PHSSL CARE LIMITED

CONTROLLED POLICY

A04 – RECORDS MANAGEMENT, CONFIDENTIALITY AND DATA PROTECTION POLICY

Policy Reference	A04
Version	1.0
Policy Owner	PHSSL Care Limited
Approved By	Lade Awosika, Director
Approval Method	Approved electronically
Approval Date	September 2026
Review Date	September 2027
Status	Controlled Document
Applies To	All PHSSL Care Limited staff, workers and relevant contractors
Supersedes	New policy

1. Purpose

This policy sets out PHSSL Care Limited's arrangements for creating, using, storing, sharing, accessing, retaining and disposing of records and personal information. It supports lawful, confidential and secure information handling while ensuring that accurate records are available for safe, effective and continuous care.

2. Scope

This policy applies to all staff, workers, managers and relevant contractors and covers paper, electronic, photographic, audio, video and other records relating to people receiving care, applicants, staff, professionals, incidents, complaints, safeguarding, governance and business administration.

3. Policy Statement

PHSSL Care Limited will protect confidentiality and process personal information lawfully, fairly, transparently and securely. Records will be accurate, relevant, proportionate and accessible only to authorised persons with a legitimate need. Information will not be kept longer than necessary and will be disposed of securely.

4. Legal and Regulatory Framework

This policy will be applied with regard to UK GDPR; the Data Protection Act 2018; the Human Rights Act 1998; common-law duties of confidentiality; the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014, particularly Regulation 17; the Care Act 2014; the Mental Capacity Act 2005; applicable safeguarding and employment requirements; and current CQC and Information Commissioner's Office guidance.

5. Data Protection Principles

Personal information will be processed lawfully, fairly and transparently; collected for specified and legitimate purposes; limited to what is necessary; kept accurate and up to date where required; retained only as long as necessary; and protected by appropriate security. PHSSL Care Limited will be able to demonstrate accountability for these principles.

6. Lawful Processing

PHSSL Care Limited will identify an appropriate lawful basis for processing personal data and, where special-category information is processed, an appropriate additional condition. Consent will not be relied upon where another lawful basis is more appropriate or where consent cannot be freely given or withdrawn.

7. Confidentiality

Confidential information must not be disclosed to people who are not authorised to receive it. Staff must discuss sensitive information discreetly and avoid conversations where they may be overheard. Confidentiality obligations continue after employment or engagement ends.

8. Record-Keeping Standards

Records must be factual, clear, timely, legible where handwritten, dated and attributable to the person making the entry. They must distinguish fact from professional opinion, avoid inappropriate or discriminatory language and provide sufficient information to support continuity, accountability and safe care.

9. Care Records

Care records may include assessments, care and support plans, risk assessments, visit notes, medicines records, consent and capacity information, reviews, professional communications, incident information and other records necessary for safe care. Staff must record care delivered and relevant changes or concerns.

10. Corrections and Amendments

Records must not be altered in a way that hides the original information. Corrections must preserve an appropriate audit trail and identify the person making the amendment and, where relevant, the date and reason. Staff must not falsify, backdate or deliberately obscure records.

11. Access Controls

Access to records will be based on role, responsibility and legitimate need. Passwords, authentication credentials and access devices must not be shared. Managers will review access where roles change or employment ends.

12. Paper Records

Paper records must be stored securely and protected from unauthorised access, loss, theft, fire, water damage and inappropriate viewing. Records taken away from an authorised location must be limited to what is necessary and kept secure.

13. Electronic Records

Electronic records must be held on approved systems or devices with appropriate access controls and security. Staff must follow organisational requirements for passwords, screen security, updates, backups and secure transmission. Personal email accounts or unapproved storage services must not be used for confidential PHSSL information.

14. Records in People's Homes

Where records are appropriately kept in a person's home, their privacy and confidentiality must be respected. Records should be positioned and stored to reduce unauthorised access while remaining available to authorised care staff and professionals when needed.

15. Information Sharing

Information will be shared only where there is a lawful and legitimate reason and only to the extent necessary. Staff should consider the person's wishes and consent where appropriate, but information may be shared without consent where law permits or requires this, including certain safeguarding, serious-risk or emergency situations.

16. Safeguarding and Serious Risk

Concerns about abuse, neglect, exploitation or serious risk must not be withheld solely because information is confidential. Staff must follow safeguarding procedures and share relevant information with authorised persons or agencies when lawful and necessary to protect a person or others.

17. Mental Capacity and Representatives

Where a person may lack capacity for a particular information decision, staff will follow the Mental Capacity Act 2005 and PHSSL Care Limited's Mental Capacity and Consent Policy. Representatives may receive information only where they have appropriate authority or another lawful basis applies.

18. Children and Young People

Information relating to children and young people requires particular care. Decisions about consent, confidentiality, parental responsibility, safeguarding and information sharing will reflect the child's circumstances, competence, best interests and applicable law.

19. Data Subject Rights

PHSSL Care Limited will support individuals to exercise applicable data-protection rights, including rights relating to access, rectification and other rights provided by law. Requests will be recognised promptly and referred to the appropriate responsible person for lawful handling.

20. Subject Access and Access to Care Records

Requests by individuals or authorised representatives for access to personal information will be handled in accordance with applicable data-protection law and PHSSL Care Limited's Access to Records and Retention Policy. Identity and authority will be verified where necessary.

21. Third-Party Information

Records may contain information about other people. Before disclosure, PHSSL Care Limited will consider confidentiality, legal rights, safeguarding and whether third-party information should be withheld or redacted.

22. Photography, Video and Audio

Images and recordings are personal data where individuals can be identified. They must only be created, used, shared or stored for an authorised purpose and in accordance with consent, capacity, safeguarding, confidentiality and PHSSL Care Limited's digital-communications requirements.

23. Email, Messaging and Digital Communication

Confidential information must only be sent using approved methods and to verified recipients. Staff should check addresses and attachments before sending and use the minimum information necessary. Unapproved messaging applications must not be used for confidential care information.

24. Data Breaches

Loss, misdirection, unauthorised disclosure, inappropriate access, cyber incidents or other suspected personal-data breaches must be reported immediately through PHSSL Care Limited's escalation arrangements. Management will assess, contain, investigate and document the incident and make external notifications where legally required.

25. Records Retention

Records will be retained in accordance with an approved retention schedule based on applicable law, regulatory expectations, contractual requirements and recognised records-management guidance. Retention periods may vary according to the record type and circumstances.

26. Secure Disposal

Records that have reached the end of their authorised retention period will be destroyed securely unless a legal, safeguarding, investigation, complaint, litigation or other legitimate hold requires continued retention. Disposal methods must prevent reconstruction or unauthorised recovery.

27. Data Minimisation and Duplicate Records

Only information necessary for the intended purpose should be collected or copied. Uncontrolled duplicate records should be avoided. Where temporary copies are necessary, they must be secured and disposed of appropriately when no longer needed.

28. Business Continuity and Backups

PHSSL Care Limited will maintain proportionate arrangements to protect essential records and support continuity during system failure or emergencies. Where temporary downtime records are used, they must be reconciled with the main record system when normal operations resume.

29. Staff Records

Recruitment, employment, training, supervision, competency, attendance and other workforce records will be managed confidentially and accessed only by authorised persons. Staff information will be retained and disposed of in accordance with applicable requirements.

30. Monitoring and Audit

PHSSL Care Limited will monitor record quality, confidentiality, access, data protection and secure storage through audits, spot checks, incident review, supervision and governance activity. Identified shortfalls will result in proportionate corrective action.

31. Staff Responsibilities

Staff must maintain accurate records; protect passwords and devices; keep information confidential; share information only when authorised; report errors, losses and breaches promptly; complete required training; and follow current information-governance procedures.

32. Management Responsibilities

Management will maintain appropriate information-governance systems, access controls, retention arrangements, staff training, breach-management processes and audit. Managers will ensure that concerns are investigated and that regulatory or statutory requirements are met.

33. Related PHSSL Policies

- A01 Governance and Quality Assurance Policy
- A03 Business Continuity and Emergency Planning Policy
- B01 Safeguarding Adults Policy
- B02 Safeguarding Children and Young People Policy
- B05 Mental Capacity, Consent and Best-Interest Decision-Making Policy
- F01 Information Sharing and Communication Policy
- F02 Social Media, Photography and Digital Communications Policy
- F03 Access to Records and Retention Policy

34. Review and Document Control

This policy will be reviewed at least annually and sooner following significant legal, regulatory, technological or service changes, data breaches, audit findings or identified information-governance risks. The current approved electronic version is the controlled master. Printed or locally saved copies are uncontrolled unless specifically issued and recorded as controlled copies.

Approved by	Lade Awosika
Position	Director
Approval method	Approved electronically
Approval date	September 2026
Next review date	September 2027