DONEGAL CENTRE FOR INDEPENDENT LIVING CLG

RECORDS MANAGEMENT & DATA RETENTION POLICY & PROCEDURE

Revision History

Version	***Revision Date***	***Revised by***	***Section Revised***
	12/5/18	Fiona Farren/Bernie Walsh	
	24/08/22	Fiona Farren	

Document Control

Document Owner:	***Document No:***	***Status:*** Draft/Approved	***Date Approved:***
Security Classification: High/Medium/Low	***Next Review Date:***	***Version:*** V1.3	***Department:***

1. Introduction

A variety of records are held by DCIL, financial records, HR records, service user (Leader) healthcare records and general administrative records. Records are traditionally paper-based but increasingly are now being stored electronically also. This document outlines the minimum retention period for records and applies to records of all types regardless of the medium on which they are held.

2. Definition of a Record

A record is defined under the FOI Acts 1997 & 2003 as "any memorandum, book, plan, map, drawing, diagram, pictorial or graphic work or other document, any photograph, film or recording (whether sound or images or both) any form in which data (within the meaning of the Data Protection Act, 1988 and 2003) are held, any other form (including machine-readable form) or device in which information is held or stored manually, mechanically or electronically and anything that is a part or a copy, in any form of any of the foregoing or is a combination of two or more of the foregoing" (Freedom of Information Act, 1997, 2003).

Records created by DCIL should be both accurate and complete. They must provide evidence of the function or activity they were created to document. In order to be evidential, records must be authentic, reliable, have integrity and be useable.

An *authentic* record is one that can be proven to be what it purports to be. In order to ensure that the records created are authentic then records should be dated, timed and signed. They should be placed into the filing system to form part of the retention schedule so that they are protected against unauthorised addition, deletion or alteration.

A *reliable* record is one that can be trusted to be an accurate representation of a function or action taken by DCIL. Therefore, records should contain all relevant facts and be created at the time of the action or transaction or as soon as possible afterwards by a person authorised to carry out that function, action or transaction.

The *integrity* of a record refers to it being complete and unaltered. Once created, additions or annotations to the record can only be carried out by those authorised to do so and any amendment should be explicitly indicated on the record.

A *useable* record is one that can be located, retrieved, presented and interpreted or read whenever or wherever there is a justified need for that information. It should be traceable within a records management system. Record schedules and filing indices that capture the records are essential in ensuring records are useable. In

electronic records, metadata or contextual information is required in addition to the physical transfer of records to ensure their continued usability.

Records retained should be original (or an electronic copy, transferred using the appropriate and verifiable system), unique or of continuing importance to the DCIL. They should have fiscal, legal, administrative or historical purpose.

3. Legal obligation and good practice

DCIL must comply with the provisions of Section 2(1)(c) of the Data Protection Acts 1998 and 2003. The Acts set out the principle that personal data shall not be kept for longer than is necessary for the purpose or purposes for which it was obtained. This requirement places a responsibility on DCIL to be clear about the length of time personal data will be kept and the reasons why the information is being retained. To comply with this rule the DCIL must have a policy on retention periods for personal data that is retained. This policy must include defined retention periods for records and systematic disposal of records within a reasonable period after the retention period expires. Since 2003, Data Protection legislation applies to both electronic and hard copy records.

The DCIL is committed to effective records management retention and disposal to ensure that it:

- Meets legal standards in terms of retention periods
- Optimises the use of space
- Minimises the cost of record retention
- Securely destroys outdated records

The categories of records referred to in this document are as follows:

- Personnel/HR records
- Financial Records
- Other Records

Prior to implementation of this policy, the following issues should be considered:

- Recommended minimum retention periods should be calculated from the end of the calendar month or accounting year following the last entry on the record
- Local requirements/instructions (e.g. if there is live litigation) must be considered before activating retention periods in this schedule
- Decisions should also be considered in the light of the need to preserve records, whose use cannot be anticipated fully at the present time, but which may be of value to future generations

- On-going legislative requirements

4. Assessing the value of Records

This involves determining retention periods for records and any special protection or preservation requirements. Determining a retention period for each record series is based on the value of the series and relevant statutory requirements, regulations and policy. In some instances, for example financial records, the retention periods are fixed.

In other cases, there may not be legal or regulatory retention requirements, in which case a decision must be made on the basis of need and good practice.

There may even be cases where the administrative or operational need of the service deems it appropriate to retain certain records for longer than the statutory retention period.

5. Documenting the Retention Schedule

The implementation of this retention policy should involve the departments who create and use the records as well as (legal) and financial advice, where appropriate. This policy sets out the minimum retention periods and when implementing it the following should be taken into consideration:

- You must comply with relevant legislation
- Avoid trying to accommodate every conceivable need
- Retain information if it is likely to be needed in the future and if the consequences of not having it would be substantial
- Be conservative, avoid inordinate degrees of risk
- Apply common sense
- Ensure systematic disposal of records within a reasonable period after their retention period expires.

Human Resources Records including records retained by line Managers

RECORD	***MINIMUM RETENTION PERIOD***	***FINAL ACTION***
ER/IR Case files	7 years from completion of case	Destroy under confidential conditions
IR/Trade Union negotiations	Indefinitely	
Pay and Conditions (exceptions)	Indefinitely	
Agreements/Circulars	Indefinitely	
Decisions Registers	10 yrs from issuing of Decision (for precedent purposes)	Destroy under confidential conditions
Personnel Files	To be retained for 7 years after the employees' term of service has completed. Retain for duration of employment and hold for 7 years on retirement	Destroy under confidential conditions
Internal/local personnel files – sick leave certs/records and internal issues	Retain for duration of employment	Destroy under confidential conditions
Incident Report Books	10 years	Destroy under confidential conditions
Training Records Hard Copies and files	Indefinitely	Not applicable
Accident/Incident Investigation Report Forms	10 years from date of accident if no claim made in the interim	Destroy under confidential conditions
HR/Health & Safety Investigation Reports	10 years from date of accident if no claim is made in the interim	Destroy under confidential conditions
Recruitment Campaigns	6 years or to the expiry of date of panel	Destroy under confidential conditions
Copy of interview marks	7 years	Destroy under confidential conditions
Copy of interview notes	7 years	Destroy under confidential conditions
Appeals correspondence	7 years	Destroy under confidential conditions
Garda Vetting Application Forms	Original application forms are sent to and are held by the Garda Vetting Unit only. No	Destroy under confidential conditions

	application forms should be held at local level. Confirmation notices are held at local level for 7 years	

RECORD	**MINIMUM RETENTION PERIOD**	**FINAL ACTION**
Complaint Files FOI Requests Data Protection requests Ombudsman/Information Commissioner Requests	It is recommended that a retention period of 7 years applies to files created under; FOI Acts, Data Protection Acts, complaints to DCIL ad Ombudsman or Information Commissioner. Where possible electronic copies of files should be created, therefore avoiding the need to keep the paper copies for the 7 year period	Destroy under confidential conditions
3rd Party Case files, Rights Commissioner, Labour Court, EAT etc	7 years from date of completion of case	Destroy under confidential conditions
Investigation Files, Dignity at Work, Disciplinary etc	7 years from date of completion of investigation	Destroy under confidential conditions
Grievances	7 years from closing of the file	Destroy under confidential conditions
General Correspondence	7 years from closing of the file	Destroy under confidential conditions
Contracts	7 years post termination/expiry. Terms of Employment (info) Act 1994	Destroy under confidential conditions
Annual Leave Records	7 yrs	Destroy under confidential conditions
Letters	7 yrs	Destroy under confidential conditions
Personnel Files	Retain for duration of employment. Hold for 7	Destroy under confidential conditions

	yrs	
Resignations	7 yrs post resignation.	Destroy under confidential conditions
Individual correspondence to Queries	7 yrs from close of file	Destroy under confidential conditions
Minutes of meetings with Company Management	7 yrs	Destroy under confidential conditions
Parental Leave/Force Majeure Leave Maternity Leave Form	8 years As per personnel file	Destroy under confidential conditions
Probation Report Form	As per personnel file	Destroy under confidential conditions
Candidates not qualified or short listed	6 yrs or to the expiry of panel	Destroy under confidential conditions
Applications & CV of candidates who are called for interview	6 yrs or to the expiry of the panel	Destroy under confidential conditions
Candidates shortlisted but not successful at interview or are successful but do not accept job	6 yrs or to the expiry of the panel	Destroy under confidential conditions
Induction Letter	See Personnel file	Destroy under confidential conditions
Copy of eligibility criteria	See Personnel file	Destroy under confidential conditions
Spreadsheet/lists containing candidate contact details, education, current employer, interview scores, order of merit	6 yrs or to the expiry of panel	Destroy under confidential conditions
Invitation to interview letters, reminders and cancellations	6 yrs or to the expiry of panel	Destroy under confidential conditions
Success letters	6 yrs or to the expiry of panel	Destroy under confidential conditions
Regret letters	6 yrs or to the expiry of panel	Destroy under confidential conditions

6. Records Retention Periods – Financial Records

Section 886 of the Direct Tax Acts states that the Revenue Commissioners require records to be retained for a minimum period of six years after the completion of the transactions, acts or operations to which they relate. *These requirements apply to manual and electronic records equally*.

If under investigation or if litigation is likely, files must be held in original form indefinitely, otherwise hold files for the minimum periods set out below. These retention periods are the suggested time periods for which the records should be held based on the organisation's needs, legal and/or fiscal precedence or historical purposes.

Financial Records	***Minimum Period***	***Final Action***
Invoices and Vouchers	Hold for current yr + 6 yrs	Destroy under confidential conditions
VAT Records	Hold for current yr + 6 yrs	Destroy under confidential conditions
Tax Clearance Certs	Hold for current yr + 6 yrs	Destroy under confidential conditions
Debtors Ledger	Hold for current yr + 6 yrs	Destroy under confidential conditions
Income Listings	Hold for current yr + 6 yrs	Destroy under confidential conditions
Income Control Acs	Hold for current yr +6 yrs	Destroy under confidential conditions
Receipt Reconciliation	Hold for current yr + 6 yrs	Destroy under confidential conditions
Paid Cheques	Hold for current yr + 6 yrs	Destroy under confidential conditions
Bank Reconciliations	Hold for current yr + 6 yrs	Destroy under confidential conditions
Bank statements	Hold for current yr + 6 yrs	Destroy under confidential conditions
Procurement card/credit card records	Hold all records for 18 months in hard copy. Hold soft copy of voucher/receipts for 6 yrs	Destroy under confidential conditions
Fixed Assets		
Deeds & Titles of property and assets	Retain indefinitely in original form	Archive
Record of sales & purchases of DCIL property	Retain indefinitely in original form	Archive

Lease Agreements	Hold for current yr + 6yrs	Destroy under confidential conditions
Assets Register	Retain indefinitely in original form	Archive
Depreciation Schedules	Hold for current yr + 6 yrs	Destroy under confidential conditions

Insurance Records	***Minimum Period***	***Final Action***
Property Insurance Policies	Retain indefinitely in original form	Archive
Liability Insurance Policies	Retain indefinitely in original form	Archive
Insurance Claim documents	Hold for 5 years	Destroy under confidential conditions
Incident Report Forms (general)	Hold for 10 years	Destroy under confidential conditions
Incident Report Forms (in specific where exposure to physical, biological or chemical agents)	Hold indefinitely in original form	Archive
Accident Reports	10 years	Archive and/or Destroy under confidential conditions
Other Records		
Financial Statements	Retain indefinitely in original form	Archive
Final Budgetary Reports for any year	Retain indefinitely in original form	Archive
Inventory	Hold for current yr + 6 yrs	Destroy under confidential conditions
Àudit Reports General	Hold for current yr + yrs	Destroy under confidential conditions
Audit Reports used in fraud investigations	Hold for 6 yrs after legal proceedings have been completed	Destroy under confidential conditions
Monthly income and expenditure reports	Hold for 4 years	Destroy under confidential conditions
Dept of Health Circulars and correspondence	Retain indefinitely	Archive
Internal financial policies, accounting standards, procedures etc	Hold in original form until superseded	Store indefinitely electronically
Cancelled chequest	Hold for current yr + 6 yrs	Destroy under confidential conditions
Travel claims	Hold for current yr + 6 yrs	Destroy under confidential conditions
Receipt Books	Hold for current yr + 6 yrs	Destroy under confidential conditions
Purchase Orders	Hold for current yr + 6 yrs	Destroy under confidential conditions
Delivery Dockets	Hold for current yr + 6 yrs	Destroy under confidential conditions

Other Records continued	***Minimum Period***	***Final Action***
Contract and Contract management files	Hold for 2 years after expiry of contract	Destroy under confidential conditions
Payroll		
Taxation records/reports/pension records/calculations/pay awards/payscales/increments	Hold indefinitely	Archive
Authorisations to deduct from pay	Hold until 6 years after employee ceases to be paid	Destroy under confidential conditions
Time sheets/clock cards	Hold until 3 years after employee ceases to be paid	Destroy under confidential conditions
Personal information including changes affecting: name(copy of marriage cert), address, bank Ac details/telephone number etc	Only current personal information should be retained and only where necessary. The retention period reflects the current lifespan of the file	Destroy under confidential conditions
Leave entitlement records (compassionate leave, unpaid leave, sick leave etc	Only current personal information should be retained and only where necessary. The retention period reflects the current lifespan of the file	Destroy under confidential conditions

7. Disposal of records

It is vital that the process of record disposal safeguards and maintains confidentiality of the records. This can be achieved internally or via an approved records shredding contractor, but it is the responsibility of DCIL to satisfy itself that the methods used provide adequate safeguards against accidental loss or disclosure of the records.

A register of records destroyed should be maintained as proof that the record no longer exists. The register should show:

- Name of the file
- Former location of file
- Date of destruction
- Who gave authority to destroy the records

8. What is confidential?

Any record containing personal identifiable information such as name, address, date of birth, PPS number, employee number is deemed confidential. Other records may also be confidential if they contain information about DCIL business or finances. Examples of confidential documents include financial records, payroll records, personnel files or legal documents.

9. Segregation of confidential waste

Only a minority of documents are confidential, and should be disposed in confidential paper bins or security bags. Alternative paper recycling options should be provided for non-confidential paper/magazines.

There are two confidential waste disposal options: on site DCIL shredding, or shredding by an approved contractor.

- DCIL staff may shred confidential records into confetti-like particles using in-house shredders. This shredded paper can be recycled as part of a recyclables collection.

- Bags of confidential records can also be collected for shredding in a shredding contractor's vehicle on-site. *All waste contractors must have a local authority waste collection permit*.

If shredding off-site, confidential waste should be secured until uplift by the shredding contractor. Confidential waste bags/wheelie bins should be exchanged by the shredding contractor, and shredded off-site at an agreed location. If confidential waste is transported off-site, documents should never be legible by members of the public.

10. Data Protection Breaches

If personal data is inadvertently released to a third party without consent, this may constitute a breach of the Data Protection Acts. If a member of staff is aware of a breach or suspected breach of the Data Protection Act they must:

Implement the DCIL's Breach Management Policy, as follows:

1. Identification and Classification – what information was breached and how sensitive is it?

2. Containment and Recovery – minimise the damage and retrieve the data if possible

3. Risk Assessment – what are the potential adverse consequences of this breach?

4. Notification of Breach – notify the Manager who will, if required, notify the Data Protection Commissioner

5. Evaluation and Response – aim to establish how the breach occurred and take action to ensure it doesn't occur again

Comply with requirements/recommendations of the Data Protection Commissioner's office.

11. Summary

This document aims to provide minimum retention periods for the various categories of documents referred to. As circumstances and priorities change it is important that the policy be subject to periodic review.