Social Care Association of Ireland (SCI) Data Retention Policy

1. The purpose of this policy

The Data Protection Acts 1988 and 2003 (the DPA) (as amended) and, from the 25th of May 2018, the General Data Protection Regulation (the GDPR) imposes 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.

1.1. Grounds for processing

Under the DPAs and the GDPR, Social Care Association of Ireland (SCI) is 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; or Legitimate interests.
- Explicit consent is required where special categories, also known as sensitive personal data are being processed.

Social Care Association of Ireland (SCI) may be able to rely a number of legal bases for collecting personal data. For example, as employers, Social Care Association of Ireland (SCI) can justify processing an employee's personal data as necessary for the performance and offering of a contract and as part of a statutory requirement for recruitment for the services that Social Care Association of Ireland (SCI) provides.

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 members or employees to help us to provide a better service to them in the future, we must obtain their consent in advance.

1.2. Further processing

Further retention of the personal data should be lawful only when it is compatible with the purposes 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.

1.3. 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, or
- Where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her,
- 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.

2. Document Retention Procedure

As a 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.

We must retain certain records because they contain information that:

- Serves as Social Care Association of Ireland's (SCI) corporate memory.
- Have enduring business value (for example, they provide a record of a business transaction, evidence Social Care Association of Ireland's (SCI) 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 Social Care Association of Ireland (SCI)' documents.

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

3.1. Records
A record is any type of information created, received or transmitted in the transaction of Social Care Association of Ireland's (SCI) 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 programmes.
- Contracts.
- Electronic files.
- E-mails.
- Handwritten notes.
- Invoices.
- Letters and other correspondence.
- Memory in mobile phones and PDAs.
- Online postings, such as on Facebook, Twitter 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 Charlotte Burke who can be contacted at cpd@socialcareireland.ie.

3.2. 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 Social Care Association of Ireland (SCI) and retained primarily for reference purposes.
- Spam and junk mail.

3.3. 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.

3.4. Confidential Information Belonging to Others
Any confidential information that an employee may have obtained from a source outside of Social Care Association of Ireland (SCI), such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used by Social Care Association of Ireland (SCI) for any other reason, other than what it was obtained for. Unsolicited confidential information submitted to Social Care Association of Ireland (SCI) should be refused, returned to the sender where possible and deleted, if received via the internet.

4. The role of the Data Protection Officer in Records Management

Our Data Protection Officer, in conjunction with the Directors, is responsible for identifying the documents that Social Care Association of Ireland (SCI) must or should retain, and determining the proper period of retention.

The responsibilities of the Data Protection Officer include:

- Arranging for the proper storage and retrieval of records, coordinating with outside vendors where appropriate.
- Handling the destruction of records whose retention period has expired.
- Planning, developing and prescribing document disposal policies, systems, standards and procedures.
- Monitoring compliance so that members know how to follow the document management procedures and the Directors have confidence that Social Care Association of Ireland's (SCI) records are controlled.
- Ensuring that the Directors are aware of SCI's document management responsibilities.
- Developing and implementing measures to ensure that the Directors know what information Social Care Association of Ireland (SCI) has and where it is stored, that only authorised users have access to the information, and that Social Care Association of Ireland (SCI) keeps only the information it needs, thereby efficiently using space.
- Establishing standards for filing and storage equipment and record-keeping supplies.
- In cooperation with the Directors, identifying essential records and establishing a disaster plan for Social Care Association of Ireland (SCI) to ensure maximum availability of Social Care Association of Ireland (SCI)' records in order to re-establish operations quickly and with minimal interruption and expense.
- Determining the practicability of and, if appropriate, establishing a uniform filing system and a forms design and control system.
- In conjunction with the Directors, periodically reviewing the records retention schedules and legislation to determine if Social Care Association of Ireland's (SCI) document management programme and its Records Retention Schedule is in compliance with legislation.
- In conjunction with the Directors, informing the Members of any laws and administrative rules relating to corporate records.

- Ensuring that the maintenance, preservation, microfilming, computer disk storage, destruction or other disposition of Social Care Association of Ireland's (SCI) records is carried out in accordance with this policy, the procedures of the document management programme and our legal requirements.
- Planning the timetable for the annual records destruction exercise and the annual records audit, including setting deadlines for responses from staff.
- Evaluating the overall effectiveness of the document management programme.
- Reporting annually to the Board of Directors on the implementation of the document management programme.

5. How to Store and Destroy Records

5.1. Storage
Social Care Association of Ireland's (SCI) records must be stored in a safe, secure and accessible manner. Any documents and financial files that are essential to our business operations during an emergency must be duplicated and/or backed up at least once per week and maintained off site.

5.2. Destruction
Social Care Association of Ireland (SCI) is 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 records must be conducted by shredding. To this end, we have secured the services of www.greatwhite.ie, who are contracted to collect all items for shredding from the Social Care Association of Ireland (SCI) Office, whereby all items are shredded at their premises and confirmation of shredding is provided to Social Care Association of Ireland (SCI) in the form of a Destruction Certificate. The destruction of electronic records must be coordinated with the Data Protection Officer.

The destruction of records must stop immediately upon notification from the Directors that a litigation hold is to begin because Social Care Association of Ireland (SCI) may be involved in a litigation or an official investigation. Destruction may begin again once the Directors lift the relevant litigation hold.

6. 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.