Keeping Records and Data Protection Policy

Policy Data Sheet

Policy Name:	Keeping Records and Data Protection Policy
Document Reference:	BLG0010
Version Number:	8
Ratified By:	Executive Team
Exec Team Ratified Date:	Apr 18
Board approval needed?	Yes CSGB
Board Ratified Date:	April 18
Review Period:	2 years
Review Date:	April 2020

Contents:

ADVICE: Before using this document you should ensure that you have the most up-to-date version. If you are referring to a printed version it may be out-of-date. If in any doubt please check with Human Resources.

Keeping Records and Data Protection Policy

1. Aim of the Policy

Good record keeping and data protection are key to effective information governance and essential for the planning and delivery of high quality, safe and efficient services and business systems. The Big Life group collects, holds and processes personal data about many individuals including clients, staff, suppliers and stakeholders. This policy aims to ensure that all records, both electronic and paper are accurate, secure, accessible to the right people at the right time, and kept for the appropriate period of time. It ensures that The Big Life group is compliant with data protection legislation and commissioners' quality standards.

2. Scope of the Policy

This policy covers all the systems and proceses required to ensure that The Big Life group operates a comprehensive system for the completion, use, storage, retrieval, archiving and disposal of all records (electronic and manual) which include personal identifiable or sensitive information.

This policy contributes to the Information Governance Framework and is supported by associated policies (see Section 11)

Failure to keep records in line with this policy and to work within data protection guidelines will be treated as a disciplinary matter and may also lead to a professional governing body being informed if appropriate

3. Roles and Responsibilities

Board
The Board is responsible for ensuring that there are effective policies, equipment and systems for the completion, use, storage, retrieval, archiving and disposal of all records.

Clinical and Service Governance Board
Receives reports on any incidents relating to records, ensuring lessons are learned and implemented. It ensures that this policy is regularly reviewed and updated in line with best practice and that there are systems in place for auditing compliance with the policy.The information governance lead and Data Protection Officer for The Big Life Group is a member of this board.

Executive Team
The Executive Team is responsible for ensuring that this policy is disseminated to staff and training is provided. They will ensure that there are resources available to protect the storage and transfer of records, and for the training of staff.

Leadership Team
The Leadership Team are responsible for ensuring that the policy is implemented in their business areas and taking appropriate action to investigate, report and mitigate any incidents regarding record keeping.

Caldicott Guardian
The Caldicott Guardian is responsible for protecting the confidentiality of personal information and enabling appropriate information sharing. The Caldicott Guardian is a member of the Board, Clinical and Service Governance Board, and The Executive Team.

Data Protection Officer/Information Governance Lead
Provides assistance to monitor internal compliance, informs and advises on data protection obligations, provides advice regarding Data Protection Impact Assessments (DPIAs) and acts as a contact point for data subjects and the supervisory authority. Ensures the Framework and Policies are updated in line with best practice and learning; and participates in the investigation and reporting of information incidents.

Quality Lead
The Quality Lead is responsible for maintaining an up-to-date registration for each business within the group, with the Information Commissioner Office,

Managers
Are responsible for ensuring that their staff teams operate within this policy. They will ensure that any breach of the policy is investigated and mitigated, and is reported as an incident.

Staff
Are required to ensure they understand and operate in accordance with this policy. All relevant staff will receive data protection/record keeping training as a part of their mandatory training within their probationary period. The training will enable staff to be responsible for producing and updating records accurately and in a timely manner. Staff are responsible for the safe use of confidential records and for reporting any incident relating to the loss of information, or breach of confidentiality in line with the information goverance framework and this policy.

4. Data Processing

The Data Protection Act 1998 (DPA) came into force on 1st March 2000, and it is being updated in 2018 to comply with the EU's General Data Protection Regulation (GDPR). In the UK, compliance with data protection legislation is overseen by The Information Commissioner's Office (ICO). Data protection legislation sets out rules for processing personal data.

Personal data is any information relating to a person who can be directly or indirectly identified. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect

information about people. Data protection legislation applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data. Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of data protection legislation depending on how difficult it is to attribute the pseudonym to a particular individual.

Special Category data –as defined in GDPR (similar to the definition of sensitive personal data in the Data Protection Act) is data that is more sensitive. For example, information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life
- sexual orientation

Personal data relating to criminal convictions and offences are not included, but extra safeguards apply to its processing

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Within the GDPR, personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, (having regard to the purposes for which it is processed), is erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data was processed
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The lawful bases for processing personal data are set out in the GDPR. At least one of these must apply whenever personal data is processed:

- **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
- **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- **Vital interests:** the processing is necessary to protect someone's life.
- **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

In order to process special category data, one of the following conditions needs to apply ***in addition*** to one of the six core lawful bases for processing personal data

- The data subject has given explicit consent to the processing of the personal data for one or more specified purposes
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- Processing relates to personal data which is made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee,

medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Data Subject: The individual that is the subject of the data

Data Controller: a person or organisation that (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed

Data Processor: any organisation or person (not an employee of the data controller) who processes the data on behalf of the data controller.

Processors have specific legal responsibilities, for example to maintain records of personal data and processing activities. Processors have legal liability if they are responsible for a breach. Controllers have further obligations on them to ensure contracts with processors comply with data protection legislation. In most case businesses within the group will be data controllers for the information they hold. However in partnership arrangements or the delivery of commissioned services, this responsibility may be held by – or shared with – another organisation.

All businesses within the group would be defined by the ICO as data controller for at least some of the information they process. Each business must maintain an up-to-date registration as a data controller with the Information Commissioner Office; renewing registration is the responsibility of the Group's Quality Lead. All new businesses must be registered with the ICO.

The group must maintain an up-to-date record of its data processing activities; appropriate legal bases must apply to all data processing activities. Each service area should contribute to this.

5. Data Subject Rights

The GDPR provides the following rights for individuals:

- The right to be informed

- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

6. Right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. All services should provide the following information to individuals at the time we collect their personal data from them, either in a policy, a standalone privacy notice, or attached to a consent form.

- The name and contact details of our organisation.
- The name and contact details of our representative (if applicable)
- The contact details of the data protection officer.
- The purposes of the processing.
- The lawful basis for the processing
- The legitimate interests for the processing (if applicable)
- The categories of personal data obtained (if the personal data is not obtained from the individual it relates to)
- The recipients or categories of recipients of the personal data
- The details of transfers of the personal data to any third countries or international organisations (if applicable)
- The retention periods for the personal data.
- The rights available to individuals in respect of the processing
- The right to withdraw consent (if applicable)
- The right to lodge a complaint with a supervisory authority
- The source of the personal data (if the personal data is not obtained from the individual it relates to)
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to)
- The details of the existence of automated decision-making, including profiling (if applicable).

7. Access Rights

Under the data protection legislation, the right of access allows an individual to gain access to their personal records. This right also allows parents/guardians to gain access to some information held about their children. As a result clients, staff and volunteers have the right to access records held about them. Services must respond fully to a subject access request within the statutory timescale (currently one month). However some services may be contractually required to respond faster than this

Each business must have operational procedures to upheld subject access rights and comply with subject access requests. The procedures must include the following elements

- Individuals or their representatives must be provided with information outlining how they make a request
- There must measures to validate the identity of the requester.
- In the case of the request coming from a client's representative (e.g. a solicitor), the service needs to establish consent
- Prior to disclosing information the following redactions must be made
    - Information pertaining to a 3rd party
    - Information which may cause harm to someone if disclosed

  Where redactions are used these must be clearly flagged.
- The information must be signed off by an experienced manager before it is disclosed to the client. This manager should have a knowledge of the service context and DPA subject access legislation
- Businesses must keep a record of subject access requests they have responded to
- Statutory and contractual timescales must be adhered to

The Data Protection Act only applies to living people. However rights exist within other legislation for access to records of deceased people. If businesses get requests for access to a deceased individual's record, they should seek the advice of the Data Protection Officer/Information Governance Lead.

In addition to subject access requests, requests can come from other agencies for personal information (i.e the Police, Probation, Home Office) without the consent of the data subject. These are not subject access requests and these cases the Confidentiality Policy must be consulted (section 'Information Sharing Without Consent')

In addition to access rights, individuals have the right to object to data processing or request that data processing is restricted, inaccuracies are corrected, or information is erased. These rights are not absolute and the implementation depends on the purpose and lawful basis for the data processing (see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/) for more detail. All such requests should be forwarded to the data protection officer/information governance lead for action/advice.

8. Record Keeping

The type of records being kept will depend on the services being delivered. Wherever possible standard formats should be used and services should provide operational guidance for staff and volunteers for recording information. Although records are 'confidential', the purpose of this confidentiality is to protect the data subject NOT the person entering the data. It should be assumed that - subject to adherence to data protection and confidentiality legislation – the group may have to release any of the information recorded on the database to a third party.

The following record-keeping principles should be followed:

- Write what is necessary for the purpose of your work. Do not miss out important/pertinent details, however do not include irrelevant information
- Be factual – include what has been observed and what has been disclosed
- Record all actions and decisions and to whom information has being shared
- For any record that exists it must be possible to determine the following:
    - When was it written and by whom?
- Records must be contemporaneous – i.e. written close to the time of the event that they refer to.
- Records should only be deleted if the process is part of an authorised disposal regime. If it is necessary to amend a record, the original record should not be deleted. In addition to the amendment there should be details of when the amendment was made, by whom, and for what reason. We have a duty to be open and transparent.
- Records should be self-explanatory and easy-to-understand by someone not working in the sector.

9. Retention and destruction

Records need to be retained for contractual or legislative reasons for a fixed period of time. Executive Directors are responsible for identifying the length of time client records should be kept and suitable storage arrangements and implementing appropriate operational procedures for retention and destruction

The HR manager is responsible for removing electronic records of staff that have left, archiving and destroying them after the required period

The Finance Director is responsible for ensuring that records relating to contracts and funding are stored safely and destroyed after the required period.

The Group ICT Director is responsible for ensuring that records relating IT assets and access are maintained accurately and up-to-date. It is also the responsibility of this role to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

10. Audit of Records

Businesses must implement effective operational procedures for ensuring that records are accurate. These processes should include automatic data validation and audit. Anyone processing records must be aware of operational procedures that apply.

11. Associated Policies

- Information Governance Framework
- Confidentiality
- IT, Email, social networking policy

ADVICE: Before using this document you should ensure that you have the most up-to-date version. If you are referring to a printed version it may be out-of-date. If in any doubt please check with Human Resources.

- Serious Untoward Incident and Incident
- Safeguarding Children and Young People
- Safeguarding Adults
- Information Security