BRIGHTER DAYS RESIDENTIAL

LLAWNROC

Data Protection Policy

Policy Publication Date: April 2025

Review Date: April 2026

Brighter Days Residential Ltd

Data Protection Policy

Publication Date: April 2025

Review Date: April 2026

Contents

1. Purpose and Scope

This policy outlines how Brighter Days Residential Ltd manages personal data in compliance with the UK GDPR and Data Protection Act 2018.

It applies to all staff, children, visitors, contractors, and professionals who access or process data on behalf of the organisation.

2. Legal Framework

This policy is underpinned by the Data Protection Act 2018 and UK General Data Protection Regulation (GDPR).

3. Definitions

Personal Data: Any information that can identify a living individual (e.g. name, address, date of birth).

Special Category Data: Sensitive data such as health, ethnicity, religious beliefs, and sexual orientation.

Data Subject: The person to whom the data relates (e.g. children, staff).

Data Controller: Brighter Days Residential Ltd determines how and why personal data is used.

Data Processor: An external party processing data on behalf of Brighter Days.

4. Data Protection Principles

We follow the six key principles of the UK GDPR. Personal data must be:

• Processed lawfully, fairly, and transparently.

• Collected for specified, explicit, and legitimate purposes.

• Adequate, relevant, and limited to what is necessary.

• Accurate and kept up to date.

• Retained only as long as necessary.

• Secured appropriately.

5. Roles and Responsibilities

• The Responsible Individual oversees data protection compliance.

• The Registered Manager ensures all staff follow this policy.

• All staff are responsible for keeping information confidential, secure, and accurate.

• External contractors must follow written data agreements.

6. Legal Bases for Processing

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

• Consent (e.g. photos, media sharing).

• Legal obligation (e.g. safeguarding reporting).

• Contractual necessity (e.g. staff contracts).

• Vital interests (e.g. emergency medical care).

• Public task (e.g. local authority requirements).

• Legitimate interests (only where no rights are overridden).

7. Collecting and Using Personal Data

We collect data to provide safe and effective care, including:

• Children's records (e.g. health, education, safeguarding).

• Staff records (e.g. employment history, DBS, training).

• Visitor information (e.g. names, times, purpose).

We inform individuals of how their data is used through privacy notices.

8. Storing and Securing Data

• Paper records are stored in locked cabinets.

• Electronic data is stored on secure, password-protected systems.

• Access to records is limited to those who need it to do their job.

• Devices and USBs must be encrypted and approved by management.

9. Sharing Personal Information

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

• Local Authorities

• Health professionals

• Police or emergency services

• Regulatory bodies (e.g. Ofsted)

All sharing is recorded and justified based on the legal basis.

10. Retention and Disposal

Data is retained according to our Data Retention Schedule (based on NSPCC and ICO guidance).

• Records are securely destroyed when no longer needed.

• Electronic files are deleted, and paper records shredded by authorised services.

11. Data Subject Rights

Individuals have the right to:

• Access their data

• Request correction or deletion

• Object to processing

• Restrict data use

• Withdraw consent (if applicable)

Requests should be made in writing to the Registered Manager and responded to within 30 days.

12. Data Breaches and Reporting

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

Serious breaches will be reported to the ICO within 72 hours.

A breach log is maintained and reviewed for trends or system improvements.

13. CCTV and Monitoring

CCTV is not used at the property .

14. Access Requests

Data subjects (or parents with rights) may request access to personal data.

Requests must be responded to within 30 calendar days, unless complex.

Copies of records are provided securely and access may be limited to protect others' privacy.

15. Staff Responsibilities and Training

All staff receive annual data protection training and updates.

Staff must report data concerns and follow safe data handling procedures.

Breaches of this policy may result in disciplinary action.

16. Review and Oversight

The Responsible Individual reviews this policy annually or after a breach or legal change.

Feedback from staff, professionals, or data subjects is welcomed and used to improve practice.

Appendix 1

Key Terms and Definitions

This guide explains key terms used in data protection so all staff can understand their responsibilities.

Personal Data:
Information about a person that could identify them (e.g. name, address, phone number, medical history).

Special Category Data:
Sensitive information like health, religion, ethnicity, or sexual orientation that requires extra care.

Data Subject:
The person whose data is being collected (e.g. child, staff, visitor).

Data Controller:
Brighter Days Residential Ltd – the organisation deciding how and why data is used.

Data Processor:
Someone (often external) who handles data for Brighter Days (e.g. payroll service).

Consent:
When someone agrees to share their information, usually in writing.

Appendix 2

Lawful Bases for Processing Data

We must have a legal reason (lawful basis) to use any personal data. Here are the 6 lawful reasons and examples:

1. Consent: The person agrees to it – e.g. a parent signs a form for photo use.

2. Contract: Needed to fulfil a contract – e.g. paying a staff member.

3. Legal Obligation: Required by law – e.g. reporting safeguarding concerns.

4. Vital Interests: To protect someone's life – e.g. sharing medical info with ambulance staff.

5. Public Task: Used to carry out official functions – e.g. working with local authorities.

6. Legitimate Interests: Needed for our work – only when it doesn't override someone's rights.

Appendix 2

Personal Data Handling Checklist

Use this checklist to make sure you're handling personal data safely and legally.

☐ Only collect the data you need.

☐ Store it securely (locked cupboard or password-protected system).

☐ Only share data with people who need to know.

☐ Check data is accurate and up to date.

☐ Delete or destroy data when it's no longer needed.

☐ Never leave paper files or screens unattended.

☐ Use encrypted USBs or devices approved by management.

☐ Report any data loss, theft, or error immediately.