Our Lady and All Saints Catholic Multi Academy Company

Data Retention and Disposal Policy

Version:	1.0
Ratified by:	Peter Davis - CSEL
Date ratified:	25th March 2026
Name of originator/author:	Ben Clayton, Chief Information Officer – OLAAS MAC
Circulated to:	Board of Directors, Local Governing Bodies, and all Schools
Date issued:	7th April 2026
Review date:	March 2027

1. Introduction

This policy sets out how the Our Lady & All Saints Catholic MAC manages the retention, storage and secure disposal of information. It ensures that personal data is only kept for as long as it is needed, remains accessible during that time, and is securely destroyed afterwards.

It supports our duty to protect personal data under UK GDPR and the Data Protection Act, and aligns with the OLAAS Data Protection Policy.

2. Scope

This policy applies to all OLAAS schools and to anyone who handles data on behalf of the MAC, including:

- Staff and governors
- Volunteers and contractors
- Visitors and service providers
- Central MAC staff

It covers all systems including Google Workspace, Microsoft 365, MIS, finance systems, HR systems, safeguarding systems, CCTV and paper-based records.

3. Aims

This policy aims to:

- Ensure records are kept only for the time they are required
- Support safeguarding, HR, legal and operational duties
- Set clear retention expectations for staff
- Ensure secure disposal of all personal data
- Maintain compliance with UK GDPR and OLAAS policies

4. Retention Rules for Cloud Systems (Email & Drive)

These settings apply across all OLAAS schools for consistency and compliance.

Learners

- Email: deleted emails retained for **365 days**
- Drive: deleted items retained for **365 days**

Staff

- Gmail: deleted emails retained for 7 years (2,557 days)
- Drive: deleted items retained for 7 years (2,557 days)

System Logs

- Minimum of 12 months

These periods support safeguarding, employment, audit and operational requirements.

5. Retention Periods – Key Categories

All schools must follow the Trust-wide retention schedule. Key statutory periods include:

- Safeguarding/Child Protection: until the pupil is 25
- SEN/EHCP: DOB + 31 years
- Pupil Records (general): DOB + 25 years
- Staff HR Files: 6 years after employment ends
- Recruitment Records (unsuccessful): 6 months
- Accident/Medical Records: DOB + 21 years and 3 months
- Finance Records: 6–7 years
- CCTV Footage: 30 days, unless needed for an investigation

The full retention schedule is held centrally and updated as required.

6. Storage and Access

Schools must ensure that:

- All data is stored in approved systems only
- Access is restricted to staff who need it
- Paper records are kept securely in locked storage
- Personal devices are not used to store MAC data unless authorised

- Sensitive data is encrypted where appropriate

These expectations align with section 15 of the OLAAS Data Protection Policy.

7. Archiving

Schools must archive records securely and ensure:

- Archived data is labelled with destruction dates
- Only necessary long-term records are archived
- Records remain accessible during their retention period
- Individuals do not store archives in personal areas or email accounts

8. Secure Disposal

When retention periods end, data must be securely destroyed.

Paper

- Shredded using cross-cut shredders
- Or disposed of by a certified confidential waste service

Digital

- Permanently deleted from systems
- Securely wiped from devices
- Removed from backups when possible
- Redundant hardware disposed of via WEEE-compliant processes

These processes reflect section 16 of the OLAAS Data Protection Policy.

9. Leavers

Staff

- Important files must be transferred to shared areas before accounts are closed
- Accounts are deleted in line with cloud retention rules
- Personal data must not be left in email or personal drives

Students

- Accounts deleted after the 365-day retention period
- Work requiring long-term retention must be saved by the school

10. Roles and Responsibilities

Chief Information Officer (CIO)

- Leads MAC-wide retention implementation
- Ensures cloud retention rules are correctly applied
- Oversees secure disposal arrangements

Data Protection Leads

- Support school-level compliance
- Advise on retention and disposal decisions

All Staff

- Follow the retention schedule
- Store data only in approved systems
- Avoid unnecessary duplication
- Report any concerns about data retention or security

Third-Party Providers

- Must follow OLAAS retention requirements
- Must delete MAC data when access ends

11. Review and Governance

This policy is reviewed annually or earlier if required by changes in legislation, systems or Trust procedures.