposal
Records relating to the appointment of new members of staff (successful candidates) Including DBS certificates	Application forms, reference and other documents for the duration of the employment + 6 years	Secure Disposal

Type of file	Retention period	Action taken after Retention period ends
Proof of identify as part of the enhanced DBS check	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	Secure Disposal
Evidence of right to work in the UK	Added to staff personal file and destroyed in line with staff file destruction date	Secure Disposal
Single Central Record (SCR)	Only when employed/ volunteering	Secure Disposal
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 6 months	Secure Disposal – if placed on staff personal file, removed from file
Written warning – level 1	Date of warning, plus 6 months	Secure Disposal – if placed on staff personal file, removed from file
Written warning – level 2	Date of warning, plus 12 months	Secure Disposal – if placed on staff personal file, removed from file
Final warning	Date of warning, plus 18 months	Secure Disposal – if placed on staff personal file, removed from file
Case note found	If the incident is related to child protection, then see above, otherwise dispose of at the conclusion of the case	Secure Disposal

Retention of management records

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	Retention period	Action taken after Retention period ends
Governing Committee/Directing Board		
Agendas for governing committee/board meetings	One copy alongside the original set of minutes – all others disposed of without Retention	Secure Disposal
Original, signed copies of the minutes of governing committee/board meetings	Permanent however the organisation or Local Authority is only required to make these available for 10 years from the date of the meeting	Consult local archives before disposal
Reports presented to the governing committee / board which are referred to in the minutes	Permanent however the organisation or Local Authority is only required to make these available for 10 years from the date of the meeting	Consult local archives before disposal
Articles of association	For the life of the Trust	
Trusts and endowments managed by the board	For the life of the School	
Action plans created and administered by the governing committee/board	Until superseded or whilst relevant	Secure Disposal

Type of file	Retention period	Action taken after Retention period ends
Policy documents created and administered by the governing committee /board	Until superseded. The school should consider keeping all policies relating to safeguarding, child protection or other pupil related issues such as exclusion until the IICSA has issued its recommendations	
Records relating to complaints dealt with by the governing committee/board	Major complaints: current year + 6 years. If negligence involved then: current year + 15 years. If child protection or safeguarding issues are involved then current year + 40 years	Secure Disposal
Proposals concerning changing the status of the school	Date proposal accepted or declined, plus three years	Secure Disposal
CEO, Head teachers and senior leadership team (SLT)		
Log books of activity in CLT schools maintained by the Head teachers	Date of last entry, plus a minimum of 6 years	Reviewed and securely disposed of
Minutes of SLT meetings and the meetings of other internal administrative bodies	Date of the meeting, plus 3 years	Reviewed and securely disposed of
Reports created by the CEO, Head teacher or SLT	Date of the report, plus a minimum of 3 years	Reviewed and securely disposed of
Records created by any member of staff with administrative responsibilities	Current academic year, plus 6 years	Reviewed and securely disposed of
Correspondence created by the CEO, Head teacher, SLT, heads of year and other members of staff with administrative responsibilities	Date of correspondence, plus 3 years	Secure Disposal
School development plan	Duration of the plan, plus 3 years	Secure Disposal

Retention of health and safety records

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.

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 and Safety		
Health and safety policy statements	Duration of policy, plus 3 years	Secure Disposal
Health and safety risk assessments	Duration of risk assessment, plus 3 years provided that a copy of the risk assessment is stored with the accident report if an incident has occurred	Secure Disposal
Accident reporting records relating to individuals	3 years after the last entry	Secure Disposal
Records relating to any reportable death, injury, disease or dangerous occurrence	Date of incident plus 3 years provided that all records relation to the incident are held on personnel file	Secure Disposal
Accident requiring reporting to HSE – adults	Date of the incident, plus six years	Secure Disposal
Accident requiring reporting to HSE – pupils	25 years after the pupil's date of birth, on the pupil's record	Secure Disposal
Accidents not requiring reporting to HSE	1 yr from date of incident	Secure Disposal
Control of substances hazardous to health (CoSHH)	Current academic year, plus 40 years	Secure Disposal
Information relating to areas where employees and persons are likely to come into contact with asbestos	Date of last action, plus 40 years	Secure Disposal

Type of file	Retention period	Action taken after Retention period ends
Information relating to areas where employees and persons are likely to come into contact with radiation	2 years from the date on which the examination was made and that the record includes the condition of the equipment at the time of examination	Secure Disposal
Fire precautions log books	Current academic year, plus 3 years	Secure Disposal

Retention of financial records

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.

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 tax year, plus three years	Secure Disposal
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Retained until further recommendations (pensions regulator)	Secure Disposal
Risk management and insurance		
Employer's liability insurance certificate	Closure of the school, plus 40 years	Secure Disposal to be passed to the LA if the school closes.
Asset Management		
Inventories of furniture and equipment	Current academic year, plus 6 years	Secure Disposal
Burglary, theft and vandalism report forms	Current academic year, plus 6 years	Secure Disposal

Type of file	Retention period	Action taken after Retention period ends
Accounts and statements including budget management		
Annual accounts	Current academic year, plus 6 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 3 years	Secure Disposal
Invoices, receipts, order books, requisitions and delivery notices	Current financial year, plus 6 years	Secure Disposal
Records relating to the collection and banking of monies	Current financial year, plus 6 years	Secure Disposal
Records relating to the identification and collection of debt	Current financial year, plus 6 years	Secure Disposal
Contract management		
All records relating to the management of contracts under seal	Last payment on the contract, plus 12 years	Secure Disposal
All records relating to the management of contracts under signature	Last payment on the contract, plus 6 years	Secure Disposal
All records relating to the monitoring of contracts	Life of contract, plus 6 or 12 years	Secure Disposal
School fund		
Cheque books, paying in books, ledgers, invoices, receipts, bank statements and journey books	Current academic year, plus 6 years	Secure Disposal
School meals		
Free school meals registers	Current academic year, plus 6 years	Secure Disposal
School meals registers	Current academic year, plus 3 years	Secure Disposal
School meals summary sheets	Current academic year, plus 3 years	Secure Disposal

Retention of other school records

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.

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 6 years	Secure Disposal
Records relating to the letting of school premises	Current financial year, plus 6 years	Secure Disposal
Maintenance		
All records relating to the maintenance of the school carried out by contractors	For as long as the building belongs to the school and then transferred to new owners if the building is leased or sold	Secure Disposal
All records relating to the maintenance of the school carried out by school employees	For as long as the building belongs to the school and then transferred to new owners if the building is leased or sold	Secure Disposal
Operational administration		
General file series	Current academic year, plus 5 years	Secure Disposal
Records relating to the creation and publication of the school brochure and/or prospectus	Current academic year, plus 3 years	Preserve a copy for archive and then disposed of against common standards
Records relating to the creation and distribution of circulars to staff, parents or pupils	Current academic year, plus 1 year	Disposed of against common standards

Type of file	Retention period	Action taken after Retention period ends
Telephone and call records (call recordings are not standard)	3 months	Any recordings made are deleted automatically
Newsletters and other items with short operational use	Current academic year plus 1 year (schools may decide to archive a copy)	Disposed of against common standards
Visitors' books and signing-in sheets	Last entry in the book, plus 6 years	Reviewed then securely disposed of
Records relating to the creation and management of parent-teacher associations and/or old pupil associations	Current academic year, plus 6 years	Reviewed then securely disposed of

Storing and protecting information

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

IT Services will conduct a back-up of information:

- Sharepoint daily differential, 30-day full backup
- Information on One-Drive is not backed up.
- Information on emails is not backed up apart from key email boxes such as Office and Headteacher accounts.

This is 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.

Data is backed up to a cloud third party solution stored in a UK data centre. More information can be found at <https://www.redstor.com/>

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

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

Digital data is coded, encrypted or password-protected on a network drive that is regularly backed-up.

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

USB external devices are not to hold personal information.

USB external devices are to be password-protected and fully encrypted.

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

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

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

Emails containing sensitive or confidential information are password-protected to ensure that only the recipient is able to access the information. The password will be shared with the recipient in a separate email.

Circular emails to parents are sent via a messaging service so that email addresses are not disclosed to other recipients.

Where personal information that could be considered private or confidential is taken off the premises, to fulfil the purpose of the data in line with the GDPR, either in an electronic or paper format, staff take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

Before sharing data, staff always ensure that:

- They have the correct legal basis to share it.
- Adequate security is in place to protect it.
- The data recipient has been outlined in a privacy notice.

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

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

The physical security of the school's buildings and access is reviewed termly by the Caretaker in conjunction with the Head teacher. If an increased risk in vandalism, burglary or theft is identified, this will be reported to the Operations Manager and extra measures to secure data storage will be put in place.

The school takes its duties under the Data Protection Act 2018 seriously and any unauthorised disclosure may result in disciplinary action.

IT Services is responsible for continuity and recovery measures are in place to ensure the security of protected data.

Accessing Information

CLT is transparent with data subjects, the information held and how it can be accessed.

All members of staff, parents of registered pupils and other users of CLT schools, 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 Data Protection Act 2018.

All members of staff, parents of registered pupils and other users of the school and its facilities have the right, under the DPA 2018, to access certain personal data being held about them or their child.

Personal information can be shared with pupils above the age of 12, when they are considered to be at an appropriate age and responsible for their own affairs; although, this information can still be shared with parents, with their consent.

Pupils aged 12 and above are considered to be at an appropriate age to make decisions for themselves, and are entitled to have their personal information handled in accordance with their rights.

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

Digital continuity statement

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

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

The data will be archived to Office 365 which is password protected, and securely backed up to a protected cloud provider off site.

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

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

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

- A statement of purpose and requirements for keeping the records
- The names of the individuals responsible for long term data preservation
- A description of the information assets to be covered by the digital preservation statement
- A description of when the record needs to be captured into the approved file formats
- A description of the appropriate supported file formats for long-term preservation
- A description of the Retention of all software specification information and licence information
- A description of how access to the information asset register is to be managed in accordance with the Data Protection Act 2018

Information audit

CLT conducts information audits on an annual basis against all information held by CLT to evaluate the information CLT is holding, receiving and using, and to ensure that this is correctly managed in accordance with the Data Protection Act 2018. This includes the following information:

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

The information audit may be completed in a number of ways, including, but not limited to:

- Interviews with staff members with key responsibilities – to identify information

and information flows, etc.

- Questionnaires to key staff members to identify information and information flows, etc.
- A mixture of the above

The Data Protection Officer, in conjunction with the GDPR Trust lead, is responsible for completing the information audit. The information audit will include the following:

- CLT'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

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

Disposal of data

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

Where 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.

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

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

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

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

PC hardware that store any data are destroyed via a third party company who provide certification of the work completed.

Monitoring and review

This policy will be reviewed every three years by GDPR Trust lead in conjunction with the CEO.

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