Information Governance & Data Protection (GDPR) Framework

At Nextsmartstep, we recognize that we are entrusted with highly sensitive personal and clinical information. Backed by over 20 years of industry expertise, our governance framework is strictly aligned with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

We operate a "Privacy by Design" approach, ensuring that confidentiality and data security are woven into every aspect of our supported living services.

1. Our Regulatory Status

Nextsmartstep is a registered Data Controller with the Information Commissioner’s Office (ICO). We undergo regular internal audits to ensure our data handling remains compliant with the evolving landscape of UK digital law and social care standards.

2. Special Category Data & The "Caldicott Principles"

Unlike a standard business, we process Special Category Data (Article 9 of the GDPR), which includes mental health records, medical history, and criminal justice information. We adhere to the Caldicott Principles:

- Justification: Every use of personal data must be for a specific, documented purpose.

- Need to Know: Only staff directly involved in a resident's support plan have access to their specific records.

- Minimal Necessary: We only share the minimum amount of data required to ensure safe and effective care.

3. Technical & Organizational Security

• Digital Security: All digital records are stored on encrypted, password-protected UK-based servers. We utilize Multi-Factor Authentication (MFA) to prevent unauthorized access.

• Physical Security: Any paper-based records are kept in locked, fireproof cabinets within restricted-access staff offices and are digitized as soon as practically possible.

• Data Minimization: We only collect and retain information that is legally necessary to provide safe support and satisfy local authority auditing requirements.

4. Information Sharing & "The Golden Rule"

We maintain a "Ring of Safety" by sharing data with the NHS, Police, and Local Authorities. We follow the "Golden Rule" of information sharing in social care:

"The duty to share information can be as important as the duty to protect confidentiality when it comes to safeguarding a human life."

5. Your Data Rights

Under UK GDPR, our residents and professional partners have the following rights:

• The Right of Access: You can request a copy of the data we hold (Subject Access Request).

• The Right to Rectification: You can ask us to correct inaccurate information.

• The Right to Erasure: While care records must be kept for 7–10 years for legal auditing, you can request the deletion of non-essential contact data.

Contact our Data Protection Lead

For any questions regarding your data or to make a Subject Access Request (SAR), please contact our Data Protection Officer (DPO):

- Email: info@nextsmartstep.co.uk

- Subject: "Data Protection Inquiry"