

DATA RETENTION SCHEDULE

VERSION: SEPTEMBER 2020

1. INTRODUCTION AND BACKGROUND

- 1.1 This Data Retention Schedule attempts to identify processes which records support, rather than identifying individual types of records. This is for two reasons:
- to ensure that retention periods are applied independent of any format i.e. the same rules apply to a paper file, an e-mail or another electronic document / digital file; and
 - to allow flexibility in developing the schedule to cover new processes and amend existing ones over time.
- 1.2 The Data Retention Schedule is intended to cover the lifecycle of records and information from creation through to destruction or permanent preservation.
- 1.3 Records intended for destruction under the Data Retention Schedule may be destroyed in accordance with the provisions of this schedule. Backup copies stored on alternative media (server / microfilm / paper) should also be destroyed. Typical methods to destroy electronic records, which including holding media such as optical, magnetic and solid state storage, include overwriting, degaussing and physical destruction. In all instances where IT storage media is destroyed, a certificate of destruction shall be provided and held as a permanent record. This is vital to ensure compliance with the requirements of data protection laws. The Diocesan IT Manager can facilitate secure destruction of storage media.
- 1.4 LIMITATION OF SCOPE
- This Data Retention Schedule gathers together retention criteria from a comprehensive best practice review of a wide range of guidance. However, few types of records have specified retention periods given law or in official government guidance. Where no guidance has been given, the Chief Operating Officer will advise retention periods.
- 1.5 OBJECTIVES OF THE RETENTION GUIDELINES
- The aims of the Data Retention Schedule are to:
- prevent the premature destruction of records that need to be retained for a specified period to satisfy legal, financial and other requirements of public administration;

- provide consistency for the destruction of those records not required permanently after specified periods in order to reduce unnecessary storage;
- promote improved records management practices within the Diocese, including concerning the safe destruction of obsolete records;
- create space following procedures to ensure the timely destruction of records;
- assist in identifying records that should be preserved permanently as part of the Diocesan Archive; and
- assist in identifying what data (as opposed to what documents) should be retained to ensure that the principle of data minimisation is adhered to.

1.6 RESPONSIBILITY

It is the responsibility of all staff, volunteers and clergy to ensure that proper records management practices are implemented in line with this guidance.

1.7 DESTRUCTION OF RECORDS

Whenever there is the possibility of litigation, the records and information that are likely to be affected should not be amended or disposed of until the threat of litigation has been removed. Records that are currently (or likely to be) the subject of a request or appeal under data protection laws must not be destroyed until that request or appeal has been completed.

1.8 Staff and volunteers must have any destruction approved in writing by their manager.

1.9 Destruction should be carried out in a secure manner utilising the expertise of external waste management and document destruction providers where appropriate. Redundant or discarded IT equipment, including networked printers, must be securely wiped or destroyed. The Diocesan IT Manager can facilitate secure destruction of disused equipment.

1.10 GENERAL AND MISCELLANEOUS RECORDS

There are some records that do not need to be kept at all, which may be routinely destroyed. This usually applies to information that is duplicated or unimportant and includes:

- 'with compliments' slips;
- printed catalogues and trade journals;
- telephone message slips;
- non-acceptance of invitations;
- trivial electronic mail messages or notes that are not related to Diocesan business;
- requests for stock information;

- out-of-date distribution lists; and
- duplicated and superseded material such as drafts, forms, manuals and copies.

Approval

This policy was approved by the Diocesan Board of Trustees on:	8 October 2020
The next review is due by:	31 October 2022

Type of Record	Nature of data	How long to keep	What actions to take after this
Marriage – key paperwork	Completed Marriage Information form; baptism certificate of Catholic and other Christian party; letters of freedom; Marriage course certificate and permission from bishop if required e.g. convalidation, mixed marriage, disparity of cult, canonical form. Any significant related correspondence.	Permanently	Held securely in parish archive
Marriage – general	Arrangements for the wedding and related general communication	1 year	Destroy securely
Financial records	This includes gift aid; cash books; bank statements; financial returns; accounting records and subsidiary financial records; insurance policies	Current financial year + 6 Gift Aid Declarations 6 years after last used	Destroy securely
Finance – Parish Committee	Records of meetings and decisions	Permanently	Held securely in parish archive
Records relating to bequests and legacies	Documentation from bank or solicitors	Permanently	Held securely in parish archive
Documents relating to property projects	As these form part of the parish history and may be required at a later date there are clear reasons to retain such documentation	Permanently	Held securely in parish archive
CCTV recording	Tapes and other recording devices (NB: storage tapes and/or backs up encrypted and password protected; held securely)	Max. of 30 days before deletion	Destroy securely
Baptisms – preparation	Completed baptism enquiry forms, proof of baptism or confirmation (God-Parent); contact details of families; arrangements for the day	1 year	Destroy securely
Confirmation- preparation	Completed confirmation enquiry forms; consents; sensitive data (i.e. family, medical or behavioural); catechist notes; retreat (where applicable); sponsors Records of catechesis attendance by children	1 year 75-100 years (safeguarding)	Destroy securely Held securely
Weddings – preparation	Correspondence relating to the wedding service; third party contacts;	1 year	Destroy securely
First Holy Communion – preparation	Completed registration forms; parental consents; sensitive data (i.e. family, medical or behavioural); general communications Records of catechesis attendance by children	1 year 75-100 years (safeguarding)	Destroy securely Held securely

Parish Registers	Baptism, First Communion, Confirmation, Marriage, Catechumens, Death, and any others kept by the parish	Permanently	Held securely in parish office and/or archive
Weddings – Civil Registers	Marriage Registrar entries	Permanently	Held securely
Safeguarding	Volunteer applications; DBS processes; requests for advice; investigation records including email trails; training course records;	75-100 years (safeguarding)	Held securely
Parish Census data	Physical or electronic application forms;	Destroy when no longer required	Held securely
Church rotas	Physical and/or electronic forms;	Destroy records when no longer required	Destroy obsolete records securely
Altar Servers	Signing in sheets for altar servers;	75-100 years (safeguarding)	Held securely in parish archive (links to Safeguarding)
Databases, mailing and emailing contact lists	Review on a routine basis and retain the most up to date version	Destroy records when no longer required	Destroy obsolete records securely
Youth Groups	Records of attendance.	75-100 years (safeguarding)	Held securely
	Membership; general communication	Destroy records when no longer required	Destroy obsolete records securely
Parish census database	Records of registered parishioners; general information; volunteering	Destroy records when no longer required	Held securely
Human Resources	Individual HR Files to be retained until employee reaches age 100. Records relating to employees' health and safety must be retained for 40 years after the last entry	Held securely	Destroy obsolete records securely
Property Management	Deeds;	Permanently	Held securely in parish office and/or archive
Parish Organisations	Minutes	Permanently	Held securely in parish office and/or archive
	General correspondence	2+ current year	Retain key correspondence in archive and destroy general correspondence securely

Parish Committees (i.e. Pastoral, Fabric & Finance)	Minutes	Permanently	Held securely in parish office and/or archive
Priest's Official correspondence	Letters, key communications etc..	Permanently	Held securely in parish office and/or archive