BRIGHTMOVE
CHILDREN'S RESIDENTIAL CARE HOMES
Suite 217 Queens Dock Business Centre,
Norfolk Street, Liverpool, L1 0BG

Brightmove Care
Data Protection & GDPR Policy

Policy Owner: Registered Manager
Approved by: Director
Date Made: 01/03/2026
Review Date: 01/03/2027
Policy Reviewer: David Locke – Manager
Version: 1.0

1. Purpose

This policy sets out how Brightmove Care manages personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. The organisation is committed to protecting the privacy, dignity, and rights of children, families, staff, and others.

2. Scope

This policy applies to all personal data processed by Brightmove Care, including data relating to children, parents, carers, staff, volunteers, contractors, and visitors.

3. Legal and Regulatory Framework

This policy is written in line with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Children's Homes (England) Regulations 2015 – Regulation 22 (Records)
- Human Rights Act 1998
- Working Together to Safeguard Children

• Ofsted SCCIF

4. Data Protection Principles

Personal data will be:

• Processed lawfully, fairly, and transparently
• Collected for specified, explicit purposes
• Adequate, relevant, and limited to what is necessary
• Accurate and kept up to date
• Kept only as long as necessary
• Processed securely to prevent unauthorised access or loss

5. Roles and Responsibilities

Registered Manager – David Locke:

• Overall responsibility for data protection compliance

• Day-to-day oversight of data handling

Director – Gemma Winn:

• Strategic oversight and accountability

All staff:

• Must handle personal data securely and lawfully

6. Lawful Basis for Processing

Brightmove Care processes personal data under lawful bases including:

• Legal obligation
• Vital interests
• Public task
• Consent (where appropriate)

Special category data is processed in line with safeguarding and employment requirements.

7. Data Subject Rights

Individuals have the right to:

- Access their data
- Request correction
- Request erasure (where applicable)
- Restrict processing
- Object to processing
- Data portability (where applicable)

8. Subject Access Requests (SARs)

Requests for access to personal data must be made in writing.

Requests will be responded to within one calendar month, in line with UK GDPR.

9. Data Sharing and Disclosure

Personal data may be shared with external agencies where required by law or to safeguard children. Information sharing decisions will follow statutory guidance.

10. Data Security

Brightmove Care uses appropriate technical and organisational measures to protect data, including:

- Secure storage
- Password protection
- Restricted access
- Secure disposal of records

9A. Information Sharing and Safeguarding

Where there are safeguarding concerns relating to a child, information may be shared with appropriate agencies to protect the child.

10A. Electronic Data Security

Electronic records must be stored on secure systems with password

protection and restricted access. Where appropriate, encryption and secure

networks will be used to protect sensitive information.

Information sharing decisions will follow statutory safeguarding guidance and prioritise the welfare of the child.

11. Data Breaches

All data breaches or suspected breaches must be reported immediately to the Registered Manager.

Serious breaches will be reported to the Information Commissioner's Office (ICO) within 72 hours where required.

12. Data Retention and Disposal

Personal data will be retained only for as long as necessary in line with legal and regulatory requirements and securely disposed of when no longer needed.

13. Training and Awareness

All staff receive data protection training as part of induction and ongoing development.

14. Monitoring and Review

Compliance with this policy is monitored through audits, supervision, and

Regulation 44 visits. This policy is reviewed annually.

Appendix 1 – Staff Step-by-Step Guide (Data Protection)

1. Only access data you are authorised to see
2. Keep information secure at all times
3. Share information lawfully and Proportionately
4. Report any data breach immediately
5. Follow retention and disposal procedures

Appendix 2 – Data Breach Response Flowchart

Breach identified → Secure data → Inform Manager → Assess risk → Report to ICO if required →
Record → Review and learn