

DATA PROTECTION POLICY



Effective Date(s)	Oct26 – Oct 2027
Approved By	Trustees
Approval Date	01 October 2026
Policy Owner/Dept	Caroline Reid
Policy Author	Caroline Reid - Manager , Gary Reid - Trustee
Review Date	October 2027
Version Number	1.0

1. Purpose

Cadrene Supported Living (CSL) is committed to protecting the personal information and confidentiality of service users, staff, volunteers, trustees and other individuals. CSL will handle personal information lawfully, securely and responsibly in accordance with UK data protection law and relevant regulatory requirements.

2. Scope

This policy applies to all employees, trustees, volunteers, contractors and others handling personal information on behalf of CSL. It covers information held electronically, on paper, in emails, photographs, records and other formats.

3. Data Protection Principles

CSL will ensure personal information is:

1. Processed lawfully, fairly and transparently.
2. Collected for clear and legitimate purposes.
3. Limited to what is necessary.
4. Accurate and kept up to date where necessary.
5. Retained only for as long as required.
6. Processed in accordance with individuals' legal rights.
7. Protected against unauthorised access, loss, damage or disclosure.
8. Transferred internationally only where applicable legal requirements are met.

CSL will maintain appropriate records and procedures to demonstrate compliance.

4. Lawful Processing

CSL will identify a lawful basis for processing personal information, such as consent, contractual necessity, legal obligation or legitimate interests, where applicable.

Signing an employment contract or service agreement does not automatically constitute consent to all processing.

Health information and other special category data will only be processed where an appropriate lawful basis and additional legal condition apply.

5. Confidentiality and Information Sharing

Staff must only access information required for their role and must not disclose it to unauthorised people.

Information may be shared where lawful and necessary for care and support, safeguarding, legal obligations or other legitimate purposes. Consent will be obtained where required or appropriate, but is not always necessary for lawful safeguarding or statutory disclosures.

Before sharing information, staff must check the recipient, purpose, necessity and security of the disclosure. Uncertain requests must be referred to the Manager.

Photographs, videos and personal stories must not be used for publicity without an appropriate lawful basis and suitable permissions or consent where required.

6. Security of Information

CSL will use appropriate measures to protect personal information, including:

- Locked storage for paper records.
- Password protection and restricted access to electronic records.
- Secure email and information-sharing methods.
- Secure storage, backups and disposal arrangements.
- Removal of access when staff or volunteers no longer require it.

Staff must not share passwords, leave confidential records unattended or store personal information on unauthorised devices or accounts.

7. Retention and Disposal

CSL will retain records only for as long as necessary, taking account of legal, regulatory, safeguarding and operational requirements.

A retention schedule will identify appropriate periods for service-user, safeguarding, employment, financial and other records. Information must be securely destroyed or deleted when no longer required, unless there is a lawful reason to retain it.

8. Rights of Individuals

Individuals have rights under data protection law, which may include the right to:

- Access their personal information.
- Request correction of inaccurate information.
- Request deletion or restriction of processing where the law permits.
- Object to certain processing.
- Request a copy of their data in a portable format where applicable.
- Withdraw consent where processing relies on consent.
- Complain to the Information Commissioner's Office (ICO).

Requests may be made verbally or in writing. CSL may offer a request form but will not require its use. Requests will normally be answered within one month, subject to applicable legal provisions. Requests are generally free of charge.

9. Data Breaches

Any suspected loss, unauthorised disclosure or access to personal information must be reported immediately to the Manager or designated data protection lead.

CSL will record the incident, take steps to contain it, assess the risk and decide whether the ICO or affected individuals must be notified.

Where a breach is reportable to the ICO, notification must normally be made within 72 hours of CSL becoming aware of it. All breaches and decisions must be documented, and lessons learned used to prevent recurrence.

10. Responsibilities and Training

The Board of Trustees will oversee compliance with this policy. The Manager will ensure appropriate procedures, staff guidance, security measures and training are in place.

All staff and volunteers must:

- Follow this policy and maintain confidentiality.
- Access and share information only when authorised.
- Keep records secure and accurate.
- Report suspected breaches or inappropriate access immediately.
- Complete relevant data protection training.

Unauthorised access, disclosure or misuse of information may result in disciplinary or other appropriate action.

11. Reporting Concerns

Concerns about misuse of information, unlawful disclosure or deliberate concealment of a data breach should be reported to the Manager or, where the concern involves the Manager, to an appropriate trustee.

CSL will investigate concerns fairly and will not tolerate retaliation against anyone who raises a genuine concern. This section should be read alongside CSL's Whistleblowing Policy.

12. Monitoring and Review

CSL will monitor information security, complaints, data requests, breaches, training and record-retention arrangements. Identified weaknesses will be addressed through appropriate corrective action.

This policy will be reviewed annually or sooner if legislation, regulatory guidance, organisational practice or significant incidents require changes.

13. Legislative and Regulatory Framework

This policy should be read in conjunction with:

- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018, as amended.
- Data (Use and Access) Act 2025, where applicable.
- Human Rights Act 1998, where relevant.
- Health and Social Care Act 2008 (Regulated Activities) Regulations 2014, including Regulation 17 on good governance where applicable.

14. Related Documents

- Safeguarding Policy.
- Confidentiality Policy, if maintained separately.
- Complaints Procedure.
- Whistleblowing Policy.
- Records Retention and Disposal Schedule.
- Data Breach Reporting Procedure.
- Recruitment Policy.
- Mental Capacity and Consent policies, where applicable.