CONTINUING COMMUNITY CARE

Data Protection Policy

Registered Charity Number: 1204035
Organisation Name: Continuing Community Care (CCC)
Policy Owner: Chief Executive Officer
Last Review Date: December 2025
Next Review Due: December 2026

---

1. Purpose

Continuing Community Care is committed to protecting the privacy and personal data of all individuals we work with, including clients, staff, volunteers, donors, trustees, and partners.

This policy explains how we collect, use, store, share and protect personal data in compliance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Any other relevant data protection legislation

We take data protection seriously. We collect only what we need, use it responsibly, keep it secure, and never misuse it.

---

2. Scope

This policy applies to:

- All staff, contractors, volunteers and trustees
- All personal data processed by Continuing Community Care
- All formats of data — electronic, paper, verbal, visual or recorded

---

3. Definitions

Personal Data: Any information that can identify a living person (e.g., name, address, email, phone number, medical information, payment details).

Special Category Data: Sensitive personal data such as health information, disability status, or safeguarding records.

Data Subject: The individual whose data is being processed.

Processing: Any activity involving personal data — collecting, storing, sharing, editing, deleting, etc.

---

4. Data Protection Principles

We follow the 7 UK GDPR principles:

1. Lawfulness, fairness and transparency
2. Purpose limitation — used only for legitimate purposes
3. Data minimisation — only what is necessary
4. Accuracy — kept up to date
5. Storage limitation — not kept longer than needed
6. Integrity and confidentiality — kept secure
7. Accountability — we can demonstrate compliance

---

5. Lawful Basis for Processing

We process personal data only when we have a lawful basis, including:

- Consent
- Contractual necessity (e.g., delivering services)
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

Special category data (e.g. health data) is processed only where additional legal conditions are met, such as explicit consent or provision of health and social care.

---

6. What Data We Collect

We may collect:

- Name, address, phone number, email
- Emergency contact details
- Medical or health information relevant to services
- Attendance and session records
- Payment and donation records
- Staff and volunteer HR records
- Safeguarding and incident reports

- Marketing preferences

We never collect unnecessary data.

---

7. How We Use Data

We use personal data to:

- Deliver services safely and effectively
- Communicate with clients and stakeholders
- Manage bookings, payments, staffing and compliance
- Meet legal and regulatory obligations
- Safeguard vulnerable adults
- Improve our services
- Fundraise and communicate (where consent is given)

---

8. Data Storage and Security

We protect data using:

- Password-protected systems
- Access controls (only authorised staff can access data)
- Secure cloud services compliant with UK/EU standards
- Locked storage for paper records
- Staff training on confidentiality and data protection

Data is never stored on personal devices unless authorised and secured.

---

9. Data Sharing

We only share data when necessary and lawful, including with:

- Healthcare professionals (with consent or legal basis)
- Local authorities or safeguarding bodies
- Regulators or auditors
- IT and payroll providers under contract
- Emergency services when required

We never sell personal data.

---

10. Data Retention

We keep data only as long as necessary:

- Client records: retained in line with clinical and legal guidance
- Financial records: 6 years minimum
- Safeguarding records: retained securely for longer if required
- Marketing data: until consent is withdrawn

Data is securely deleted when no longer required.

---

11. Individual Rights

Individuals have the right to:

- Access their data
- Correct inaccurate data
- Request deletion (where applicable)
- Restrict or object to processing
- Data portability
- Withdraw consent at any time
- Complain to the ICO

Requests should be made in writing and will be responded to within 30 days.

---

12. Data Breaches

Any actual or suspected data breach must be reported immediately to the CEO or nominated Data Protection Lead.

We will:

- Investigate the breach
- Contain the risk
- Notify the ICO within 72 hours where required
- Notify affected individuals if there is a high risk

---

13. Responsibilities

- The CEO is responsible for overall compliance.
- All staff and volunteers must follow this policy.
- Breaches of this policy may result in disciplinary action.

14. Contact Details

For data protection enquiries:

Data Protection Lead: Chief Executive Officer
Organisation: Continuing Community Care
Email: ccc.hydrotherapy@gmail.com
Website: www.ccc-hydrotherapy.org

You also have the right to complain to the Information Commissioner's Office (ICO).

---

15. Review

This policy will be reviewed annually or sooner if legislation changes.