

Rayner House and Yew Trees Ltd

RECORD AND DOCUMENT RETENTION AND DESTRUCTION SORP

The purpose of this statement is to ensure that necessary records and documents are adequately protected and maintained and that records that are no longer needed or of no value are discarded at the appropriate time and in an appropriate manner.

Rayner House and Yew Trees Ltd shall retain records for the period of their immediate or current use, unless retention is necessary for historical reference or to comply with contractual or legal requirements. Records include paper and electronic records.

Employees are expected to fully comply with the Record and Document Retention and Destruction policy. An exception to this is if the employee believes or is advised that records are relevant to any litigation or potential litigation. In such cases records must be retained until Trustee Directors (or a delegated person) advise that records are no longer required.

Records fall into a number of categories:

Legal, resident and tenant information, financial, employee and employment information (including personnel files), payroll (including Inland Revenue records), health and safety, buildings, maintenance, insurance and those with general content.

Legal Obligations

Destruction of records is an important part of Rayner House and Yew Trees Ltd approach towards protecting the security of information in its possession. In particular there are legal obligations that require effective adherence to this statement of recommended practice :-

The provisions and principles of the Data Protection Act 2018 require any record containing personal data (name, address, information relating to personal health or financial or legal matters) to be managed in a way that prevents inadvertent disclosure or loss of information. In effect this requires Rayner House and Yew Trees Ltd to destroy personal data of this nature under secure and confidential conditions.

Data Protection legislation states that 'personal data should not be kept longer than is necessary for that purpose'. However, Data Protection law does not prescribe how long data should be retained. It is the responsibility of the Trustee Directors to identify how long data needs to be retained and also the documents of which the data forms part. It is recognised that the document/file retention practice needs to take account of the fact that personal data may be held in files together with other information.

DESTRUCTION SCHEDULE

Type of Document	Minimum Retention	Retention period
<u>Legal records</u>		
Articles of Association	Permanently	Permanently
Charters	Permanently	Permanently
Minutes of Trustee Directors Meetings	Permanently	Permanently
Deeds and titles	Permanently	Permanently
Leases (e.g. Leases relating to property) (after termination)	6 years	7 years
Leases (operating e.g. Equipment)	6 years	7 years
Policy statements	10 years	10 years
Contracts and Agreements	7 years	7 years

Financial

One copy of signed year-end financial statement		Permanently
Including Year End Accounts, Audited Financial Statements, Bank statements Management accounts – year end only Tax and PAYE records Payroll records Invoices – purchase and sales ledger Sage Accounting records – year end back up	7 years	7 years

Resident and Tenants records

(After termination of permanent occupancies/tenancies)

Occupancy agreements and Residents' files		
Permanent	7-10 years	7 years
Short stay		3 years
Tenancy agreements and tenants files		7 years
Medical records	7-10 years	7 years
Applications withdrawn/not processed for Rayner House and Yew Trees		2 years
Waiting lists		2 years

Employment and Employee files

Including time sheets	7 years	7 years
Application forms (not leading to employment)	6 months	6 months

Health and Safety

Accident/Incident Reports	25 – 30 years	30 years
Other records		7 years

Maintenance

Building maintenance		10 years
Equipment maintenance & contracts		10 years

Insurance

Liability Insurance policy documents & certificates	40 years	40 years
---	----------	----------

Buildings

Plans and drawings		Permanently
Building projects documentation		Permanently

Electronic Mail

All e-mails need to be reviewed annually (after 31st March year-end) and deleted correctly using the following procedure:

1. Delete all e-mails in folders (e.g. Inbox, sent, personal folders)
2. Delete deleted folder
3. Empty recycle bin

Computer Data

All folders on each PC to be reviewed annually (after 31st March year –end) and deleted correctly using following procedure:

1. Delete file
2. Empty recycle bin

IT maintenance contract provider will be asked to clear all data from the server older than a year after 31st March year end each year.

Destruction Process

It is the responsibility of all staff to ensure information they are handling is destroyed effectively and securely in accordance with this statement.

Waste bins

Only non confidential information should be placed in waste paper bins. The bins are emptied on a regularly basis (at least weekly) by the cleaners and then disposed of in the paladins for collection by the authorised Local Authority Waste Collection contractor. This waste is not shredded.

Confidential information

Records containing any personal data – name, address, contact details, dates of birth or similar must be shredded.

Highly confidential information

Highly confidential material includes data relating to confidential financial activities of the organisation, policy decisions, payroll or pension data, sensitive personal data as defined under the Data Protection Act 2018 (including but not exclusively relating to racial, ethnicity, health or data relating to criminal offences), records containing private personal information (such as information relating to an individual's home life, personal finances or personal reference) must be shredded by a senior member of staff or at the discretion of Trustee Directors by an outside organisation under secure conditions.

In the event of a high volume of documentation requiring destruction, the Trustee Directors will give due consideration to engaging an outside organisation to carry out this process under secure conditions on their behalf.

This statement of recommended practice is to be reviewed every three years.

Reviewed by: Ms A Bassett, Business Manager – January 2023
Date of next review: January 2026