MIST Head Office

Records Retention Statement and Schedule (July 2022)

INTRODUCTION

Methodist Independent Schools Trust (MIST) is an educational charity operating in England and Wales. MIST Head Office is based at 27 Tavistock Square, London, WC1H 9HH. MIST can be contacted on 020 7935 3723 and admin@methodistschools.org.uk. MIST's charity registration number is 1142794 and company number is 07649422.

RETENTION STATEMENT

Underlying an efficient records management system is a thorough document retention policy for both digital and physical data. A retention policy offers guidance and provides a framework for employees to manage information across its lifecycle enabling the organisation to adhere with the various laws and regulations pertaining to data management. According to its published privacy notices MIST will retain information for as long as it has a purpose and a lawful basis for doing so.

MIST's Privacy Notices are publicly available and can be accessed via on the website at:

www.methodistschools.org.uk/privacy_notices.

RETENTION POLICY

Head Office has referred to the Information and Records Management Societies Records Management Toolkit for Schools (2019). Records provide evidence for protecting the legal rights and interests of the office and provides evidence for demonstrating performance and accountability. This document provides the policy framework through which this effective management can be achieved and audited.

It covers:

- Scope
- Responsibilities
- Relationships with existing policies
- Data Subject Access Requests (DSARs)

SCOPE

This policy applies to all records created, received or maintained by employees at Head Office while carrying out its functions.

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

RESPONSIBILITIES

Responsibility for data governance lies with the Audit & Risk Management Committee and is implemented by the members of staff at Head Office.

Individual staff and employees must ensure that records for which they are responsible are accurate and are maintained and disposed of in accordance with the Head Office's records management guidelines.

MIST maintains a schedule of indicative data retention periods which are used to guide staff actions in relation to the retention of data. Except where there is a specific statutory obligation to destroy

records, staff will always be expected to exercise judgement and consider the specific circumstances when reviewing records and identifying data for deletion.

RELATIONSHIPS WITH EXISTING POLICIES/PRIVACY NOTICES

- Data Protection Policy
- Privacy Notice
- Staff/Volunteer Privacy Notice
- Data Subject Access Requests (DSAR)

DATA SUBJECT ACCESS REQUESTS (DSAR)

All data subjects past and present (staff, volunteers, pupils, parents, Church stakeholders etc.) have the right to contact MIST and make a DSAR. The DSAR must be answered within 1 calendar month.

The DSAR Policy can be accessed via www.methodistschools.org.uk/privacy_notices.

QUERIES AND COMPLAINTS

Any comments or queries on this statement and schedule should be directed to the Business Director and Information & Communications Manager (admin@methodistschools.org.uk 020 7935 3723).

If an individual believes that MIST Head Office has not complied with this policy or acted otherwise than in accordance with Data Protection Law, they should utilise the Trust's complaints procedure and should also notify the Business Director and Information & Communications Manager. You can also make a referral to or lodge a complaint with the Information Commissioner's Office (ICO), although the ICO recommends that steps are taken to resolve the matter with the data controller before involving the regulator.

Reviewed: July 2022
Next Review: July 2025

RETENTION SCHEDULE

'Secure Destruction' of physical documentation is shredding with a cross shredder at MIST Head Office. When destruction is done externally then a certificate must be acquired from the shredding company.

RECORD TYPE	**DATA PROTECTION CONCERN?**	**GUIDELINE RETENTION PERIOD**	**DELETION/ DESTRUCTION**
GOVERNANCE & TRUST BUSINESS			
Instrument of Government, Articles of Association	No	Permanent (or until dissolution of company – review for archive)	n/a
Trust Deeds (Trust and Schools)	No	Permanent (or until dissolution of company – review for archive)	n/a
Certificates of Incorporation	No	Permanent (or until dissolution of company – review for archive)	n/a
Employers' liability certificate	No	Permanent (or until dissolution of company – review for archive)	n/a
Records for all full Trustee body meetings, committee, sub-committee and working party meetings, including: 1. agendas 2. signed minutes 3. reports noted in minutes	Yes – may contain personal data depending on meeting and subject	Permanent 1 master meeting record should be retained (maintained but also downloaded from Board Intelligence and saved in Laserfiche) – all other copies deleted.	Digital/physical) copies to be securely destroyed.
Action Plans created by the Trust	No	Project Lifespan + 6 years	Kept digitally – deletion from server. Securely destroy hard copies.

RECORD TYPE	**DATA PROTECTION CONCERN?**	**GUIDELINE RETENTION PERIOD**	**DELETION/ DESTRUCTION**
Policy documents agreed by Trust (not including safeguarding related policies)	No	Policy Lifespan + 6 years post review period	Kept digitally – deletion from server. Destroy hard copies.
Annual Reports	No	6 years + review for archiving	Kept digitally – deletion from server. Destroy hard copies.
Risk Assessments	No (if not relating to safeguarding)	7 years from completion of relevant project, incident, event or activity. Should the risk assessment relate to a safeguarding matter the record should maintained for a longer term)	Digital/physical copies to be securely destroyed.
Serious Incident Reports	Yes	Permanent	n/a
DBS Documentation	Yes	Verification information only until DBS is successfully completed. But kept no longer than 6 months (including DBS certificate). DBS numbers - duration staff/volunteer is engagement with Trust business + review at that point.	Kept digitally – deletion from server. Securely destroy hard copies.
Trustee/Governor Application Forms & Declaration Forms	Yes	Duration volunteer is engagement with Trust business + 7 years from departure **unless there is a lawful basis for continued retention – see privacy notice.**	Kept digitally – deletion from server. Securely destroy hard copies.
Trustee Register of Interests	Yes	Duration volunteer is engagement with Trust business + 7 years from departure **unless there is a lawful basis for continued retention – see privacy notice.**	Kept digitally – deletion from server. Securely destroy hard copies.

RECORD TYPE	**DATA PROTECTION CONCERN?**	**GUIDELINE RETENTION PERIOD**	**DELETION/ DESTRUCTION**
Trustee Visit Reports	No (unless a safeguarding concern has been disclosed during the visit and noted on the Visit profoma)	7 years **unless there is a lawful basis for continued retention – see privacy notice.**	Kept digitally – deletion from server. Securely destroy hard copies.
Records (i.e. register and outcomes) relating to complaints dealt with by the Trust Head Office.	Yes	10 years **unless there is a lawful basis for continued retention – see privacy notice.**	Kept digitally – deletion from server. Securely destroy hard copies.
FINANCE, INSURANCE AND CONTRACTS/AGREEMENTS			
Insurance Policies (private, public, professional indemnity)	No	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage for any run-off arrangement and coverage of insured risks (until it is possible that no living person could make a claim)	Kept digitally – deletion from server. Securely destroy hard copies.
Correspondence related to claims/renewals/notification	No	7 years	Kept digitally – deletion from server. Securely destroy hard copies.
Accounting Records (local and schools)	No	6 years from the end of the financial year in which the transaction took place	Kept digitally – deletion from server. Securely destroy hard copies.

RECORD TYPE	**DATA PROTECTION CONCERN?**	**GUIDELINE RETENTION PERIOD**	**DELETION/ DESTRUCTION**
Tax Returns (local and schools)	No	6 years from the end of the financial year in which the transaction took place	Kept digitally – deletion from server. Securely destroy hard copies.
VAT Returns (local and schools)	No	6 years from the end of the financial year in which the transaction took place	Kept digitally – deletion from server. Securely destroy hard copies.
Budget and internal financial reports (local and schools)	No	3 years from the end of the financial year in which the transactions took place	Kept digitally – deletion from server. Securely destroy hard copies.
Signed or final/concluded agreements (including any signed or final/concluded variations or amendments)	No	7 years from completion of contractual obligations or term of agreement, whichever is the later	Kept digitally – deletion from server. Securely destroy hard copies.
Deeds (or contracts under seal)	No	13 years from completion of contractual obligation or term of agreement	Kept digitally – deletion from server. Securely destroy hard copies.
Formal documents of title (trademarks, registered design certificates, patents, utility model certificates)	No	Permanent (if permanently extended (e.g. trademark) Otherwise – expiry of right + 7 years	Kept digitally – deletion from server. Securely destroy hard copies.

RECORD TYPE	**DATA PROTECTION CONCERN?**	**GUIDELINE RETENTION PERIOD**	**DELETION/ DESTRUCTION**
IP / IT agreements (including software licences and ancillary agreements e.g. maintenance, storage, development, coexistence agreements, consents)	No	7 years from completion of contractual obligation concerned or term of agreement	Kept digitally – deletion from server. Securely destroy hard copies.
Methodist Bursary Application Forms and supporting evidence	Yes	Verified at time of application and then destroyed. Name, school and bursary amount – 7 years	Kept digitally – deletion from server. Securely destroy hard copies.
HR ADMINISTRATION – HEAD OFFICE			
Single central record of staff/volunteers	Yes	Permanent record of all mandatory checks undertaken	n/a
Contracts of employment	Yes	7 years from the effective date of end of contract **unless there is a lawful basis for continued retention – see privacy notice.**	Kept digitally – deletion from server. Securely destroy hard copies.
Employee appraisals or reviews	Yes	Duration of employment + 7 years **unless there is a lawful basis for continued retention – see privacy notice.**	Kept digitally – deletion from server. Securely destroy hard copies.
Staff personnel file	Yes	Duration of employment + 7 years **unless there is a lawful basis for continued retention – see privacy notice.**	Kept digitally – deletion from server. Securely destroy hard copies.
Payroll, salary, maternity pay records	Yes	6 years	Kept digitally – deletion from server. Securely destroy hard copies.

RECORD TYPE	**DATA PROTECTION CONCERN?**	**GUIDELINE RETENTION PERIOD**	**DELETION/ DESTRUCTION**
Pension or other benefit schedule records	Yes	Permanent (depending on the nature of the scheme)	n/a
Job application, interview/rejection records (unsuccessful applicants)	Yes	6 months **unless successful has given explicit and noted consent for longer retention.**	Kept digitally – deletion from server. Securely destroy hard copies.
Disciplinary records	Yes	Oral Warning – Date of warning + 6 months Written warning (1st) – Date of warning + 6 months Written warning (2nd) – 12 months Final warning – Date of warning + 18 months Retention may be longer if gross misconduct. + 2 years from expiration.	Kept digitally – deletion from server. Securely destroy hard copies.
Absence records/ sickness records	Yes *note that sickness records are sensitive information and should be kept separate from accident records	current year + 3 years	Kept digitally – deletion from server. Securely destroy hard copies.
Annual Leave records	No	Current year + 3 years	Kept digitally – deletion from server. Securely destroy hard copies.

RECORD TYPE	**DATA PROTECTION CONCERN?**	**GUIDELINE RETENTION PERIOD**	**DELETION/ DESTRUCTION**
Immigration records	Yes	Current year + 3 years	Kept digitally – deletion from server. Securely destroy hard copies.
Accident at work records	No	4 years from date of accident – review case-by-case	Kept digitally – deletion from server. Securely destroy hard copies.
RECORD TYPE	**DATA PROTECTION CONCERN?**	**RETENTION PERIOD**	**DELETION/DESTRUCTION**
Staff use of hazardous substances	No	7 years from end of date of use – review case-by-case	Kept digitally – deletion from server. Securely destroy hard copies.
DATA PROTECTION			
Records documentation (including processing activity, data breaches, DPIA assessments)	No	Permanent – as long as up to date and relevant	Kept digitally – deletion from server. Securely destroy hard copies.
SAFEGUARDING			
Policies and Procedures	No	Permanent	n/a
Accident / Incident reporting	Yes	Periodic review by suitable person. Keep on record for as long as any living person may bring a claim. **See MIST Privacy Notice.**	n/a

RECORD TYPE	**DATA PROTECTION CONCERN?**	**GUIDELINE RETENTION PERIOD**	**DELETION/ DESTRUCTION**
Low Level Concerns	Yes	Periodic review by suitable person**. See MIST Privacy Notice.**	n/a
LOCAL SCHOOL GOVERNING PAPERS			
Copies of local school Governing Body Papers	Yes – depending on committee (e.g., safeguarding).	7 years	Kept digitally – deletion from server. Securely destroy hard copies.
COMMUNICATIONS (REMOTE MEETINGS AND VOICEMAILS)			
Remote meetings – visual and audio on software (e.g. Zoom or MS Teams), IP addresses	Yes	Minutes are kept of remote meetings. The latter are kept according to the applicable retention periods (see above). Audio, visual and IP addresses are not kept/recorded and are disposed of after the remote meeting. Where a meeting is recorded is it recorded with permission and kept for current year +3 years.	n/a – data disposed after the remote meeting. Attendees' email addresses are kept and retention period for this is above
Voicemails - via VoIP system	Yes	Unsaved messages are deleted after 90 days retention period. Saved messages should be kept according to the subject matter e.g. safeguarding.	Systems destroys unsaved messages after 90 days retention period.