

Health Research Board – Document Retention Policy

|  |  |
| --- | --- |
| **Title:** | Document Retention Policy |
| **Document Type:** | Policy |
| **Reference/version no:**  | 1 |
| **Status:** | Final |
| **Last Updated:** | 18 May 2018 |
| **Background:** | This retention policy sets out how long HRB will hold different categories of records and data. |

Table of Contents

[The purpose of this policy 3](#_Toc514426045)

[Grounds for processing 3](#_Toc514426046)

[Further processing 4](#_Toc514426047)

[Right of erasure 4](#_Toc514426048)

[Document Retention Procedure 5](#_Toc514426049)

[Types of Documents 5](#_Toc514426050)

[Records 5](#_Toc514426051)

[Disposable Information 6](#_Toc514426052)

[Personal Data 7](#_Toc514426053)

[Confidential Information Belonging to Others 7](#_Toc514426054)

[The role of the Data Protection Officer in Records Management 7](#_Toc514426055)

[How to Store and Destroy Records 9](#_Toc514426056)

[Storage 9](#_Toc514426057)

[Destruction 9](#_Toc514426058)

[Questions about the Policy 9](#_Toc514426059)

[Appendix 10](#_Toc514426060)

[Record Retention Schedule 10](#_Toc514426061)

[Personnel Records 10](#_Toc514426062)

[Payroll Records 13](#_Toc514426063)

[Prospective employees 13](#_Toc514426064)

[Grant applicants 14](#_Toc514426065)

[CCTV 15](#_Toc514426066)

[Databases held in HRB with data supplied by HSE-funded service providers 16](#_Toc514426067)

[Accounting and Finance 17](#_Toc514426068)

[Tax Records 17](#_Toc514426069)

[Legal and Insurance Records 18](#_Toc514426070)

# The purpose of this policy

The HRB are firmly committed to complying with our data protection obligations. In this context, and to achieve consistency and excellence of service, we believe that it is important to have a policy setting out how we manage document retention.

The Data Protection Acts 1988 and 2003 (as amended) (the “DPA”) and, from 25 May 2018, the General Data Protection Regulation (the “GDPR”) impose obligations on us, as a Data Controller, to process personal data in a fair manner which notifies data subjects of the purposes of data processing and to retain the data for no longer than is necessary to achieve those purposes.

Under these rules, individuals have a right to be informed about how their personal data is processed. The GDPR sets out the information that we should supply to individuals and when individuals should be informed of this information. We are obliged to provide individuals with information on our retention periods or criteria used to determine the retention periods.

## Grounds for processing

Under the DPAs and the GDPR, HRB are required to provide data subjects with the legal grounds or lawful basis that they are relying on for processing personal data.

The legal grounds for processing personal data are as follows:

* Consent;
* Performance of a contract;
* Legal obligation;
* Vital interest;
* Public interest;

Explicit consent or an alternative limited lawful basis is required where special categories, also known as sensitive personal data are being processed.

If there is no justification for retaining personal information, then that information should be routinely deleted. Information should never be kept "just in case" a use can be found for it in the future. If we want to retain information about our clients to help us to provide a better service to them in the future, we must obtain their consent in advance.

## Further processing

Further retention of the personal data should be lawful only when it is compatible with the purposes/consent for which it was originally collected. In this case no separate legal basis is required - it should be relied on where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims, the benefit of the owner of the personal data for post contractual obligations or requirements.

## Right of erasure

Individuals have the right to have their personal data erased and no longer processed in the following circumstances:

* where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed,
* where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or
* where the processing of his or her personal data does not otherwise comply with the GDPR.

That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing and later wants to remove such personal data, especially on the internet.

The data subject shall be able to exercise that right notwithstanding the fact that he or she is no longer a child.

# Document Retention Procedure

As an organisation or company, we are required to retain certain records, usually for a specific amount of time. The accidental or intentional destruction of these records during their specified retention periods could result in the following consequences:

* Fines and penalties.
* Loss of rights.
* Obstruction of justice charges.
* Contempt of court charges.
* Serious disadvantages in litigation.
* Disadvantage to the owner of the data

We must retain certain records because they contain information that:

* Serves as HRB’s organisational memory.
* Have enduring business value (for example, they provide a record of a business transaction, evidence HRB’s rights or obligations, protect our legal interests or ensure operational continuity.
* Must be kept in order to satisfy legal, accounting or other regulatory requirements.

We must balance these requirements with our statutory obligation to only keep records for the period required and to comply with data minimisation principles. The retention schedule below sets out the relevant periods for the retention of HRB’s documents.

# Types of Documents

This policy explains the differences among records, disposable information, personal data and confidential information belonging to others.

## Records

A record is any type of information created, received or transmitted in the transaction of HRB’s business, regardless of physical format. Examples of where the various types of information are located are:

* Appointment books and calendars.
* Audio and video recordings.
* Computer programs.
* Contracts.
* Electronic files.
* E-mails.
* Handwritten notes.
* Invoices.
* Letters and other correspondence.
* Magnetic tape.
* Memory in mobile phones and PDAs.
* Online postings, such as on Facebook, Twitter, Vine and other sites.
* Performance reviews.
* Voicemails.

Therefore, any paper records and electronic files, that are part of any of the categories listed in the Records Retention Schedule contained in the Appendix to this policy, must be retained for the amount of time indicated in the Records Retention Schedule.

A record must not be retained beyond the period indicated in the Record Retention Schedule, unless a valid business reason (or a litigation hold or other special situation) calls for its continued retention. If you are unsure whether to retain a certain record, contact the Data Protection Officer.

Our Data Protection Officer is: The Director of Corporate Operations

## Disposable Information

Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a record as defined by this policy. Examples may include:

* Duplicates of originals that have not been annotated.
* Preliminary drafts of letters, memoranda, reports, worksheets and informal notes that do not represent significant steps or decisions in the preparation of an official record.
* Books, periodicals, manuals, training binders and other printed materials obtained from sources outside of HRB and retained primarily for reference purposes.
* Spam and junk mail.

## Personal Data

Personal Data is defined as any data which can identify an individual either on its own or when combined with other data which we possess. Some examples of personal data include names and addresses, email addresses, CVs, details of previous employment, medical records and references. We have specific obligations relating to personal data as set out in the DPA.

## Confidential Information Belonging to Others

Any confidential information that an employee may have obtained from a source outside of HRB, such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used by HRB. Unsolicited confidential information submitted to HRB should be refused, returned to the sender where possible and deleted, if received via the internet.

# The role of the Data Protection Officer in Records Management

Our Data Protection Officer, in conjunction with senior management, is responsible for identifying the documents that HRB must or should retain, and determining, in collaboration with the Legal Department, the proper period of retention. The responsibilities of the Data Protection Officer include:

1. Arranging for the proper storage and retrieval of records, coordinating with outside vendors where appropriate.
2. Handling the destruction of records whose retention period has expired without further notice that the records are being destroyed.
3. Planning, developing and prescribing document disposal policies, systems, standards and procedures.
4. Monitoring departmental compliance so that employees know how to follow the document management procedures and the Legal Department has confidence that HRB’s records are controlled.
5. Ensuring that senior management is aware of their departments' document management responsibilities.
6. Developing and implementing measures to ensure that the Legal Department knows what information HRB has and where it is stored, that only authorised users have access to the information, and that HRB keeps only the information it needs, thereby efficiently using space.
7. Establishing standards for filing and storage equipment and recordkeeping supplies.
8. In cooperation with department heads, identifying essential records and establishing a disaster plan for each office and department to ensure maximum availability of HRB’s records in order to re-establish operations quickly and with minimal interruption and expense.
9. Determining the practicability of and, if appropriate, establishing a uniform filing system and a forms design and control system.
10. In conjunction with the Legal Department, periodically reviewing the records retention schedules and legislation to determine if HRB’s document management program and its Records Retention Schedule is in compliance with legislation.
11. In conjunction with the Legal Department, informing the various department heads of any laws and administrative rules relating to corporate records.
12. In conjunction with the HR Department explaining to employees their duties relating to the document management program.
13. Ensuring that the maintenance, preservation, microfilming, computer disk storage, destruction or other disposition of HRB’s records is carried out in accordance with this policy, the procedures of the document management program and our legal requirements.
14. Planning the timetable for the annual records destruction exercise and the annual records audit, including setting deadlines for responses from departmental staff.
15. Evaluating the overall effectiveness of the document management program.
16. Reporting annually to the Legal Department on the implementation of the document management program in each of [Insert client name]’s departments.

# How to Store and Destroy Records

## Storage

HRB’s records must be stored in a safe, secure and accessible manner. Any documents and financial files that are essential to our organisation’s operations during an emergency must be duplicated and/or backed up at least once per week and maintained off site.

## Destruction

HRB Facilities and/or ICT are responsible for the continuing process of identifying the records that have met their required retention period and supervising their destruction. The destruction of personal data, confidential, financial and personnel-related paper records must be conducted by shredding. The destruction of electronic records must be coordinated with the ICT Department.

The destruction of records must stop immediately upon notification from the Legal Department that a litigation hold is to begin because HRB may be involved in a litigation or an official investigation. Destruction may begin again once the Legal Department lifts the relevant litigation hold.

# Questions about the Policy

Any questions about this policy should be referred to the Data Protection Officer who is in charge of administering, enforcing and updating this policy.

# Appendix

## Record Retention Schedule

In this policy HRB establishes retention or destruction schedules or procedures for specific categories of records. This is done to ensure legal compliance and accomplish other objectives, such as protecting intellectual property and controlling costs. Employees should give special consideration to the categories of documents listed in the record retention schedule below. Avoid retaining a record if there is no legitimate reason for doing so, and consult with the Data Protection Officer or Legal Department if unsure.

### Personnel Records

|  |  |  |  |
| --- | --- | --- | --- |
| Record | Retention Period | Justification for time frame | Legal basis for processing  |
| Benefits descriptions per employee | Permanent | Irish employment law and for pension calculation and record keeping |  |
| Donor records and acknowledgement letters | 7 years | Irish employment law |  |
| Employee applications and resumes | 6 years or where successful, for the duration of the employment plus 7 years from the date of termination of employment | Section 11 of The Statute of Limitations Act 1957 |  |
| Employee benefit plans  | 6 years from when the record was required to be disclosed save pension detail requirements  | Benefit of the employee |  |
| Employee offer letters (and other documentation regarding hiring, promotion, demotion, transfer, termination or selection for training) | 6 years from date of making record or action involved, whichever is later, or 1 year from date of involuntary termination | Benefit of the employee |  |
| Records relating to background checks on employees | 6 years from when the background check is conducted |  |  |
| Employment contracts; employment and termination agreements | 7 years from the date of expiry of the contract or agreement | Benefit of the employee |  |
| Employee records with information on pay rate or weekly compensation | 3 years | Benefit of the employee |  |
| Tax forms | 6 years after date of hire  | Revenue obligation |  |
| Injury and Illness Incident Reports and related Annual Summaries; Logs of work-related injuries and illnesses  | 6 years following the end of the calendar year that these records cover | Statute of Limitations |  |
| Supplemental record for each occupational injury or illness; Log and Summary of Occupational Injuries and Illnesses  | 6 years following the year to which they relate | Statute of Limitations |  |
| Job descriptions, performance goals and reviews; garnishment records | For the duration of the employment plus 7 years from the date of termination of employment | Benefit of employee |  |
| Employee tax records | 6 years from the date tax is due or paid | Revenue obligations |  |
| Medical exams required by law | Duration of employment + 30 years | Benefit of employee |  |
| Personnel or employment records  | 6 years from the date the record was made  | Benefit of employee |  |
| Pension plan and retirement records | Permanent | Benefit of employee |  |
| Pre-employment tests and test results | 2 years from date of termination | Benefit of employee |  |
| Salary schedules; ranges for each job description | 2 years | Benefit of employee |  |
| Time reports | Termination + 3 years | Benefit of employee |  |
| Training agreements, summaries of applicants' qualifications, job criteria, interview records  | Duration of training + 4 years | Benefit of employee |  |

### Payroll Records

|  |  |  |  |
| --- | --- | --- | --- |
| Record | Retention Period | Justification for time frame | Legal basis for processing  |
| Payroll registers (gross and net) | 3 years from the last date of entry | Benefit of employee |  |
| Time cards; piece work tickets; wage rate tables; pay rates; work and time schedules; earnings records; records of additions to or deductions from wages; records on which wage computations are based | 7 years | Benefit of employee |  |

### Prospective employees

|  |  |  |  |
| --- | --- | --- | --- |
| Record | Retention Period | Justification for time frame | Legal basis for processing  |
| Curriculum vitae | 2 years | For future employment opportunities |  |
| Interview notes | 2 years | For future employment opportunities |  |

### Grant applicants

|  |  |  |
| --- | --- | --- |
| Categories of personal information  | Retention period | Justification for timeframe |
| Unsuccessful applications |

|  |  |
| --- | --- |
| Board approval plus 5 years, at annual data cleanse |  |

 | To respond to PQ, evaluation queries |
| Peer reviewers’ comments | In line with application |  |
| Panel members’ comments |

|  |  |
| --- | --- |
| In line with application |  |

 |  |
| Peer and panel members contact details | In line with application |  |
| Successful applications/awards after period of award | EOG plus 10 years, at annual data cleanse | To measure impact of awards/career of PI, scheme review and evaluation activities. |
| Personnel information on awards | EOG plus 10 years, at annual data cleanse |  |
| All associated documents and emails | EOG plus 10 years, at annual data cleanse |  |
| Applicant team contact details in application | EOG plus 10 years, at annual data cleanse |  |
| HRB as partners in EU Projects | In line with data retention requirements of funder |  |
| Outcome Tracker |

|  |  |
| --- | --- |
|  | EOG plus 10 years, at annual data cleanse  |

 |  |
| Public reviewer database | In every email include opt out possibility | Consent |

### CCTV

|  |  |  |  |
| --- | --- | --- | --- |
| Record | Retention Period | Justification for time frame | Legal basis for processing  |
| CCTV recordings | 30 days | Security purposes |  |

### Databases held in HRB with data supplied by HSE-funded service providers

|  |  |  |  |
| --- | --- | --- | --- |
| Record | Retention Period | Justification for time frame | Legal basis for processing  |
| Personal data and sensitive personal data relating to disability service use and need. From NIDD database. | 8 years | As per HCR23 of HSE’s Health Service Record Retention Policy, 2013 | Statutory function |
| Personal data and sensitive personal data relating to disability service use and need. From NPSDD database. | 8 years | As per HCR23 of HSE’s Health Service Record Retention Policy, 2013 | Statutory function |
| Personal data and sensitive personal data relating to disability service use and need. From NASS database (2018 onwards) | 8 years | As per HCR23 of HSE’s Health Service Record Retention Policy, 2013 | Statutory function |
| Personal data and sensitive personal data relating to drug treatment episodes. (NDTRS or LINKS database) | 8 years | As per HCR23 of HSE’s Health Service Record Retention Policy, 2013 | Statutory function |
| Personal data and sensitive personal data relating to psychiatric in-patients held on database (NPIRS or LINK database) | 20 years after date of last contact with service user or 8 years after the death of the service user if sooner | As per HCR23 of HSE’s Health Service Record Retention Policy, 2013 | Statutory function |
| Data relating to service providers including name and contact details of staff | 2 years from conclusion of relationship | Proper management of information |  |

### Accounting and Finance

|  |  |  |  |
| --- | --- | --- | --- |
| Record | Retention Period | Justification for time frame | Legal basis for processing  |
| Accounts Payable and Receivables ledgers and schedules | 7 years | Revenue Requirements |  |
| Annual audit reports and financial statements | Permanent |  |  |
| Annual plans and budgets | 2 years |  |  |
| Bank statements, cancelled checks, deposit slips | 7 years |  |  |
| Business expense records | 7 years |  |  |
| Cash receipts | 2 years |  |  |
| Details of cheques/stubs | 7 years |  |  |
| Electronic fund transfer documents | 7 years |  |  |
| Employee expense reports | 7 years |  |  |
| General ledgers | Permanent |  |  |
| Journal entries | 7 years |  |  |
| Invoices | 7 years |  |  |
| Petty cash vouchers | 3 years |  |  |

### Tax Records

|  |  |  |  |
| --- | --- | --- | --- |
| Record | Retention Period | Justification for time frame | Legal basis for processing  |
| All tax records | 7 years |  |  |

### Legal and Insurance Records

|  |  |  |  |
| --- | --- | --- | --- |
| Record | Retention Period | Justification for time frame | Legal basis for processing  |
| Appraisals | 6 years from termination |  |  |
| Insurance claims/ applications | Permanent |  |  |
| Insurance disbursements and denials | Permanent |  |  |
| Insurance contracts and policies (Director and Officers, General Liability, Property, Workers' Compensation) |  |  |  |
| Leases | 6 years after expiration |  |  |
| Patents, patent applications, supporting documents |  |  |  |
| Real estate documents (including loan and mortgage contract, deeds) | Permanent |  |  |
| Stock and bond records | Permanent |  |  |
| Trademark registrations, evidence of use documents | Permanent |  |  |
| Warranties | Duration of warranty + 7 years |  |  |