Confidentiality Policy for Clarity House London

Version 1.0

Effective Date: 3 July 2026

---

1. Purpose

1.1 Document Objective

This Confidentiality Policy (the "Policy") defines the standards, protocols, and legal boundaries governing the protection of confidential information at Clarity House London. It ensures that our organization balances the human-centric core of emotional wellbeing support with strict legal compliance.

1.2 Dual Utility

This document serves a dual purpose:

- **Public Transparency:** It is published on our website to inform members, funders, commissioners, and statutory bodies exactly how we protect and respect their data.
- **Internal Governance:** It functions as an operational standard operating procedure (SOP). All workforce members must comply with this policy as a condition of their engagement.

1.3 Legal and Regulatory Compliance

This policy is meticulously drafted to satisfy:

- The UK General Data Protection Regulation (UK GDPR);
- The Data Protection Act 2018 (DPA 2018);
- The Common Law Duty of Confidentiality;
- The Care Act 2014 and the Children Act 1989/2004; and
- The Information Commissioner’s Office (ICO) Data Sharing Code of Practice.

---

2. Scope

2.1 Personnel Boundaries

This policy applies universally to all individuals who act on behalf of, advise, govern, or work within Clarity House London (collectively referred to as "Workforce Members"). This includes:

- Board Members and Trustees;
- Executive and Administrative Staff;
- Paid personnel, including **Clarity Guides** and **Managers**;
- Contracted clinical and therapeutic professionals, including **Clarity Companion Associates** and **Psychologists**; and
- Unpaid personnel, including volunteers and specialized **Clarity Fellows**.

2.2 Data Boundaries

The scope encompasses all confidential information obtained, generated, or stored by the organization. This includes written case notes, electronic data, verbal disclosures, assessment scales, recruitment files, and corporate administrative records.

---

3. Our Commitment to Confidentiality

3.1 Fundamental Premise

Clarity House London treats all personal and special category information with the highest level of confidentiality. We recognize that establishing an emotionally safe environment is impossible without robust information boundaries.

3.2 The Non-Absolute Rule

We aim to preserve confidentiality in every possible scenario. However, **confidentiality is not absolute**. It is bounded by a definitive ethical and legal threshold: the protection of human life and compliance with the laws of the United Kingdom. There are strictly defined circumstances where information must be shared without consent to protect vulnerable individuals or comply with statutory obligations.

---

4. What Information We Keep Confidential

We enforce strict security controls over two primary classes of data:

4.1 Identifiable Personal Data

Any information that directly or indirectly identifies a living individual, including names, dates of birth, personal email addresses, phone numbers, residential addresses, and emergency contact details.

4.2 Special Category and Narrative Data

Highly sensitive contexts collected during our wellbeing, problem-solving, and therapeutic support blocks, including:

- Diagnosed or suspected physical and mental health conditions;
- Psychiatric histories, pharmaceutical logs, and substance misuse notes;
- Narrative disclosures concerning family conflict, domestic abuse, housing instabilities, or financial hardships; and
- Technical evaluation data generated through our clinical-adjacent frameworks.

---

5. Who Has Access to Information: Role-Based Access Control (RBAC)

5.1 The Need-to-Know Principle

Information within Clarity House London is strictly ring-fenced. No Workforce Member has blanket access to our case management systems. Access is granted systematically on a **need-to-know basis**, determined exclusively by the active duties of an individual's role.

5.2 Specific Matrix of Access Permissions

The organization enforces the following strict role-based data permissions:

- **Clarity Guides:** As the primary operational case managers, Clarity Guides have comprehensive access to member profiles. This includes initial intakes, **Clarity House Assessment Manual (CHAM)** profiles, active **Clarity Case Severity**

Scale (CCSS) scores, case notes, and historical review data. They require this data to manage service pathways and update complexity tiers during check-in calls.

- **Clarity Companion Associates & Psychologists:** These therapeutic practitioners have targeted access to member files. This includes baseline CHAM assessment summaries, active referral briefs, information necessary to deliver structured emotional wellbeing support blocks, and their own dedicated session therapy notes. **Upon completing a support call or session, Companion Associates are authorized to adjust a member's CCSS complexity score based on their updated clinical and practical assessment.** These score adjustments are systematically routed to a **Manager**, who holds ultimate review and sign-off authority over all CCSS tier updates.
- **Managers:** Managers possess comprehensive system access to review updated CHAM metrics and evaluate the clinical rationale behind any changes made to CCSS tiers by Companion Associates. They carry final operational authority to approve or reject complexity score shifts before they are formally finalized.
- **Clarity Fellows & Volunteers:** These community-facing personnel have highly restricted access. They are granted visibility *only* over the specific administrative parameters required to execute their assigned shift or group duty, such as attendance rosters for local peer circles or basic contact validation fields. They are blocked from viewing deep case management histories, clinical assessments, or CHAM problem logs.
- **Administrative Staff:** Administrative personnel are granted access strictly to logistical and scheduling fields (e.g., appointment self-booking calendars, contact details, email queues) necessary to fulfill daily operations. They have no permission to review clinical session logs or detailed safeguarding disclosures.
- **Board Members:** Board Members do not routinely access or review identifiable member records. They govern the organization via fully anonymized, aggregated statistical dashboards. Identifiable records are only exposed to the Board under exceptional legal circumstances, such as a formal high-level member appeal or a statutory negligence investigation.

---

6. Confidentiality Frameworks Within Operations

6.1 Confidentiality During Assessments (CHAM & CCSS Data)

All assessment profiles generated via the Clarity House Assessment Manual (CHAM) and graded on the Clarity Case Severity Scale (CCSS) are strictly confidential.

- **Permitted Internal Use:** This diagnostic-adjacent data is used strictly for selecting support pathways, monitoring longitudinal progress, ensuring internal clinical quality assurance, and managing safe case-load scaling.
- **Strict Commercial Prohibition:** CHAM and CCSS assessment data is **never sold, leased, or traded** to commercial entities, advertising networks, or third-party corporations under any circumstances.
- **Aggregated Impact Reporting:** Fully anonymized, non-identifiable demographic and complexity data derived from CHAM and CCSS metrics may be used to compile corporate Key Performance Indicators. These aggregated reports are shared with grant funders, local authority commissioners, and research institutions to demonstrate service efficacy and secure operational funding.

6.2 Confidentiality During Support Sessions and Case Notes

All one-to-one emotional wellbeing blocks and psychological support sessions must be conducted in private environments where conversations cannot be overheard.

- **Digital Records Security:** All therapeutic case notes and session summaries written by Companion Associates must be logged directly into our centralized, encrypted case management system.
- **Paper Prohibition:** Writing or keeping unstructured paper notes, local word documents, or unencrypted personal diary entries containing member disclosures is strictly prohibited across all roles.

6.3 Digital Records and Infrastructure Controls

Our software platforms enforce automated audit tracking. Every instance of record creation, modification, or viewing is permanently logged against the individual Workforce Member's digital signature. Multi-factor authentication (MFA) is mandatory for all system logins.

6.4 Email and Telephone Communications

- **Email Safety:** Workforce Members must utilize their authorized corporate `@clarityhouselondon.com` email address for all professional correspondence. Identifiable case data must never be sent to a member or external partner via unencrypted standard email text.
- **Verbal Safety:** Telephone triage sessions and check-in calls must be executed from secure rooms. The use of speakerphone options in open-plan offices or public environments is a severe breach of this policy.

7. Mandatory Onboarding Confidentiality Agreements

7.1 Pre-Access Mandate

The execution of a formal, legally binding Non-Disclosure and Confidentiality Agreement is a mandatory step in our onboarding pipeline.

7.2 Strict Enforcement

No volunteer, Clarity Fellow, Clarity Guide, Companion Associate, Psychologist, Manager, Board Member, or independent IT contractor will be granted a digital log-in, assigned a shift, or permitted to access any confidential system until they have reviewed this policy and signed their confidentiality deed. This obligation survives the formal termination of their employment or volunteer tenure with Clarity House London.

---

8. Data Sharing and External Protocols

8.1 Third-Party Referrals

We frequently signpost or actively refer members to external agencies (such as housing associations, debt advice charities, or NHS clinical units) to help resolve practical bottlenecks mapped under CHAM Presenting Problems Taxonomy (PPT) codes.

- **Consent Directive:** Active digital referrals require the member's explicit, informed consent. We will clarify exactly what information is being shared, with whom, and for what specific purpose prior to data transmission.

8.2 Recruitment and Employment Information

Confidentiality extends fully to job applicants, volunteer applicants, and prospective Board Members. All CVs, interview metrics, professional references, and enhanced Disclosure and Barring Service (DBS) certificates are processed on a strictly confidential, restricted-access basis by our executive management team and are never disclosed externally without legal justification.

---

9. Statutory Safeguarding Exceptions to Confidentiality

9.1 The Public Interest Threshold

Under the Common Law Duty of Confidentiality and UK GDPR Article 9, the duty to preserve a member's privacy is explicitly overridden when a compelling, urgent public interest or statutory mandate requires disclosure.

9.2 Authorized Disclosure Triggers

Clarity House London will share personal and special category data with statutory authorities (such as the Police, NHS Crisis Teams, or Local Authority Safeguarding Boards) **without the individual's consent** if a Workforce Member or supervising clinician determines that:

- A child (under the age of 18) is at risk of active abuse, severe neglect, or exploitation;
- A vulnerable adult is facing immediate severe harm, coercive control, or systemically dangerous exploitation;
- There is an immediate, explicit, and unambiguous risk of death or severe self-harm to the member (acute suicide intervention threshold);
- Disclosure is strictly necessary to prevent, detect, or prosecute a serious indictable crime (including acts of terrorism, human trafficking, or money laundering); or
- We are served with a legally binding Court Order requiring the immediate production of our case notes.

9.3 Documentation Mandate

Whenever a confidentiality exception is triggered, the handling personnel must explicitly document the legal rationale, the specific information disclosed, and the receiving agency within our secure safeguarding log. The member will only be informed of the disclosure if doing so does not increase the risk of harm to the victim or compromise an active police investigation.

---

10. Storage, Retention, and Disposal

10.1 Technical Safeguarding

All digital records are encrypted both at rest and in transit using advanced cryptographic standards. Data is hosted securely within data centers that maintain compliance with UK data residency regulations.

10.2 Retention Framework

We store confidential data only for as long as necessary to fulfill our service delivery and statutory defense obligations:

- **Active Member Case Files:** Retained for a flat period of **6 years** from the date of formal case closure, aligned with standard UK limitation periods for contract and negligence claims.
- **Safeguarding Records:** Retained for **10 years** from the date of the last logged alert to satisfy institutional liability reviews and statutory oversight.
- **Unsuccessful Recruitment Portfolios:** Securely deleted **6 months** after the close of the respective application window.

10.3 Secure Disposal Protocols

Physical documents (where exceptionally generated) must be cross-shredded using high-security industrial shredders. Digital records reaching their retention threshold are permanently purged from our primary servers and background cloud backups using verified cryptographic deletion tools.

---

11. Breaches of Confidentiality

11.1 Definition of a Breach

A breach of confidentiality occurs when data is accessed, altered, lost, or disclosed by unauthorized individuals, or if a Workforce Member bypasses the RBAC framework out of personal curiosity.

11.2 Disciplinary Actions

Any unauthorized access, deliberate leak, or negligent sharing of confidential member information constitutes **gross misconduct**. If proven following an internal investigation, it will result in:

- Immediate termination of employment or volunteer placement;

- Absolute removal from the Board of Directors (for Board Members);
- An immediate formal notification to the relevant professional regulatory body (e.g., the British Psychological Society, Health and Care Professions Council, or British Association for Counselling and Psychotherapy) for qualified practitioners; and
- Potential civil or criminal prosecution under the Computer Misuse Act 1990 or the Data Protection Act 2018.

11.3 Statutory Reporting Obligation

If a breach creates a structural risk to the rights and freedoms of an affected individual, Clarity House London is legally required to report the incident to the Information Commissioner's Office (ICO) within **72 hours** of becoming aware of the breach.

---

12. Bilateral Responsibilities

12.1 Staff and Workforce Obligations

Every Workforce Member must:

- Complete mandatory data protection and confidentiality training annually;
- Secure their digital screens whenever stepping away from a workstation; and
- Immediately report any suspected data breach or system vulnerability to management.

12.2 Member and Service User Responsibilities

Members interacting with our community spaces, peer groups, or digital portals share the responsibility for safety. Members must respect the strict confidentiality of their peers. Disclosing the identity, personal situation, or statements of another member outside of a support group context is a material breach of our service terms and will result in immediate termination of support.

---

13. Complaints Handling

If you believe your confidentiality has been compromised by any representative of Clarity House London, or if you wish to challenge an information-sharing action, you

have the right to lodge a formal complaint. Please email your detailed grievance to our administrative team at admin@clarityhouselondon.com. We will investigate all complaints transparently and respond within 10 working days.

---

14. Policy Review

This Confidentiality Policy is a core governing document. It must be reviewed **annually** to ensure absolute alignment with evolving UK statutory laws and organizational scaling. Immediate out-of-cycle updates will be enforced if we modify our internal CHAM tracking systems, update manager verification processes, or implement new digital case-management software.

---

15. Contact Information and Corporate Placeholders

15.1 Direct Inquiries

For any clarifications regarding this policy, or to submit a formal confidentiality query, contact our administrative hub:

- **Organisation Name:** Clarity House London
- **Primary Contact Email:** admin@clarityhouselondon.com

15.2 Future Registry Integration

The placeholders below will be systematically populated upon the formal issuance of active registry certificates by the respective UK regulatory bodies:

- **Registered Office Address:** [To be updated upon office establishment]
- **Company Registration Number:** [To be updated upon company registration]
- **ICO Data Controller Registration Number:** [To be updated upon data controller registration]
