Data Retention Policy

This Policy has been approved and adopted by the Xavier Catholic Education Trust in May 2026.
To be reviewed May 2027

Committee Responsible: Risk & Audit Committee

Data Retention Policy

Any reference within this policy to Xavier Catholic Education Trust, XCET or the Trust also incorporates its constituent schools.

Introduction

The Xavier Catholic Education Trust has a responsibility to maintain its records and record keeping systems. When doing this, the Trust will take account of the following factors:

- The most efficient and effective way of storing records and information.
- The confidential nature of the records and information stored.
- The security of the record systems used.
- Privacy and disclosure; and
- Their accessibility.

This policy does not form part of any employee's contract of employment and is not intended to have contractual effect. It does, however, reflect the Trusts' current practice, the requirements of current legislation and best practice and guidance. It may be amended by the Trust from time to time and any changes will be notified to employees within one month of the date on which the change is intended to take effect. The Trust may also vary any parts of this procedure, including anytime limits, as appropriate in any case.

Data Protection

This policy sets out how long employment-related and pupil data will normally be held by us and when that information will be confidentially destroyed in compliance with the terms of the General Data Protection Regulation (GDPR) and the Freedom of Information Act 2000.

Data will be stored and processed to allow for the efficient operation of the schools. The Trusts' Data Protection Policy outlines its duties and obligations under the GDPR.

Retention Schedule

The Trust has adopted the Retention Schedule of its DPO. When managing records, the Trust will adhere to the standard retention times listed within that schedule.

The schedule is a relatively lengthy document listing the many types of records used by schools and the applicable retention periods for each record type. The retention periods are based on business needs and legal requirements.

Destruction of Records

Where records have been identified for destruction, they must be disposed of in an appropriate way. All information must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints, or grievances.
All paper records containing personal information, or sensitive policy information should be shredded before disposal where possible or disposed of via a confidential waste service. All other paper records should be disposed of by an appropriate wastepaper merchant. All electronic information will be deleted. The schools maintain a database of records which have been destroyed and who authorised their destruction. When destroying documents, the appropriate staff member should record in this list at least:

- File reference (or other unique identifier).
- File title/description.
- Number of files; and
- Name of the authorising officer.

Archiving

Where records have been identified as being worthy of preservation over the longer term, arrangements should be made to transfer the records to the archives. A database of the records sent to the archives is maintained by: Database Managers, HR Teams and/or Administrative teams. The appropriate staff member, when archiving documents should record in this list the following information:

- File reference (or other unique identifier).
- File title/description.
- Number of files; and
- Name of the authorising officer.

Transferring Information to Other Media

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as digital media or virtual storage centres (such as cloud storage). The lifespan of the media and the ability to migrate data where necessary should always be considered.

Responsibility and Monitoring

The School Business Managers/Office Managers, Chief Financial and Operations Officer, Data Managers and IT Network Managers have joint overview in the primary and day-to-day responsibility for implementing this Policy. The Data Protection Officer, in conjunction with the schools, is responsible for monitoring its use and effectiveness and dealing with any queries on its interpretation. The Data Protection Officer will consider the suitability and adequacy of this policy and report improvements directly to management.

Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective in creating, maintaining and removing records.

Management at all levels are responsible for ensuring those reporting to them are made aware of and understand this Policy and are given adequate and regular training on it.