Data Retention & Destruction Policy

Approved by: THE TRUST BOARD OF GREENSAND MULTI-ACADEMY TRUST	**Date:** Monday 11th March 2019
Last reviewed on: Monday 20th October 2025	

Next review due by: September 2027

Greensand Multi-Academy Trust ("the Trust") is committed to maintaining the confidentiality of its information and ensuring that all records within its member schools are only accessible by the appropriate individuals. The Trust and its schools also have 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 Trust's and its schools' statutory requirements.

Legal framework

This Policy has due regard to legislation and guidance including, but not limited to:

UK General Data Protection Regulation & Data Protection Act 2018

Freedom of Information Act 2000

Limitation Act 1980 (as amended by the Limitation Amendment Act 1980)

Information & Records Management Society (2019) 'Information Management Toolkit for Schools'

Department for Education (2018) 'Data protection: a toolkit for schools' and updated guidance dated February 2023

This Policy will be implemented in accordance with the Trust's Data Protection Policy.

Responsibilities

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

The Data Protection Officer (DPO), Mrs Wendy Hill, is responsible for the management of records of the Trust's member schools and can be contacted on w.hill@greensandacademytrust.co.uk Each school has a Data Protection Lead (DPL), who ensures adoption of this Policy within their school, and an overview is also shared with IT managers with the schools.

The DPO is responsible for promoting compliance and reviewing the Policy every two years in conjunction with the CEO. The DPO 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.

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 child's time in the education system

– they are passed to each school that a child attends and include all personal information relating to them, e.g. date of birth, home address, as well as their progress and achievement.

Pupil files may contain any or all of the following information:

- Forename, surname, gender and date of birth
- Unique pupil number (UPN)
- Ethnic origin, religion and first language
- Any preferred names
- Position in their family, e.g. eldest sibling
- Emergency contact details and doctor's details
- 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
- Agency involvement, e.g. speech and language therapist
- Admissions form
- SEND
- If the pupil has attended an early years setting, the record of transfer
- Annual written reports to parents
- National curriculum and agreed syllabus record sheets
- Notes relating to major incidents and accidents involving the child
- Any information about an education, health and care plan (EHCP) and support offered in relation to the EHCP
- Information relating to exclusions
- 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 child are held

The following information will be stored separately:

- Absence notes
- Parental and where appropriate, pupil consent forms for educational visits, photographs and videos (if applicable), etc.

Hard copies of disclosures and reports relating to child protection are held in a securely locked filing cabinet within each school.

Hard copies of complaints made by parents/carers or children are stored in a file in a secure area within the relevant member school.

Actual copies of accident and incident information are stored separately on the schools' management information systems and by the Central Team office. These will be held in line with the retention periods outlined in this Policy. An additional copy may be placed in the child's file in the event of a major accident or incident.

Schools will ensure that no pupil records are altered or amended before transferring them.

Electronic records relating to a pupil's record will be transferred to the child's next school using the Department for Education Schools to Schools service.

For Primary schools only within the Trust: Schools will not keep any copies of information stored

within a pupil's record, unless there is ongoing legal action at the time during which the child leaves the school.

The responsibility for these records will then transfer to the next school that the child attends.

If a child attends a member school until statutory school leaving age, the school will keep the child's records until the pupil reaches the age of 25 years.

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

Where Child Protection files are transferred, a Designated Safeguarding Lead (DSL) must sign for receipt.

Retention of pupil records and other pupil-related information

The following tables outline 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.

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

Although this list is comprehensive, schools should contact the DPO if they are unsure about any data that may not be specifically mentioned.

Type of file	Retention period	Action taken after retention period
Personal identifiers, contacts and personal characteristics		
Images used for identification purposes	Whilst the child remains at school, and up to the age of 25	Secure disposal
Images used in displays in schools	Whilst the child is at school plus one year	Secure disposal
Images used for marketing purposes, or other	In line with the consent period	Secure disposal
Biometric data	For the duration of the event/activity, or whilst the child remains at school, whichever is less, plus one month	Secure disposal
Names, addresses, and characteristics	Whilst the child is at school, and up to age 25	Secure disposal
Admissions		
Register of admissions	Whilst the child remains at the school, and up to age 25	Information is reviewed and the register may be kept permanently
Successful Admissions appeals	Whilst the child remains at school, and up to age 25	Secure disposal
Unsuccessful school Admissions	Until the appeal process is complete	Secure disposal

Pupils' educational records		
Primary Pupils' educational records	Whilst the child remains at the school	Transferred to the next destination – if this is an independent school, home-schooling or outside of the UK, a copy of the file will be retained until confirmation of delivery is received.
Secondary Pupils' educational records	25 years after the child's date of birth	Secure disposal
Public examination results	Added to the child's record and transferred to next school Whilst the child remains at the school, and up to age 25	Returned to the examination board
Internal examination results	Added to the child's record and transferred to next school Whilst the child remains at the school, and up to age 25	Secure disposal
Behaviour records	Added to the child's record and transferred to the next school Whilst the child remains at the school, and up to age 25	Secure disposal
Exclusion records	Added to the child's record and transferred to the next school Whilst the child remains at the school, and up to age 25	Secure disposal
Child protection records held in a separate file	25 years after the child's date of birth	Securely disposed of – shredded

Attendance		
Attendance registers	Whilst the child remains at school, plus one year Non-identifiable summary statistics are held after the initial retention period for 25 years after the child's date of birth	Secure disposal
Letters authorising absence	Whilst the child remains at the school, and up to age 25	Secure disposal
Medical information and administration		
Permission slips	For the duration of the period that medication is given then added to student record	Secure disposal
Medical conditions – ongoing management	Added to the child's record and transferred to the next school Whilst the child remains at the school, and up to age 25	Secure disposal
Medical incidents that have a behavioural or safeguarding influence	Added to the child's record and transferred to the next school Copies held whilst the child is at school, plus 25 years	Secure disposal

SEND		
SEND files, reviews and individual education plans	25 years after the child's date of birth (as stated on the child'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 child's date of birth (as stated on the child's record)	Secure disposal, unless it is subject to a legal hold
Information and advice provided to parents regarding SEND	25 years after the child's date of birth (as stated on the child's record)	Secure disposal, unless it is subject to a legal hold
Accessibility strategy	25 years after the child's date of birth (as stated on the child's record)	Secure disposal, unless it is subject to a legal hold
Curriculum management		
SATs results (if applicable)	25 years after the child's date of birth (as stated on the child's record)	Secure disposal
Examination papers	Until the appeals/validation process has been completed	Secure disposal
Published Admission Number (PAN) reports	Current academic year, plus six years	Secure disposal
Valued added and contextual data	Current academic year, plus six years	Secure disposal
Self-evaluation forms	Current academic year, plus six years	Secure disposal
Pupils' work	Returned to children at the end of the academic year, or retained for the current academic year, plus one year	Secure disposal

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	Secure disposal
Financial information relating to school trips	Whilst the child remains at school, plus one year	Secure disposal
Parental consent forms for specific school trips (e.g. residential) where no major incident occurred	Until the conclusion of the trip	Secure disposal
Annual parental consent forms and sporting activities consent forms	Current academic year	Secure disposal
Parental consent forms for school trips where a major incident occurred	25 years after the child's date of birth on the child's record (permission slips of all children on the trip will also be held)	Secure disposal
Educational visitors in school – sharing of personal information	Until the conclusion of the visit, plus one month	Secure disposal
Attendance Officers/Home School Link Workers		
Day books	Current academic year, plus two years	Reviewed and destroyed if no longer required
Reports for outside agencies	Duration of the child'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
Contact database entries	Current academic year	Reviewed and destroyed if no longer required
Group registers	Current academic year, plus two years	Secure disposal

Catering and free school meal management		
Meal administration	Whilst the child is at school, plus one year	Secure disposal
Meal eligibility	Current year plus 6 years	Secure disposal

Retention of staff records

The table below outlines the member schools' retention periods for staff records and the action that will be taken after the relevant 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 six years	Secure disposal
Timesheets	Current academic year, plus six years	Secure disposal
Annual appraisal and assessment records	Current academic year, plus five years	Secure disposal
Recruitment		
Records relating to the appointment of a new headteacher	Date of appointment, plus six years	Secure disposal
Records relating to the appointment of new members of staff (unsuccessful candidates)	Date of appointment of successful candidate, plus six months unless applicant has given permission to hold details on file	Secure disposal
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	Secure disposal
DBS certificates	As soon as practicable after check is complete and the outcome recorded unless there are exceptional circumstances in which case no longer than six months	Secure disposal

Proof of identify as part of the enhanced DBS check	Relevant information added to staff personal file	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
Evidence of right to work in the UK including identification documents	Added to staff personal file	Six years after employment ceases
Immigration checks	Added to staff personal file	Two years after the termination of employment
Working Time Regulations: Opt Out Forms Records of Compliance with WTR	Added to staff personal file	 Two years after commencement Two years after the relevant period
Pension records	Digital LGPS records	12 Years
Payroll & Wage Records	Edupay	6 years after tax year to which they relate to
Trade Union Agreements	Digital records	10 years after ceasing to be effective

Disciplinary and grievance procedures		
Child protection allegations, including where the allegation is unproven	Added to secure safeguarding files 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	Secure disposal – if placed on staff personal file, removed from file
Written warning – level 1	Date of warning, plus six 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
Records relating to unproven incidents	Conclusion of the case, unless the incident is child protection related and is disposed of as above	Secure disposal

Retention of Senior Leadership and management records

The table below outlines the Trust's and the member schools' retention periods for senior leadership and management records, and the action that will be taken after the relevant 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
Members' Board, Trust Board & School Committees		
Agendas for board & committee meetings	One copy alongside the original set of minutes – all others disposed of without retention	Secure disposal
Original, signed copies of the minutes of board & committee meetings	Permanent	Stored securely
Inspection copies of the minutes of board & committee meetings	Date of meeting, plus three years	Shredded if they contain any sensitive and personal information
Register of business interests	Date appointment ceases plus 6 years	Secure disposal
Reports presented to the boards & committees	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
Register of attendance at Trust Board and Committee meetings	Date of last meeting plus 6 years	
Instruments of government, including articles of association	Permanent	Stored securely
Trusts and endowments managed by the Trust Board	Permanent	Retained in the school/ centrally for the Trust whilst it remains open
Action plans created and administered by the Trust Board & committees	Duration of the action plan, plus three years	Secure disposal
Policy documents created and administered by the Trust Board & committees	Duration of the policy, plus three years	Secure disposal

Records relating to complaints dealt with by the schools/Trust Board	Date of the resolution of the complaint, plus a minimum of six years. If negligence involved plus 15 years. If safeguarding of child protection issues are involved: current year plus 40 years	Reviewed for further retention in case of contentious disputes, then securely disposed of
Annual reports required by the Department for Education	Date of report plus 10 years	Secure disposal
All records relating to conversion of schools to academy status	For the life of the organization	Consult local archives before disposal
Annual reports created under the requirements of The Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002	Date of report, plus 10 years	Secure disposal
Proposals concerning changing the status of the school	Date proposal accepted or declined, plus three years	Secure disposal
Personal data for Members, Trustees & Governors	Date appointment ceases plus 6 years	
Headteacher 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 then secure disposal
Reports created by the headteacher or SLT	Date of the report, plus a minimum of three years	Reviewed then secure disposal
Records created by the headteacher, deputy headteacher, heads of year and other members of staff with administrative responsibilities	Current academic year, plus six years	Reviewed then secure disposal
Correspondence created by the headteacher, deputy headteacher, heads of year and other members of staff with administrative responsibilities	Date of correspondence, plus three years	Reviewed then secure disposal
Professional development plan	Duration of the plan, plus six years	Secure disposal

School development plan	Duration of the plan, plus three years	Secure disposal

Retention of Health and Safety records

The table below outlines the member schools' retention periods for health and safety records, and the action that will be taken after the relevant 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 three years	Secure disposal
Health and Safety Risk Assessments	Duration of risk assessment, plus three years	Secure disposal
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	Secure disposal
Accident reporting – adults	Date of the incident, plus 3 years	Secure disposal
Accident reporting – pupils	25 years after the child's date of birth, on the child's record	Secure disposal
Control of substances hazardous to health	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
Information relating to areas where employees and persons are likely to come into contact with radiation	Date of last action, plus 50 years	Secure disposal
Fire precautions log books	Current academic year, plus 3 years	Secure disposal

Retention of financial records

The table below outlines the member schools' retention periods for financial records and the action that will be taken after the relevant 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 academic year, plus three years	Secure disposal
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Current academic year, plus six years	Secure disposal
Risk management and insurance		
Employer's liability insurance certificate	Closure of the school, plus 40 years	Secure disposal
Asset management		
Inventories of furniture and equipment	Current academic year, plus six years	Secure disposal
Burglary, theft and vandalism report forms	Current academic year, plus six years	Secure disposal
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	Secure disposal
Invoices, receipts, order books, requisitions and delivery notices	Current financial year, plus six years	Secure disposal
Records relating to the collection and banking of monies	Current financial year, plus six years	Secure disposal
Records relating to the identification and collection of debt	Current financial year, plus six 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 six years	Secure disposal
All records relating to the monitoring of contracts	Current academic year, plus two years	Secure disposal
School fund		
Cheque books, paying in books, ledgers, invoices, receipts, bank statements and journey books	Current academic year, plus six years	Secure disposal
School meals		
Free school meals registers(if applicable)	Current academic year, plus six years	Secure disposal
School meals registers (if applicable)	Current academic year, plus three years	Secure disposal
School meals summary sheets (if applicable)	Current academic year, plus three years	Secure disposal

Retention of other school records

The table below outlines the member schools' retention periods for any other records held by the schools, and the action that will be taken after the relevant 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 six years	Secure disposal

Type of file	Retention period	Action taken after retention period ends
Property management continued		
Records relating to the letting of school premises	Current financial year, plus six years	Secure disposal
Maintenance		
All records relating to the maintenance of the school carried out by contractors	Current academic year, plus six years	Secure disposal
All records relating to the maintenance of the school carried out by school employees	Current academic year, plus six years	Secure disposal
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 pupils	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 pupil associations	Current academic year, plus six years	Reviewed then securely disposed of

Storing and protecting information

The DPO 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 by member schools.

The ICT support staff will conduct a back-up of 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.

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

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

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

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.

Memory sticks are not used to hold personal information unless they are password-protected and fully encrypted.

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

Where possible, member schools enable electronic devices to allow the remote blocking or deletion of data in case of theft.

The use of memory sticks is discouraged. However, should staff, Members, Trustees and Governors use memory sticks when completing school work, these **must** be encrypted.

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 secure manner.

Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

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

Where personal information that could be considered private or confidential is taken off the premises, staff must be vigilant and responsible concerning its security.

Before sharing data, staff always ensure that:

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

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

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

The physical security of the schools' buildings and storage systems, and access to them, is continuously monitored and reviewed. If an increased risk in vandalism, burglary or theft is identified, this will be reported to the relevant Headteacher and extra measures to secure data storage will be put in place.

The Trust and the member schools takes their duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action.

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

Any damage to or theft of data will be managed in accordance with the school's GDPR Data Protection policy.

Accessing information

The Trust schools are transparent with data subjects, the information we hold and how it can be accessed.

All members of staff, parents/carers 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

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

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

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

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

Digital continuity statement

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

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

3. The data will be archived to dedicated files on the school's server, which are password-protected – this will be backed-up in accordance with section 11 of this Policy.

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

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

Information audit

The member schools will conduct information audits on an annual basis against all information held by their 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:

- Paper documents and records
- Electronic documents and records
- Databases
- Sound recordings
- Video and photographic records

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 DPL/DPO is responsible for completing the information audit. 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

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

Once it has been confirmed that the information is accurate, the DPL will record all details on the school's Information Asset Register.
The information displayed on the Information Asset Register will be shared with the Headteacher to gain their approval.

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. Each school will keep a record of secure disposal.

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.

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 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.

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

Photographer and Marketing Company - Specific Data Handling and Retention

The Trust recognises the importance of managing photographic data responsibly and in accordance with GDPR and safeguarding principles. This section outlines expectations for the Trust's photographer White Silk Studio (WSS) and Marketing Company (YMC) and image retention practices.

Role Definition:

- The Trust photographer is an external contractor commissioned for specific events or purposes.

- Responsibilities include capturing images for events, marketing, ID photos, and educational activities.

The Trust uses Your Marketing Team as an external contractor to advise and produce printed publicity material including banners, impact reports, school open day leaflets and social media advertising.

Image Retention Periods:

Your Marketing Company – Retains images whilst under contract and until one year after. At this time images will be safely deleted. YMC do not use any images which could identify any individual child as part of their portfolio.

White Silk Studio – Retains images on a secured sharepoint and hard drive for one year. WSS do not use any images which could identify a child as part of their portfolio.

This Policy will be reviewed every two years.