BROTHERS OF CHARITY SERVICES IRELAND

RECORDS MANAGEMENT POLICY

Document reference number	2015NP11	Revision No.	4
Approved by	Brothers of Charity Services Ireland		
Signed	Michael Hennessy, Chief Executive		
Approval date	22/5/2025	Next Revision Date	22/5/2028

Contents

Ethos

'We are committed to working with people with an intellectual disability to claim their rightful place as valued citizens. Inclusion is a fundamental principle that underlies all aspects of our work. We believe in the intrinsic value of every person and we aim to further the dignity of all associated with our services.'

'We continue the Brothers of Charity Services' tradition of being open to the best contemporary influences. We want to be inspired by the most creative ideas ...and to ask how we give them concrete expression.'

The Brothers of Charity Services Ethos (2001), Going Forward Together.

1.0 Introduction

The Brothers of Charity Services Ireland (BOCSI) endeavours to offer services/supports in local communities. This enables each person who is supported by our services to positively engage in the social and economic life of their local towns and villages and in doing so, develop a range of relationships that enhance their quality of life.

Our responses are based on the recognition of each person (who is supported by our service) as an individual, an equal citizen with equal rights and an absolute respect of that status. We, therefore, support each person to live their lives based on their own personal visions and choices, to identify and select their personal goals in life and to develop their personal plan to achieve those goals.

2.0 Policy Statement

2.1 Records are essential to enable services and supports to be provided to people supported by services. A BOCSI record performs a number of functions in that it:

- Maintains a history of the person supported.
- Records decisions relating to the care plan of the person supported.
- Supports the workflow of clinical, social care and administrative functions within the organisation for staff.
- Supports the communication of support and clinical information with external sources such as hospitals, the HSE, GPs, statutory bodies, families, and referrals between colleagues.
- Outlines the supports and interventions delivered in the context of legislation, professional standards, guidelines, evidence, and professional and ethical conduct.

2.2 It is the policy of Brothers of Charity Services Ireland (BOCSI) that a systematic, planned and controlled approach will be operated in relation to the management of records. Effective records management is necessary to ensure that the records maintained are authentic, accurate, reliable, and complete and to ensure that they are protected and preserved as evidence to support current and future activities and to ensure current and future accountability.

2.3 In line with a Person Centred approach to service provision and privacy legislation and regulations, records relating to people supported by BOCSI are created and contribute primarily to serve the interests of the individual to whom they relate.

3.0 Purpose

3.1 The purposes of this policy are to:

- Provide a framework to facilitate the consistent management of records which aids efficiency and accountability
- Ensure that security and confidentiality of records are of the highest standard.
- Ensure preservation of records of permanent value and establish archival criteria to maintain and assure continued access to appropriate records.
- Support both protection of privacy and freedom of information requirements throughout the Service.

4.0 Scope

4.1 This policy applies to all records created or received by staff in the course of their duties on behalf of the Service and retained as evidence of the activities of the Service.

4.2 Records can be held in a variety of physical forms including: paper documents both hand written and printed matter (forms, post-it notes etc.), and electronic records held on various electronic devices (i.e. mobile phones, i-pads, tablets, USB keys, recorders, lap tops, hard drives (PCs), SD cards, e-mails, and any form of assisted technology including, door alarms, epi watches, video call bells, and Fitbit etc.), they can come in the form of drawings, photographs, or anything else on which information is recorded.

4.3 Records created or received by the Services can be classified into two main groupings:

- Health and Social Care records containing person specific information relating to the people supported by the Service; and
- Management and Administrative records which includes all other records which are created or received by staff or about staff, and organisational activities/functions in the course of their duties on behalf of the Services.

5.0 Legislation, Guidance, Regulations and Standards

5.1 The most recent legislative impact on Records Management has been the introduction of the EU General Data Protection Regulations (GDPR) and the revised Irish Data Protection Act (2018) which reflect these regulations.

5.2 The key principle of good information and records management is knowing what records/data we have, where they come from, what the data is used for, how long we should keep it, why we have it (lawful basis), and where it is filed. In order to comply with GDPR, BOCSI needs to gather, inform, store, amend, destroy, and protect any data collected in a way that is appropriate to the level of sensitive or personal information recorded. One of the key principles of Data Protection is ensuring that personal information is accurate and is not kept for any longer than is necessary. A robust records lifecycle needs to be implemented and managed and to this end this policy has a retention schedule attached at Appendix 1.

5.3 Article 30 of the GDPR forms part of the accountability principle and this is 'new' to Data Protection. This requires that BOCSI maintain accurate records of what processing of personal and sensitive data is carried out and what controls we have in place to protect and control that processing. This is referred to in the GDPR as your 'Records of Processing Activities' or ROPA for short. BOCSI have an electronic system called ‘Privacy Engine’ in place to aid with compliance. This system records the type of personal data we collect (e.g. name, age, address, telephone number, bank account, and sensitive Information as defined under the Data Protection Act 2018(Part 5. Chapter 1 ((69) and what we do with that data, not individual records. BOCSI Regions to work towards compliance as resources become available.

5.4 Under GDPR BOCSI must ensure that anyone from whom we collect data is fully informed as to what we collect, why we collect it, who we share it with, how and when we store and destroy it and their right to access, amend, or request that we erase their data. To this end the easy to read leaflet attached at Appendix 2 is issued to anyone entering our Service and staff are informed during their induction. Regions that have Council for Quality & Leadership (CQL) Accreditation, under Personal Outcome 15 which requires that people supported consent to sharing their information, in order to comply with Outcome 15, BOCSI have a consent form in place which is signed at admissions. This consent form is then stored on the individual’s Personal Profile.

5.5 The GDPR introduces the concept of Data Minimisation. This means that data collected on a person should be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed’ i.e. no more than the minimum amount of data and files required to carry out a specific function should be collected and kept.

5.6 Further Legislation and Guidance.

- Freedom of Information Act (2014)

- Health Act (2007) and related regulations
- HSE Standards and Recommended Practices for Health Care Records Management QPSD-D-006-3 V3.0
- An Board Altranais, Recording Clinical Practice Guidance to Nurses & Midwives (2002)
- The Health Act (2007) Care and support of Residents in Designated Centres for Persons (Children & Adults with Disabilities) Regulations 2013.
- BOCSI – Data Protection Handbook – GDPR – It's Everyone's Responsibility.
- BOCSI Subject Access Request Procedures (2019)
- BOCSI Data Breach Procedures (2019)
- QQI Core Statutory Quality Assurance Guidelines (2016) QG1-V2
- Health Information and Quality Authority (HIQA) National Standards for Safer, Better Care
- BOCSI Policy on Confidentiality (2019)

6.0 Glossary of Terms and Definitions

Confidentiality

Refers to the limited use of information about individuals supported by the Services or staff, which is obtained by staff during the course of their work. Only information, which is directly relevant to the provision of a service to the individual, should be sought. This information should be treated with the utmost respect at all times in order to preserve the individual's right to privacy and to establish and maintain a good working relationship. These principles should be borne in mind at all times when gathering and sharing information.

Data Concerning Health

As defined by the Data Protection Act (2018) "means personal data relating to the physical or mental health of an individual, including the provision of health care services to the individual that reveal information about the status of his or her health".

Disposition

Disposition is the action taken in regard to the disposal of active records, which can involve physical destruction by means of security shredding or recycling; or transfer to archival storage for selective or full retention.

Personal data

The term "personal data" means any information relating to a living person who is identified or identifiable. If the information can be used on its own or in combination with other information to identify a specific person, then it counts as personal data.

Processing

The term "processing" refers to any operation or set of operations performed on personal data. Processing includes storing, collecting, retrieving, using, combining, erasing and destroying personal data, and can involve automated or manual operations.

Special categories of personal data

Certain types of sensitive personal data are subject to additional protection under the GDPR. These are listed under Article 9 of the GDPR as "special categories" of personal data. The special categories are:

- personal data revealing racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- genetic data and biometric data processed for the purpose of uniquely identifying a natural person,
- data concerning health,
- data concerning a natural person's sex life or sexual orientation.

Services

This refers to the Brothers of Charity Services Ireland.

Records Management

Records management is the application of controls and procedures to the creation, maintenance, use and disposal of records, elements of which include correspondence and forms management, identification of the staff member responsible for the record, records classification, files management, retention scheduling, disaster planning, vital records protection, the administration of inactive records storage, archival preservation activities and destruction of records.

Record

A record is defined under the Freedom of Information Act (2014) as:

(a) a book or other written or printed material in any form (including in any electronic device or in machine readable form),

(b) a map, plan or drawing,

(c) a disc, tape or other mechanical or electronic device in which data other than visual images are embodied so as to be capable, with or without the aid of some other mechanical or electronic equipment, of being reproduced from the disc, tape or other device,

(d) a film, disc, tape or other mechanical or electronic device in which visual images are embodied so as to be capable, with or without the aid of some other mechanical or electronic equipment, of being reproduced from the film, disc, tape or other device, and (e) a copy or part of any thing which falls within paragraph (a), (b), (c) or (d); and

(e) a copy, in any form, of a record shall be deemed, for the purposes of this Act, to have been created at the same time as the record.

Active Records

Active records are records which are required and referred to regularly for current use, and should be retained and maintained in office space and equipment which is readily accessible to users.

Semi-Active Records

Semi-active records are records which are referred to infrequently and are not required regularly for current use. Semi-active records are removed from office space to lower cost off-site storage until they are no longer needed.

Inactive / Closed Records

Inactive records are records for which the active and semi-active retention periods have lapsed and which are no longer required to carry out the functions for which they were created.

Health and Social Care Records

Health and social care records are records which containing person specific information relating to people supported by the Services and include, reports, personal plans, training and education records, file notes, forms, correspondence, emails etc.

Management and Administrative Records

Management and Administrative records includes all records (excluding health and social care records which are person specific) which are created or received by staff in the course of their duties and include the following:

- Financial, payroll and pension records;
- Records of properties, motor vehicles and equipment;
- Legal and insurance records;
- Advocacy, training & evaluation records;
- Human resources records;
- Occupational health records;
- Management and administrative records
- Governance related records; and
- Health and safety Records.

Records Life-cycle

Records life-cycle describes the lifespan of a record from its creation/receipt through the period of its 'active' and 'semi-active' use, then into a period of 'inactive' retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.

Records Retention Schedules

A Records Retention Schedule is a control document that indicates the length of time each record series shall be retained as active before transfer to the semi-active storage; the length of time each series should be retained as semi-active prior to final disposition; and the final disposition of each series. This document serves as the legal authorisation for the disposal of records.

Record Series

Groups of related records, which are created and used with a common purpose, for example, financial records; personnel records; etc.

7.0 Roles and Responsibilities

It is the individual responsibility of all staff who create, receive or access records (irrespective of their format) to ensure that those records are created, filed and stored in accordance with standard practice in the management of those records.

Services Managers, Heads of Departments and Team Leaders must ensure that staff are adequately trained and apply the appropriate guidelines to the creation and maintenance of records in their service area.

8.0 Procedural Guidelines

8.1 Importance of Record Keeping

Records are created to:

- Provide an accurate & comprehensive assessment of a person's needs;
- Collate information that will enhance understanding a person's needs and aid decision-making;
- Enable staff to provide the service which is most beneficial to the person supported;
- Assist in the continuity of care amongst staff;
- Form the basis for planning, care & treatment;
- Accountability - Provide written evidence & a factual record of the service provided;
- Record events and incidents, positive and negative in a person's life;

- Enable people supported by services to access information about services and their interaction with that service;
- Support the communication of information between staff with others involved in the delivery of services;
- Facilitate sharing of information between staff from different areas, to ensure that appropriate support is planned for and provided;
- Enable management to monitor the work of staff and give appropriate advice, support and direction where required;
- Enable information to be collected to provide a basis for evaluating service delivery, managing resources and future planning;
- Provide a means of accountability to whoever is entitled to it, so that actions and decisions that have been taken can be understood and justified in the context of legislation, professional standards, guidelines, evidence, research and professional and ethical conduct; and
- Provide information that may be needed as evidence in court proceedings, internal and external inspections, complaints and investigations.

8.2 Ownership of Records

All records, irrespective of format and type, created or received by staff in the course of their duties on behalf of the Services are the property of the Services and subject to its overall control.

All records created by staff in the course of their duties on behalf of the Services are retained for as long as they are required to meet their legal, administrative, financial and operational requirements, after which time they are either destroyed or transferred to the archives.

8.3 Record Keeping Standards

Records held in the Services should contain information which is relevant to the provision of services. In order to be effective, accurate and safe, records must:

- provide clear evidence of the services and supports planned, decisions made, and supports availed of;
- indicate the method by which the wishes of people supported by services were elicited and how these wishes were included in planning and delivering services;
- be authentic in that they can be proven to be reliable in that the contents of which can be trusted as a complete, factual and accurate representation of the transactions, activities or facts to which they attest (opinions must be clearly recorded as such);
- be legible with clear handwriting and written in black ink so that they can be easily read and reproduced when required;

- be written using respectful language, which is clear and meaningful, so that the report can be readily understood by those who have a legitimate reason to access it. The record must not include jargon, meaningless phrases, irrelevant speculation and offensive, subjective statements. If using abbreviations they must be from an agreed abbreviation list e.g.HSE Code of Practice for Healthcare Records Management – Abbrevations (2010);
- be made as soon as possible after the events to which they relate, (if the date & time of the event differs from that of when the records are written up, this should be clearly noted). The record must demonstrate the chronology of events and all significant consultations, assessments, observations, decisions, interventions and outcomes;
- be accurately dated, timed and signed with the staff member's name printed legibly underneath the signature together with their staff title, Section 43 (8) of the Medical Practitioners Act 2007 requires all registered medical practitioners to quote their Irish Medical Council (IMC) registration number on all medical prescriptions and all other documentation and records, whether in paper or electronic format, relating to their medical practice. All CORU registered professionals must use their registered name and registration number on all records. Best practice requires that a signature bank be maintained in each service support area and kept up to date;
- be written clearly and in such a manner that the text cannot be erased, there should be no blank spaces or pages between entries. If large gaps appear in-between entries, the use of a line to separate them is advisable. Any required alterations should be made by scoring out the error ~~(error)~~ with a single line followed by the dated, timed and signed correct entry. Retrospective entries should be dated, times, signed (and counter-signed as appropriate), with the reason why the retrospective entry is being made clearly stated. It must be clear that the entry is a retrospective entry;
- allow the Services to fulfil it's legal obligations to 3rd party stakeholders e.g. Revenue Commissioners, H.S.E., Health and Safety Authority etc.
- be filed in a manner most appropriate to the type of document to allow easy retrieval e.g. numerical, chronological, alphabetical

8.4 Management of Records

- All records created or received by staff in the course of their duties on behalf of the Services must be held securely and retained for as long as they are required to meet their legal, administrative, financial and operational requirements, after which time they are either destroyed or transferred to the archives.

- The final disposition (either destruction or transfer to the Archives) of records is carried out according to approved schedules as outlined in the *Brothers of Charity Services Ireland Records Retention Schedule*. This schedule is based on a determination of retention requirements as defined in relevant statutes and regulations; administrative and operational requirements and general best practice.
- While the records schedules prescribe the minimum period that records must be retained, service areas and departments must have a reason to keep records for longer periods and record this reason.
- The same records management principles and policies applied to paper records must also govern the management of electronic records. Staff should employ good housekeeping practices in the management of electronic documents i.e. employ a naming convention, have a backup schedule, delete regularly (especially emails), use passwords, produce paper copies if required to maintain the integrity of manual files, etc

8.5 Draft Documents

A draft record is incomplete and need not be placed on file until it has been approved. As a general rule drafts/working papers should be retained if they:

- contain unique information, such as substantive remarks, explanations, interpretations, agreements or comments, which add to a proper understanding of the event/activity;
- contain material which has not yet been transcribed into more formal records (e.g. notes taken at a meeting, notes of a phone call etc.).

  Draft documents should be labelled "draft" with the version and date clearly identified.

8.6 E-Mails and Faxes

E-mails that are evidence of service provision are subject to the basic requirements that apply to all other records. Similarly information issued by fax is subject to the basic requirements that apply to all other records. However, there are some specific requirements for records made or received through e-mail. You should make sure that:

- the e-mail record includes transmission data that identifies the sender and the recipient(s) and the date and time the message was sent and/or received; and
- when e-mail is sent to a distribution list, information identifying all parties on the list is retained for as long as the message is retained.

An e-mail message is a record if it:

- reflects significant actions taken in the course of service provision;
- conveys unique, valuable information about service provision;

- approves or authorises actions;
- constitutes a formal communication between staff e.g. correspondence or memoranda relating to official business;

E-mails that contain the following do not need to be filed:

- meeting announcements;
- meeting arrangements that normally would have been done by telephone;
- copies of memoranda or text sent for information rather than action;
- messages that have only temporary value such as a message that a meeting time has changed;
- messages that contain no evidence of functions and activities of the Services; and duplicate information already documented in existing records.

8.7 Confidentiality and Security of Records

The confidentiality of the information contained in records should be maintained and kept secure at all times. Each service area must provide a secure and confidential environment in which records can be stored. All records must be maintained in an orderly filing system in designated secure storage areas with limited and restricted access. The confidentiality of the person supported by services must be maintained at all times. This duty of confidence continues even after the death of the person supported by services or when the person supported leaves the service or if the staff member is no longer employed by BOCSI.

Confidential records should not be left in any unsupervised place where they may be viewed or accessed inappropriately. Staff must keep their user name and password secure. Passwords/pins/encryption should be enacted on all electronic devices, including mobile phones. Personal data held on portable devices should be transferred or deleted as soon as possible when no longer required.

8.8 Privacy

Privacy is the right of people supported by service to keep personal information from being disclosed. However, in order to provide safe and effective services, personal information must be collected, used and disclosed.

Under the Data Protection Act (2018) and the GDPR the Services has a legal responsibility to:

- Obtain and process the information fairly. Personal data can be obtained directly from the data subject concerned or from third parties (e.g. HSE, family members, medical professionals, references, Garda Vetting etc.) This individual must be informed about the use of their data by BOCSI as set out in the leaflet at Appendix 2;

- Process data under the relevant lawful basis and record the basis and only for the purpose it was originally given (e.g. explicit consent, under contract, vital interests, legitimate activities, public interest, legal claims, the provision of health or social care treatment, medical diagnosis, archiving purposes);
  - keep it accurate and up-to-date;
  - ensure that it is adequate, relevant and not excessive;
  - retain it no longer than is necessary for the specified purpose or purposes;
  - Keep personal data safe and secure;
  - give a copy of his/her personal data to an individual, on request.

These principles entitle people supported by services to:

- feel sure that their personal information is kept safely and securely;
- check that the information held about them is factually correct, complete and up to date;
- have their information used only for its original stated purpose(s);
- know who has access to their personal information and why;
- access and receive a copy of any information held about them;
- change any details that are factually incorrect or remove any information that is not held for a valid reason.

8.9 Access to Records

There is no automatic right of unlimited access by staff to information held in records and files. All staff, students, or other individuals who have access to information, particularly information held on people supported by services, must accept personal responsibility to access only the information they need to know. When data is in the care of staff it must be keep safe and secure from unlawful or unauthorised access, modification or deletion.

Access can be refused to some or all personal information if:

- providing access would pose a serious threat to the life or health of any individual, including the requester;
- providing access would have an unacceptable impact on the privacy of other individuals.
- it is required or authorised by law.

When in constant or regular use, easy access must be available to records by appropriate staff.

The confidentiality of the person supported by services must be maintained at all times. This duty of confidence continues even after the death of the person, or if the staff member is no longer employed by the Services. Staff are required to complete training in confidentiality, be familiar with the Policy on

Confidentiality and sign the written Confidentiality Statement included in all employment contracts.

On admission/enrolment to Services, a person and/or their parents/next of kin are informed in writing (leaflet attached at Appendix 2) of the policies and procedures in relation to access to information contained in records held by the organisation.

8.10 Access to Records by Students

Where students are on placement in the Services as part of their professional training, controlled access to records and files will be permitted. The necessity and relevance of such access should be determined by the student's supervisor in the Services.

It is the responsibility of their supervisor to ensure that students are aware of the importance of confidentiality in relation to information concerning people supported by services and their families and should be directed to review the BOCSI Policy on Confidentiality as part of their induction to the Services.

8.11 Access to Records for Research Purposes

Access to information held may be granted to staff involved in particular research projects which have been authorised by BOCSI (Ethics Committees/Director of Service) subject to:

- People supported by services and/or their family members/being provided with a written explanation of the purposes of the research.
- Specification by the researcher/s of:
    - the precise information they wish to access; and
    - the ways in which the information obtained will be used and shared;

The researcher obtaining written consent for access to the information from the person supported by services and/or their family members. (see BOCSI Research Guidelines -G507)

8.12 Access to Records under the Freedom of Information Act 2014

Under the Freedom of Information 2014 three statutory rights were established in relation to personal information held by public bodies:

- The legal right for each person to access their own information held by public bodies;
- The legal right for each person to have official information relating to him/her amended where it is incomplete, incorrect or misleading.
- The legal right for each person to obtain reasons for decisions affecting him/herself.

The Services endeavour to make information available to the general public or respond to an individual request for information in accordance with the legislation taking into consideration the public interest, confidentiality and the right to privacy of people supported by services.

Access to information under the terms of the Freedom of Information Act is subject to certain exemptions, procedures and time limits.

8.13 Retention of Records

It is a fundamental requirement that all Services' records are retained for a minimum period of time for legal operational, research and safety reasons. The *Brothers of Charity Services Ireland Records Retention Schedule (Appendix 1)* outlines the types of records held by the Services, the associated regulatory framework, the minimum retention periods for records and the actions required when the minimum retention period has been reached. Services areas and Departments must have a reason to keep records for longer periods and must record this reason.

Damaged or Misplaced files must be fixed and relocated to their appropriate home. Lost files are subject to the process as set out in our Data Protection Handbook, Data Breach & Subject Access Request Policies & Procedures.

8.14 Disposal of Records

It is vital that the process of record disposal safeguards and maintains the confidentiality of the records – be they paper or digital. This can be achieved internally or via an approved records shredding contractor, but it is the responsibility of the service 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 exist. This refers to both people who were supported by the service and those who were employed by the Service. The register should show as appropriate:

- Persons' name
- Date of birth – Date of death.
- Dates in Service – date of entry to date of exit.
- Service Areas Attended.
- Date started employment and date completed.
- Position held and location worked.
- Address.
- Name of the file.
- File/record number.
- Former location of file.
- Date of destruction.
- Name of Company engaged to destroy records.

- Policy under which destruction took place e.g. (BOCSI Records Management Policy & Procedure).
- Name of person who gave the authority to destroy the records, job title, & their signature of approval for destruction.
- A register must be kept for the disposal of electronic records (e.g. a records management system or OLIS).

9.0 Revision and Audit

This policy will be reviewed after 3 years or earlier in light of changing legislation or best practice and thereafter at intervals of not more than three years.

10.0 References/bibliography:

- An Bord Altranais. Recording Clinical Practice Guidance to Nurses and Midwives 2002
- Data Protection Act 2018
- Freedom of Information Acts 2014
- General Data Protection Regulations (EU 2018)
- Going Forward Together, The Brothers of Charity Services Ethos (2001)
- Health Act 2007 and related regulations
- The Health Act 2007 (Care and Support of Residents in Designated Centres for Persons (Children and Adults with Disabilities) regulations 2013
- HSE Standards and Recommended Practices for Healthcare Records Management QPSD-D-006-3 V3.0
- QQI Core Statutory Quality Assurance Guidelines (2016) QG1-V2
- JISC infonet, Record management available at (http://www.jiscinfonet.ac.uk/infokits/records-management/)
- Brothers of Charity Services Ireland Research Guidelines
- Brothers of Charity Services Ireland Policy on Confidentiality
- Guidance on Records Retention, National Federation of Voluntary Service Providers July 2019

Appendix 1 Record Retention Schedule

RECORD RETENTION SCHEDULE

Revised March 2024 in compliance with the HSE Records Retention Policy

Record Category and Definitions based on the HSE glossary of terms relating to different record categories processed by the HSE.

Appeals Records

National appeals records are dependent on the eligibility criteria for schemes and services dealt with on an appeal. In most cases these records will contain a mix of personal and sensitive data (medical/clinical).

Protected Disclosure Records

A protected disclosure case file is the compendium of documents filed in pursuant of receiving, screen, referring, assessing/investigating, closing, and reviewing a protected disclosure of a potential wrongdoing.

Child & Family Service Records

Records related to administering and management childcare services such as respite, child in residential care and various multi-d services.

Child Protection & Welfare Records

Records created for the purpose of recognising, responding, reporting and documenting child protection and welfare concerns. Includes records created for the purpose of reporting concerns or providing assistance to TUSLA, HSE, or An Garda Síochána.

Electronic Records

There is no need to retain hard copies of original paper documents/reports that have been scanned electronically, if all of the details from the hard copies are digitised and an appropriate verification process was undertaken to ensure that the digital copy is an exact replica of the original in advance of the destruction of the physical record. The exceptions to this rule are Legally notarised documents e.g. deeds of ownership, incorporate documentation etc.

Environmental Health Records

Records related to regulatory inspection of a range of statutory functions enacted to protect and promote the health of the population. For example, food safety, drinking and bathing water quality investigations. Any international health regulations, infectious diseases investigations, pest control, planning/environment.

Financial Records
Records related to the financial management of an organisation, for example, accounts payable and supplier remittance details.

Freedom of Information Records
All records relating to the administration and management of an FOI request.

Healthcare Records
Records related to the clinical care of a person supported that are generated during the course of their engagement with BOCSI or a GP.

Clinical Audit Records – are records related to quality improvement processes that seek to improve person supported care and outcomes through systematic review of support against explicit criteria and acting to improve the standards of support.

HR Records
Records related to individuals working in an organisation.

Internal Audit Records
Records of audit reports related to the evaluation of its internal controls, governance and accounting process.

Occupational Health Records
Occupational health records provide data which may identify new hazards to which the workforce is exposed and locations within the organisation worthy of increased scrutiny and provide evidence of the efficacy of control measures.

Pathology Records
Records related to carrying out of laboratory tests and delivery of results. Although BOCSI do not carry out any laboratory tests we may have the results of tests on file.

Record Classification
Private – internal BOCSI
Confidential – Staff in specific functional areas.

Restricted – Identified staff only

Subject Access Request (SAR)

Records collated and processed under Data Protection Legislation following a SAR. (Added for BOCSI)

Test & Trace Records

Records related to the management and responses for Covid 19 related outbreak/epidemic including demographic details, referral information, appointment details, vaccinations, contact tracing and test results.

Source: Records Retention Policy (V.1) HSE 15/11/23 (adapted for BOCSI)

Notes:

HIQA Requirement - HR Files

(1) The Registered provider shall ensure that the records set out in Schedules 2,3 and 4 are kept in a designated centre and are available for inspection by the Chief Inspector.

(2) Records kept in accordance with this section and set out in Schedule 2 shall be retained for a period of not less than 7 years after the staff member has ceased to be employed in the designated centre concerned.

***Organisation of Working Time Act (OWT)** – Records 25-(1). An employer shall keep, at the premises or place where his or her employee works or, if the employee works at two or more premises or places, the premises or place from which the activities that the employee is employed to carry on are principally directed or controlled, such records, in such form, if retained by the employer for at least 3 years from the date of their making.

FOI Acts (Information Commissioner), the Data Protection Act 2018 & GDPR (Data Protection Commission), Ombudsman- It is recommended that a retention period of 7 years applies to files created under the and following engagement with the Ombudsman, and the Ombudsman for Children. Where possible electronic copies of files should be created, therefore avoiding the need to keep the paper copies for the 7 year period other than: - those files created under the Child Care Act 1991 shall be held in perpetuity; cases still ongoing; cases that involved legal action; cases that created precedent. It is recommended that a similar policy is applied to non- personal records of this nature.

CQL require training records are kept as outlined under HR Records.

RECORDS OF CHILDREN SUPPORTED BY BOCSI

General Class of Record Held And Description where applicable	Default Retention Period	Final Disposition	Source of Guidance	Lawful Basis under Data Protection Act 2018 & GDPR	Classification Of Record
Records Created under Child Care Act 1991	Hold in perpetuity	Archive	HSE Records Retention Periods 2023	Legal Obligation Child Care Act 1991	Confidential & Special Category data under Article 9 GDPR
Case records and registers: Fostering	Hold in perpetuity	Archive	Child Care (Placement of Children in Foster Care) Regulations, 1995.	Legal Obligation	Confidential & Special Category data under Article 9 GDPR
Case Records and Registers: Placement of Children with Relatives	Hold in perpetuity	Archive	Child Care (placement of Children with Relatives) regulations 1995	Legal Obligation	Confidential & Special Category data under Article 9 GDPR
Case Records and registers: Children in Residential Care	Hold in perpetuity	Archive	Child Care (Placement of Children in Residential Care) Regulations, 1995.	Legal Obligation	Confidential & Special Category data under Article 9 GDPR
Social Work – Records created under Child Care Legislation, housing, Welfare, etc.	Hold in perpetuity	Archive	Child Care (Placement of Children in Residential Care) Regulations, 1995.	Legal Obligation	Confidential & Special Category data under Article 9 GDPR
Child Protection & Welfare Records – records related to child protection & welfare concerns	Hold in perpetuity	Archive	Child Safeguarding under Children first National Guidance for the Protection and Welfare of Children and the Children First Act 2015	Legal Obligation	Confidential & Special Category data under Article 9 GDPR

General Class of Record Held And Description where applicable	Default Retention Period	Final Disposition	Source of Guidance	Lawful Basis under Data Protection Act 2018 & GDPR	Classification Of Record
Child Protection & Welfare Records (2) – records created for the purpose of maintaining a register or logging records of child protection and welfare concerns.	Dispose of when no longer an operational requirement	Destroy under confidential conditions.	HSE Records Retention Policy 2023	Public Task	Confidential & Special Category data under Article 9 GDPR
Other records of children supported by the Service	Retain indefinitely during the lifetime of the person, and for 8 years after death.	Destroy under confidential conditions	HSE Records Retention Policy 2023	Under contract, Consent, and public task could apply.	Confidential & Special Category data under Article 9 GDPR

NOTE: Records created under Child Care Legislation – hold in perpetuity Child Care Act 1991.

RECORDS OF ADULTS SUPPORTED BY BOCSI

General Class of Record Held	Default Retention Period	Final Disposition	Source of Guidance	Lawful Basis under Data Protection Act 2018 & GDPR	Classification of Record
Records of people currently supported	Retain indefinitely during the lifetime of the person, and for 8 years after death – **if serious issues arise keep for up to 30 years after death.**	Destroy under confidential conditions	HSE Records Retention Policy 2023	Legal obligation, (Common law duty to create and maintain records). Public Task	Confidential & Special Category data under Article 9 GDPR
Records of people who are no longer availing of the services.	Retain for 20 years from date of last entry in the records and retain core details. **If serious issues arise keep for up to 30 years after death.**	Destroy under confidential conditions or Archive as appropriate.	HSE Records Retention Policy 2023	Legal obligation and Public Task.	Confidential & Special Category data under Article 9 GDPR
Records of applicants for Services who are not admitted or not entered on a waiting list.	Retain for 10 years	Destroy under confidential conditions.	HSE Records Retention Policy 2023	Legal obligation and Public Task.	Confidential & Special Category data under Article 9 GDPR
Psychology Records of people supported	Retain during the lifetime of the person and for 8 years after death. **If serious issues arise keep for up to 30 years after death.**	Destroy under confidential conditions.	HSE Records Retention Policy 2023	Legal obligations Public Task	Confidential & Special Category data under Article 9 GDPR

General Class of Record Held	Default Retention Period	Final Disposition	Source of Guidance	Lawful Basis under DP Act 2018 & GDPR	Classification of Record
Clinical Records – Referral letters from HSE or GPs etc.	Retain during the lifetime of the person and for 8 years after death. **If serious issues arise keep for up to 30 years after death.**	Destroy under confidential conditions.	HSE Records Retention Policy 2023	Legal obligations Public Task	Confidential & Special Category data under Article 9 GDPR
Clinical Records – Discharge communication	Retain during the lifetime of the person and for 8 years after death. **If serious issues arise keep for up to 30 years after death.**	Destroy under confidential conditions.	HSE Records Retention Policy 2023	Legal obligations Public Task	Confidential & Special Category data under Article 9 GDPR
Social Work Records	Retain during the lifetime of the person and for 8 years after death - **if serious issues arise keep for up to 30 years after death.**	Destroy under confidential conditions.	HSE Records Retention Policy 2023	Legal obligations, vital interest, performing a public task, could apply	Confidential & Special Category data under Article 9 GDPR
Speech & Language Therapy Records	Retain during the lifetime of the person for 8 years after death - **if serious issues arise keep for up to 30 years after death.**	Destroy under confidential conditions.	HSE Records Retention Policy 2023	Legal obligations, vital interest, performing a public task, could apply.	Confidential & Special Category data under Article 9 GDPR
Clinical Audit Records	Retain for 5 years	Destroy under confidential conditions.	HSE Records Retention Policy 2023	Legal obligations and performing a public task could apply	Confidential & Special Category data under Article 9 GDPR

General Class of Record Held	Default Retention Period	Final Disposition	Source of Guidance	Lawful Basis under DP Act 2018 & GDPR	Classification of Record
Photographs (where a photo refers to a particular individual it should be treated as part of their healthcare record).	Retain during the lifetime of the person for 8 years after death **- if serious issues arise keep for up to 30 years after death.**	Destroy under confidential conditions.	HSE Records Retention Policy 2023	Performing a public task or consent could apply.	Confidential & Special Category data under Article 9 GDPR
Healthcare records (excluding records not specified elsewhere in this schedule)	Retain during the lifetime of the person, and for 8 years after death unless legal case pending	Destroy under confidential conditions.	HSE Records Retention Policy 2023	Public Task Legal Obligation Vital Interest	Confidential & Special Category data under Article 9 GDPR
Records relating to a Serious untoward incident	Retain for 30 years after the death of the individual	Destroy under confidential conditions.	HSE Records Retention Policy 2023	Public task, legal obligation Vital Interest	Confidential & Special Category data under Article 9 GDPR
Records of destruction of individual healthcare records (case notes) and other health related records contained in this schedule	Retain indefinitely	Archive	HSE Records Retention Policy 2023	Legal Obligation, Public Task	Confidential & Special Category data under Article 9 GDPR
Admission Registers/Books (where they exist in paper format)	Retain for 8 years after the last entry.	Likely to have archival value. Contact the National Archives (RADD)	HSE Records Retention Policy 2023	Legal Obligation, Public Task	Confidential & Special Category data under Article 9 GDPR

General Class of Record Held	Default Retention Period	Final Disposition	Source of Guidance	Lawful Basis under DP Act 2018 & GDPR	Classification of Record
Discharge Registers/Books (where they exist in paper format)	Retain for 8 years after the last entry.	Likely to have archival value. Contact the National Archives (RADD).	HSE Records Retention Policy 2023	Legal Obligation Public Task.	Confidential & Special Category data under Article 9 GDPR

Human Resource Management Records

This guidance covers the information held on employees past or present, commonly called HRM or personal files. The requirements of the Principal Civil Service Pension Scheme (PCSPS) were the main determinant of the retention periods for these files. Records which document the broader work of HRM are part of the registered file collection. The records held in HRM files cover six broad areas. Employment & Career (Job Application, CV, performance review, training, grievance & discipline, promotion, qualifications, Garda vetting, PPS number, address, bank details, and certificates etc.), Health, Pay, Pension, Welfare, and Security. All six areas of information is not held on one central file, but retained separately. This is to facilitate disposal, to safeguard sensitive information, or because of physical location. HR Records are being created or moved and held on an internal BOCSI data base. The retention of information so held is the same as that for any equivalent paper records.

The physical retention of files, including migration or emulation where software systems are changed or upgraded needs to be implemented and monitored carefully. Data Privacy Impact Assessments are required to be undertaken where new systems are being introduced. All BOCSI Staff are aware of the confidential nature of their work and the requirements to comply with the data protection Acts and GDPR.

The Employment, Labour and Equality Law including the Organisation of Working Time (OWT) Act, the Employment Equality Act, the Workers Protection (Regular part-time employees) Act along with the various SI's under the Safety, Health & Welfare at Work Regulations lay down certain legal requirements concerning record retention. What follows is a record retention schedule for HRM files. If under investigation or if litigation is likely hold HRM files in original form indefinitely, otherwise retain records for the minimum periods set out below. The source of guidance for these identified timeframes along with the aforementioned legislation is the Record Retention Period, HSE Records Retention Policy (V.1) HSE 15/11/23 (adapted for BOCSI)

General Class of Record Held	Default Retention Period	Final Disposition	Source of Guidance	Lawful Basis under DP Act 2018 & GDPR	Classification of Record
<u>HR File</u> • Application & CV • References • Carer's leave records, • contract/personal specification and job description	Retain for 6 years HRM retain for the duration of employment and forward to Pensions on retirement.	Destroy under confidential conditions	Organisation of Working Time Act 1997.	Legal Obligation Under Contract	Confidential
• parental leave • probation form • Sick leave	Pensions on retirement. Pensions retain for 7 years after the death of pensioner.	Destroy under confidential conditions	Organisation of Working Time Act 1997.	Under Contract and legal obligation	Confidential Special category data under GDPR
Garda Vetting Application Forms Standard forms providing individual's consent to be vetted	Retain for 3 years	Destroy under confidential conditions	National Vetting Bureau Act	Under Contract Legal Obligation	Confidential
Garda Vetting Disclosures – Individual vetting results	Held for time of employment or Retain for 3 years if new vetting occurs	Destroy under confidential conditions	National Vetting Bureau Act	Under contract Legal obligation	Restricted Special category data under GDPR
Garda Vetting Risk assessment successful candidate	Held for time of employment or retrain for 3 years	Destroy under confidential conditions	National Vetting Bureau Act	Under contract Legal Obligation	Restricted Special category data under GDPR

General Class of Record Held	Default Retention Period	Final Disposition	Source of Guidance	Lawful Basis under DP Act 2018 & GDPR	Classification of Record
Annual Leave Request Record	Retain for 3 years	Destroy under confidential conditions	Organisation of Working Time Act	Under Contract and Legal Obligation	Confidential
<u>Pensioner file</u> • Refund File • Preserved Benefit Statement • Temporary Service Files Pension Benefit Statements	Retain for 7 years after the death of the pensioner	Destroy under confidential conditions	HSE Records Retention Policy 2023	Legal Obligation and Under Contract	Confidential
Recruitment Board Papers copies of unsuccessful CVs and evaluations of applicants	One master copy should be held for 6 years all other copies should be destroyed.	Destroy under confidential conditions.	HSE Records Retention Policy 2023	Legal Obligation	Confidential
Pension files – calculations & final awards, contributions paid, reports & adjustments, copy of ID; unpaid absences, payroll adjustment, unpaid sick leave, parent leave, unpaid maternity leave, career break, pensionable service, pre entry service, purchased service, records of refunds & transferred service, certificates of service letters.	Retain for 7 years after the death of the pensioner.	Archive	HSE Records Retention Policy 2023	Legal Obligation & Under Contract	Confidential

General Class of Record Held	Default Retention Period	Final Disposition	Source of Guidance	Lawful Basis under DP Act 2018 & GDPR	Classification of Record
Occupational Health Records • Pre-employment medical report	Retain Indefinitely	Archive	HSE Records Retention Policy 2023	Legal Obligation and Under Contract	Restricted
Industrial Relations/Trade Union negotiation	Retain Indefinitely	Archive	HSE Records Retention Policy 2023	Legal Obligation and Under Contract	Confidential
Employer/Industrial Relations Case Files	7 years from completion of the case	Destroy under confidential conditions	HSE Records Retention Policy 2023	Legal Obligation and Under Contract	Restricted
Pay & Conditions (Exceptions)	Retain Indefinitely	Archive	HSE Records Retention Policy 2023	Legal Obligation	Confidential
Training course content and revision, annual programme of training courses, attendance lists for mandatory training. Information and published material on external training courses & 3rd level courses	Retain one set Indefinitely Retain for 3 years after information has been superseded	Archive Destroy by shredding	HSE Records Retention Policy 2023	Legal obligation and under contract Under contract	Confidential
Annual leave request records, sick leave records including certificates, career break applications and correspondence, special leave, jury service leave, compassionate leave record and superannuation.	Sick certificates – destroy after 3 years. Other absence records – 8 years Records required for calculation of pension - Hold for 7 years after death of pensioner.	Destroy under confidential conditions. Destroy under confidential conditions	*OWT Act 1997 (Records) (Prescribed Forms & exemptions) Regulations, 2001, S.I. 473/2001). Parental Leave Acts 1998 & 2006; Carer's Leave Act 2001	Legal obligation and under contract	Confidential

General Class of Record Held	Default Retention Period	Final Disposition	Source of Guidance	Lawful Basis under Data Protection Act 2018 & GDPR	Classification of Record
Duty staff Rosters and Staff Attendance Records	Hold for 6 years after the year to which they relate.	Destroy under confidential conditions.	HSE Records Retention Policy 2023	Legal Obligation & Under Contract.	Private
Unsolicited Job Applications	Retain for 1 year	Destroy by shredding	HSE Records Retention Policy 2023	Consent	Private
Student Work Placement Records, application forms & placement reports	Original – hold for 7 years from completion of placement	Destroy under confidential conditions	HSE Records Retention Policy 2023	Legal Obligation and Consent	Private
Allegations & Complaints	If complaint is unfounded hold in sealed envelope on file for 7 years. Where the matter involved criminal activity these records should be held indefinitely.	Destroy under confidential conditions Archive	HSE Records Retention Policy 2023	Legal Obligation & Under Contract	Restricted
Complaint files Ombudsman & Children's Ombudsman FOI and Subject Access Requests from Staff. Protected Disclosures.	Retain for 7 years. **See Note*.**	Destroy under confidential conditions	Protected Disclosures Act 2014. Data Protection Act 2018 & GDPR. FOI Act 2014. Ombudsman for Children Act 2002. Ombudsman (Amendment) Act 2012	Legal Obligation	Restricted

General Class of Record Held	Default Retention Period	Final Disposition	Source of Guidance	Lawful Basis under DP Act 2018 & GDPR	Classification of Record
Litigation dossiers & records relating to any form of litigation e.g. HR investigative files	If under investigation or if litigation is likely, files must be held in original form Indefinitely or for 10 years after the file is closed.	Archive	HSE Records Retention Policy 2023	Legal Obligation & Under Contract	Restricted
Volunteer Records including those applicants who have been judged to be unsatisfactory	Retain for 10 years after volunteer leaves service.	Destroy under confidential conditions	Volunteering Ireland Guidelines for Organisations	Consent	Confidential

OPERATIONAL & HEALTH & SAFETY RECORDS

General Class of Record Held	Default Retention Period	Final Disposition	Source of Guidance	Lawful Basis under DP Act 2018 & GDPR	Classification of Record
Staff Diaries	Retain for 5 years	Destroy by shredding	HSE Records Retention Policy 2023	Legal obligation and Under Contract	Private
Service Diaries Information relating to individual's care. House Maintenance Log	Retain indefinitely Retain for 3 years	Archive Destroy by shredding	HSE Records Retention Policy 2023	Legal obligation	Confidential
Equipment – inspection Reports Boilers & Lifts	Retain for the lifetime of the installation. If Risk of liability beyond operational life	Destroy by shredding once no longer in use. Retain indefinitely	Health & Safety at Work Act 2005	Under Contract Legal Obligation	Private
Equipment – records of non-fixed equipment, including specifications, test records, maintenance records and logs.	Retain for the Lifetime of equipment. If Risk of liability beyond their operational life.	Destroy by shredding Retain indefinitely	Health & Safety at Work Act 2005	Under Contract Legal Obligation	Private
Manuals (operating)	Retain for the Lifetime of equipment	Destroy by shredding	Health & Safety at Work Act 2005	Under contract & Legal Obligation	Private
Quality Control External records Internal Records	Retain for 2 years Retain for 10 years	Destroy by shredding	Health & Safety at Work Act 2005	Under Contract & legal Obligation	Private
Accident Statistics	Retain Indefinitely	Archive	Health & Safety at Work Act 2005	Legal Obligation	Confidential

General Class of Record Held	Default Retention Period	Final Disposition	Source of Guidance	Lawful Basis under DP Act 2018 & GDPR	Classification of Record
Fire Drill Records	Retain original indefinitely – destroy any copies after 2 years.	Archive	Health & Safety at Work Act 2005	Legal Obligation	Private
Fire Equipment Certificate Copies – Service Areas	Retain for 6 years from date equipment is decommissioned	Destroy under confidential conditions	Health & Safety at Work Act 2005	Legal Obligation	Private
Fire Registers	Retain original in perpetuity	Archive	Health & Safety at Work Act 2005	Legal Obligation	Private
H&S Audits, Site Specific Safety Statement, Insurance correspondence, hazard/Incident Reports, H&SA correspondence, records of meetings, manual handling risk assessment checklists, pregnant employee assessment forms, risk assessment reports, safety inspections, and training records.	Retain original indefinitely	Archive	Health & Safety at Work Act 2005	Legal Obligation	Private Confidential
Safety manuals, Policies & Procedures, codes of practice.	Retain for 2 years after they have been superseded	Destroy by shredding	Health & Safety at Work Act 2005	Legal Obligation	Private

LEGAL RECORDS

General Class of Record Held	Default Retention Period	Final Disposition	Source of Guidance	Lawful Basis under DP Act 2018 & GDPR	Classification of Record
Deeds & Titles of Properties/assets	Retain indefinitely	Archive	HSE Records Retention Policy 2023	Legal Obligation	Restricted
Lease Agreements	Retain for 6 years after expiration of lease	Destroy by shredding	HSE Records Retention Policy 2023	Legal Obligation & Under Contract	Restricted
Plans – building (as built)	Retain for Lifetime of Building	Archive	HSE Records Retention Policy 2023	Legal Obligation	Restricted
Properties – sale & purchase records	Retain indefinitely	Archive	HSE Records Retention Policy 2023	Legal Obligation & under contract	Restricted
Property Register	Retain indefinitely	Archive	HSE Records Retention Policy 2023	Legal Obligation & under contract	Restricted
Legal Opinion Records	Retain indefinitely	Archive	HSE Records Retention Policy 2023	Legal Obligation	Restricted
Records/documents related to any litigation	As advised by the organisation's legal advisor. All records to be reviewed. Normal retention is 10 years after the file is closed.	Archive or destroy under confidential conditions subject to legal advice.	HSE Records Retention Policy 2023	Legal Obligation	Restricted

INSURANCE & VEHICLE RECORDS

General Class of Record Held	Default Retention Period	Final Disposition	Source of Guidance	Lawful Basis under DP Act 2018 & GDPR	Record Classification
Insurance Policies Properties (Owned) Properties (Leased)	Retain indefinitely	Archive	HSE Records Retention Policy 2023	Legal Obligation	Confidential
Insurance Policies Motor Vehicles	Retain indefinitely	Archive	HSE Records Retention Policy 2023	Legal Obligation	Confidential
Insurance Policies State Claims Agency Communications & Documents	Retain indefinitely	Archive	HSE Records Retention Policy 2023	Legal Obligation	Restricted
Insurance Policies Directors & Auditors	Retain indefinitely	Archive	HSE Records Retention Policy 2023	Legal Obligation	Restricted
Vehicle Records – Drivers log books, vehicle mileage records	Retain for 5 years unless litigation ensues	Destroy by shredding	HSE Records Retention Policy 2023	Legal Obligation and under contract	Private
Vehicle Records – Registration Records	Retain for 5 years unless litigation ensues	Destroy by shredding	HSE Records Retention Policy 2023	Legal Obligation and under contract	Private
Vehicle Accident Reports	Retain original indefinitely and copies for 2 years	Archive	HSE Records Retention Policy 2023	Legal Obligation and under contract	Confidential
Copies of staff driving licences	Retain until superseded	Destroy under confidential conditions	HSE Records Retention Policy 2023	Legal Obligation & under contract	Confidential
Copies of Staff Motor Insurance Policies & indemnity	Retain until superseded	Destroy under confidential conditions	HSE Records Retention Policy 2023	Legal Obligation & under contract	Confidential

General Class of Record Held	Default Retention Period	Final Disposition	Source of Guidance	Lawful Basis under DP Act 2018 & GDPR	Record Classification
Insurance Certificates	Retain until superseded	Destroy by shredding	HSE Records Retention Policy 2023	Legal Obligation	Private
Incident Reports	Retain original indefinitely and copies for 2 years	Archive	HSE Records Retention Policy 2023	Legal Obligation and under contract	Confidential
Insurance claim documents	Retain indefinitely	Archive	HSE Records Retention Policy 2023	Legal Obligation	Restricted

FINANCIAL RECORDS

The decision on how long to keep a financial record before destroying it is influenced by statutory requirements set out in the Companies Act 2014, audit, revenue commissioners' guidelines, and the acceptability of copies as "evidence in a court of law". Archiving financial information should be considered noting that some information is of a sort, which should be retained in perpetuity e.g. annual financial statements.

General Class of Record Held	Default Retention Period	Final Disposition	Source of Guidance	Lawful Basis under DP Act 2018 & GDPR	Classification of Record
Annual Financial Statements	Retain indefinitely	Archive		Legal Obligation	Private
Audit Reports	Retain for 6 years	Destroy by shredding		Legal Obligation	Confidential
Bank Reconciliation	Monthly retain for 1 year Year end retain for 6 yrs	Destroy by shredding		Legal Obligation	Confidential
Bank Statements	Original retain for 10 years copies 2 years	Destroy by shredding		Legal Obligation	Confidential
Purchase ledger Invoices Payments	Original retain for 6 yrs copies retain for 2 years	Destroy by shredding		Legal Obligation and under contract	Confidential
Cancelled Cheques	Retain for 6 years	Destroy by shredding		Legal Obligation	Confidential
Capital Projects Invoices, quotations, and tenders	Retain for 12 years from end of project	Appraise and evaluation for Archiving or Destroy under confidential conditions		Legal Obligation and under contract	Confidential
Circulars F Team & Dep. of Health & Children	Retain indefinitely	Archive			Private
Contract Management files	Retain for 2 years after expiry of contract	Destroy by shredding			Confidential
Control Account Reports	Retain for 6 years	Destroy by shredding			Confidential
Depreciation Schedules	Retain for 6 years	Destroy by shredding			Confidential

General Class of Record Held	Default Retention Period	Final Disposition	Source of Guidance	Lawful Basis under DP Act 2018 & GDPR	
Management Account Reports	Retain for 1 year in Service areas and Retain for 6 years at Head Office	Destroy by shredding		Legal Obligation	
Purchase Order and Receipt Books	Retain original for 6 years copies for 2 years	Destroy by shredding		Legal Obligation	
Sales Ledger Invoices / Receipts	Retain original for 6 years copies for 2 years	Destroy by shredding		Legal Obligation	
Supplier Proposals	Retain for 2 years after award of contract	Destroy by shredding		Legal Obligation and under contract	
<u>Tenders</u> Invite to tender Successful Unsuccessful	Retain for 2 years Retain for tender period plus 6 years	Destroy under confidential conditions		Legal Obligation and under contract	
Tax Clearance Certificates	Retain until superseded by most recent Cert or for 6 years from last supplier interaction.	Destroy by shredding		Legal Obligation and under contract	
Travel Claims	Retain the original for 6 years and copies after 2 years.	Destroy under confidential conditions		Legal Obligation and under contract.	
Salary Scales/National Wage Agreements	Retain indefinitely	Archive		N/A	
Staff complement file/census returns/employment controls	Retain indefinitely	Archive		Legal Obligation and under contract	

General Class of Record Held	Default Retention Period	Final Disposition	Source of Guidance	Lawful Basis under DP Act 2018 & GDPR	Classification of Record
Weekly timesheets – Excel/word	Retain for 6 years to which they relate	Destroy under confidential conditions	OWT Act stipulates 3 years.	Legal Obligation and under contract.	
General Financial Correspondence	Retain for 12 years	Destroy by shredding		N/A	
House Accounts Receipts/Invoices Reports	Retain for 6 years at head office	Destroy under confidential conditions		Legal Obligation and public task	
Internal Financial policies, accounting standards & procedures	Retain for 6 years at head office	Destroy by shredding		N/A	
Journals	Retain for 6 years	Destroy by shredding		N/A	
Paid cheques/copy cheques/electronic transfers	Retain for 6 years	Destroy under confidential conditions		Legal Obligation and under contract	
Payment Authorisation books	Retain for 2 years	Destroy under confidential conditions		Legal obligation and under contract	
Property Accounts/fund Accounts of people supported by the Service	Retain for 6 years after death	Destroy under confidential conditions		Legal obligation, public task	
Buildings & engineering works, key records e.g final accounts, surveys, site plans, bills of quantities)	Retain indefinitely	Archive		Legal obligation and public task. If no personal and sensitive information then N/A	

General Class of Record Held	Default Retention Period	Final Disposition	Source of Guidance	Lawful Basis under DP Act 2018 & GDPR	Classification of Record
Petty Cash	Retain original for 6 years and copies for 2 years	Destroy under confidential conditions		Legal obligation and under contract.	
Listings/payslips	Retain indefinitely	Archive		Legal Obligation & under contract	
P35 Reports	Retain indefinitely	Archive		Legal Obligation & under contract	
P60 Reports	Retain indefinitely	Archive		Legal Obligation & under contract	
Payroll Creditors – VHI, AVC, INO	Retain indefinitely	Archive		Legal Obligation & under contract	
Payroll Month end Reports	Retain indefinitely	Archive		Legal Obligation & under contract	
Payroll Salary Adjustments	Retain indefinitely	Archive		Legal Obligation & under contract	
Payroll Union Contributions	Retain indefinitely	Archive		Legal Obligation & under contract	
Payslips	Retain indefinitely	Archive		Legal Obligation & under contract	

CORPORATE GOVERNACE RECORDS

Governance records can be defined as any records an Irish Company is required to keep during the course of business. These records can include anti-money laundering documentation, company files in line with the companies Act 2014, company accounts, tax records and other documents linked to the company. This section deals with those records that do not relate to the company accounts or financial records. These Records are kept in the Head Office of the Company.

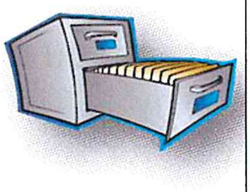
General Class of Record Held	Default Retention Period	Final Disposition	Source of Guidance	Lawful Basis under DP Act 2018 & GDPR	Classification of Record
Company Seal	Keep for 6 years after the company is dissolved.	Destroy under confidential and secure conditions or Archive	Companies Act 2014	N/A	Restricted
Company Document Arts & Memo (constitution) Charter, legal documents of incorporation etc.	Keep for 6 years after the company is dissolved.	Destroy under confidential and secure conditions or Archive	Companies Act 2014	Legal Obligation	Private
Board minutes of meetings & associated papers, agendas & reports. Written Resolutions Published Statutory Notices Copy of company letterhead Board Committee minutes of meetings & associated papers, agendas & reports.	Keep for 6 years after the company is dissolved.	Destroy under confidential and secure conditions or Archive	Companies Act 2014	Legal Obligation	Confidential
Copies of Board documentation e.g. Governance checklists, Board Training and Induction, Handbooks, Policies & Procedures for the operation of the Board, Codes of Conduct, Signed SLAs, legal and financial advice.	Keep for 6 years after the company is dissolved.	Archive	Companies Act 2014	Legal Obligation	Confidential

General Class of Record Held	Default Retention Period	Final Disposition	Source of Guidance	Lawful Basis under DP Act 2018 & GDPR	Classification of Record
Board Expense sheets, various registers, register of members, register of directors & secretaries, register of directors & secretary's interests, conflict of interest statements, Beneficial Ownership registration on RBO portal, list of directors for rotation purposes. register of debenture holders and register of company assets.	Keep for 6 years after the company is dissolved.	Archive	Companies Act 2014 Charities Act 2009 Ethics & Standards in Public.	Legal Obligation	Confidential
Reports to State Bodies from the Board e.g. copy of returns to the CRO, B10 Forms, CRA, Trustee Declaration forms, Annual Reports and Strategic Plans.	Keep for 6 years after the company is dissolved.	Archive	Companies Act 2014	Legal Obligation	
Employers' liability Insurance Policy & Schedule	Keep for 40 years from the date the company is dissolved.	Destroy under confidential conditions or Archive as appropriate	Companies Act 2014	Legal Obligation	

Appendix 2 **Leaflet for distribution at Point of Entry**

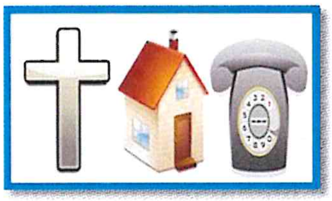
BROTHERS OF CHARITY SERVICE IRELAND - DATA PROTECTION & GENERAL DATA PROTECTION REGULATIONS - INFORMATION SHEET

	How does change in Data Protection affect you or you child? Data Protection means that any information we collect when you access our services on you or your child is stored properly and access is restricted to those who are directly involved in the delivery of the supports.
	From the 25th May 2018 the General Data Protection Regulation or GDPR came into force in Ireland. This is an update to the existing data protection law, now the Data Protection Act 2018. GDPR requires organisations like the BOCSI to be more accountable to you about the use, storage, and destruction of your information. It gives you greater control over you or your child's information by allowing you through a Subject Access Request system access to all data we may have on you. It allows you to request that the data is shared with you, updated, or deleted. It allows us to refuse to delete data if it is required for the provision of services or if we are legally obliged to do so under other legislation e.g. the Health Acts.

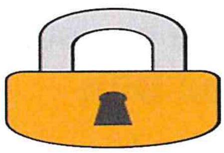


The Brothers of Charity Services Ireland collects and keeps personal and sensitive information about you or your child in a secure and confidential environment. We only share this information to ensure we can provide a good service, or if required by law.

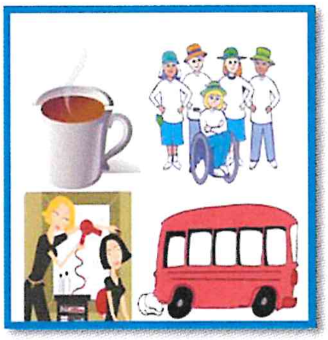
This information can include any of the following

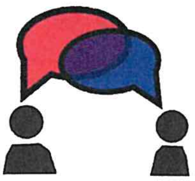
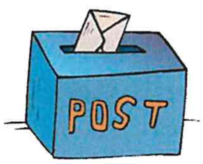


- Name
- Gender
- Date of birth
- Religion
- Address
- Phone numbers
- Next of Kin
- Medical history
- Behaviour Support Plans
- Financial details
- Multi-disciplinary Reports
- Dental and GP appointments
- Photographs
- Scans with your name on them



BOCSI Must keep your information Safe.

	People we may share information with include • Staff who work with you or your child • State Bodies who under legislation require the information • Family members who you have said we can. • Healthcare professionals • The Hospital • Law enforcement bodies
	We have your information so that we can give you or your child the best and most appropriate services and supports. The Data Protection law says the information must be kept accurately and be up to date.
  	You can see the information about you or your child if you want to. This is your right. There are some exemptions to this and if they apply this will be explained to you in detail. We must get back to you within 30 days of you asking for access to your information under Data Protection using our Subject Access Request Form. Contact your Regional Data Protection Representative for a copy of the form or look on our web site www.brothersofcharity.ie

	If we refuse to give you the information we will tell you why. If you are not happy with our response you can contact the Data Protection Commissioner, 21 Fitzwilliam Sq. South, Dublin 2, D01 RD28 - Phone 01 761104800 and make a complaint. They Data Protection Commissioners office will check what information we have and review our decision. If they don't agree they will tell us to give you your information or they will agree with us and let you know why.
	If the Brothers of Charity Services Ireland wants to use your information for any other purpose outside service delivery, we must ask you first and obtain your written consent.
 	You can contact your Regional Data Protection Representative at any time for help or advice on how to access information under the Data Protection Act. OR the BOCSI Data Protection Officer by email at DPO@bocsi.ie. or by post at: DPO, BOCSI, Kilcornan House, Clarinbridge, Co Galway H91 K2E9