

CONTROLLED DOCUMENT

N.B. Colleagues should be discouraged from printing this document. This is to avoid the risk of out-of-date printed versions of the document. The Intranet should be referred to for the current version of the document.

DATA PROTECTION POLICY

CATEGORY:	Policy
CLASSIFICATION:	Information Governance
PURPOSE:	To set out the principles and approach for the protection of data
CONTROLLED DOCUMENT NUMBER:	BC/IG/001
VERSION NUMBER:	004
CONTROLLED DOCUMENT SENIOR LEADERSHIP TEAM LEAD:	Director of Corporate Services
CONTROLLED DOCUMENT AUTHOR:	Director of Corporate Services
APPROVED BY:	Board
APPROVED ON:	18 September 2024
IMPLEMENTED ON:	30 September 2024
REVIEW PERIOD:	Every 3 years - unless changes to legislation, best practice or internal roles and responsibilities
REVIEW DATE:	Reviewed in August 2025 – to reflect new Executive Team Structure Next full review: September 2027
ASSOCIATED DOCUMENTS:	Retention and Disposal Policy Website Retention Policy Network Security Policy Social Media Policy Surveillance and CCTV Policy Data Subject Access Request Policy Clear Desk, Clear Screen Policy
Essential Reading for:	Trustees and all colleagues
Information for:	Trustees and all colleagues

Document Consultation and Review Process

Groups/Individuals who have overseen the development of this Policy:	Corporate Governance Team, Senior Leadership Team
Groups/Individuals Consulted:	Corporate Governance Team, Senior Leadership Team, PQ&E Committee, Board

Document version control:

Date	version	Amendments made	Amendments Approved by
July 2022	001	Policy updated and placed in new controlled documents format with updated reference number	SLT
February 2023	002	Minor updates and formatting	Director of Corporate Services
September 2024	003	Full review undertaken	Board – 18 September 2024
August 2025	004	Updated to reflect new Executive Team structure and adoption of the term colleague for employee	Director of Corporate Services

For the Use of the Corporate Services Team only:

Date added to Register:	September 2025 (V004)
Date Published on the Hub:	September 2025 (V004)
Does it need to be published on website:	Yes

Registered charity no: 201555 | Registered company no: 601847 | Care Quality Commission registration no: CRT1-579008632 | Homes England registration no: LH0269. Head Office - Prospect Place, Whitehall, Bristol, BS5 9FF.

CONTENTS

1. POLICY STATEMENT..... 4

2. AIM OF THE POLICY 5

3. SCOPE OF THE POLICY 5

4. DEFINITIONS 5

5. KEY PRINCIPLES AND REQUIREMENTS..... 8

6. ROLES AND RESPONSIBILITIES 12

7. EQUALITY AND DATA PROTECTION 13

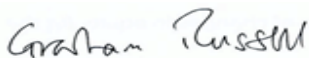
8. IMPLEMENTATION AND TRAINING 14

9. MONITORING AND REVIEW..... 14

1. POLICY STATEMENT

- 1.1 Brunelcare is committed to ensuring that any processing of personal data by or on behalf of Brunelcare is carried out in compliance with Data Protection Laws.
- 1.2 While this Policy focuses on personal data within the scope of data protection law, Brunelcare also holds other categories of information that must remain confidential, including confidential business information and sensitive operational information. This information will be handled with the same high standards as personal data.
- 1.3 Brunelcare will comply with the GDPR including its six core principles ('**6 Principles**') set out in Article 5 of the GDPR, which in summary are:
- 1. Lawfulness, fairness and transparency*
Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- 2. Purpose limitation*
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- 3. Data minimisation*
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- 4. Accuracy*
Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- 5. Storage limitation*
Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- 6. Integrity and confidentiality*
Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Signed on behalf of Brunelcare:



Graham Russell
Chair of the Board



Oona Goldsworthy
Chief Executive

2. AIM OF THE POLICY

- 2.1 This Policy is a key part of Brunelcare's Data Protection Management System ('**DPMS**'). Its purpose is to ensure Brunelcare is compliant with its obligations under all applicable data protection laws ('**DP Laws**') and contracts or other interactions with stakeholders (including colleagues, customers, suppliers, partners, regulators and investors). The DPMS also aims to reduce or eliminate the potential for the commitment of, and liability for, criminal offences in DP Laws by Brunelcare and Brunelcare's officers and colleagues.

3. SCOPE OF THE POLICY

- 3.1 This policy applies to all Brunelcare's officers, colleagues and contractors, as appropriate, those operating on its behalf. In addition, security is fundamental to data protection and the DPMS closely interacts with Brunelcare's Information Security Management System ('**ISMS**') including related policies and procedures.
- 3.2 All colleagues are contractually bound by confidentiality obligations set out in their contracts of employment. A breach of confidentiality may amount to gross misconduct and can result in disciplinary action, up to and including dismissal. For contractors, agency staff and volunteers, breaches may result in termination of engagement or contract.
- 3.3 In addition to the UK GDPR and Data Protection Act 2018, Brunelcare operates within a wider legal framework, including:

- Care Act 2014
- Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
- Mental Capacity Act 2005
- Human Rights Act 1998 (Article 8: right to private and family life)
- Access to Health Records Act 1990
- Freedom of Information Act 2000
- Computer Misuse Act 1990

Compliance with these laws is integral to maintaining privacy and confidentiality in all Brunelcare activities.

4. DEFINITIONS

- 4.1 In this policy, we use definitions from the GDPR unless otherwise stated:

‘**Anonymised data**’ means information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

‘**Controller**’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

‘**DPIA**’ means the Data Protection Impact Assessment that must be carried out in certain situations, contain certain information, and over which there are other obligations, as set out in the GDPR.

‘**EEA**’ or ‘**European Economic Area**’ means the EU and Iceland, Lichtenstein and Norway.

‘**EU GDPR**’ means the EU General Data Protection Regulation, 2016/679.

‘**GDPR**’ means either or both of the EU GDPR and UK GDPR. We will use this when there is little or no difference in the wording of the relevant law for the context.

‘**Personal data**’ means any information relating to an identified or identifiable natural person, namely one who can be identified, directly or indirectly from that information alone or in conjunction with other information ‘in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person’¹.

‘**Processing**’ means ‘any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction’.

‘**Processor**’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

‘**Pseudonymisation**’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information (such as a lookup table relating alphanumeric identifiers to the individuals), provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

‘**Special Categories of Personal Data**’ means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

¹ Examples of personal data are from the EU GDPR.

‘**Transfer**’ means the transfer of personal data either to ‘**third countries**’ (meaning countries outside the EU for the EU GDPR or outside the UK for the UK GDPR) or ‘**international organisations**’ (meaning an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries, such as the UN or WHO).

‘**UK DPA**’ means the UK Data Protection Act 2018.

‘**UK GDPR**’ means the UK-adopted version of the EU GDPR, which took effect from 1 January 2021 as a result of Brexit.

5. KEY PRINCIPLES AND REQUIREMENTS

- 5.1 As Controller, Brunelcare processes personal data only when one or more of the 6 legal bases set out in Article 6 of the GDPR applies:
- 5.1.1 the data subject has given consent to the processing of his or her personal data for one or more specific purposes
 - 5.1.2 the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
 - 5.1.3 the processing is necessary for compliance with a legal obligation to which the controller is subject
 - 5.1.4 the processing is necessary in order to protect the vital interests of the data subject or of another natural person
 - 5.1.5 the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
 - 5.1.6 The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (this basis is not available to support processing carried out by public authorities in the performance of their tasks).

Special Categories of Personal Data

- 5.2 Where Brunelcare wishes to process Special Categories of Personal Data, or personal data relating to criminal convictions and offences or related security measures, we must comply with additional requirements. Please see the Sensitive Personal Data Policy.

Brunelcare as 'controller' and 'processor'

- 5.3 While, in all cases, processing of personal data must be in accordance with applicable DP Laws:
- where Brunelcare is the controller, we will comply with all obligations applicable to controllers in DP Laws. Brunelcare, as with most businesses, is the controller of the majority of personal data we process, for example across colleague relations, marketing and finance activities, and supplier management.
 - where Brunelcare is the processor, the relevant personal data may only be processed in accordance with the contract we have with, and the instructions of, the controller. Brunelcare will also comply with any obligation on processors in DP Laws.

Risk-based Approach

- 5.4 The DPMS mirrors the GDPR and is a risk-management based system and any and all measures taken under the DPMS are to be appropriate to the risk in question. This means that, in some instances, lesser measures are required (for example in the protection of purely public Information) while in other instances significant measures are required (for example in the protection of Special Categories of Personal Data).

Governance

- 5.5 As part of its DPMS, Brunelcare has committed to maintain a governance structure to ensure compliance with DP Laws, including the following.

Records

- 5.6 Brunelcare will establish and maintain records required to demonstrate compliance, such as the privacy notices provided to data subjects, records of consent, and Article 30 Records.

Security Measures

- 5.7 As a fundamental requirement under GDPR, Brunelcare will maintain appropriate technical and organisational measures against unauthorised or unlawful processing of personal data held or controlled by Brunelcare and against accidental loss or destruction of, or damage to, such personal data. The security measures will address the need to maintain the required confidentiality, integrity and availability of personal data, including the use of encryption according to our Encryption Policy and appropriate back-up practices.
- 5.8 Personal or confidential information must not be sent to personal email accounts or stored on privately-owned devices, unless specifically authorised under Brunelcare's Bring Your Own Device Policy. Only approved, secure Brunelcare systems and devices may be used for the processing or transfer of such information.
- 5.9 When working away from Brunelcare premises, colleagues remain responsible for safeguarding personal and confidential information.

Consent

- 5.10 Whenever consent is to be the legal basis for processing personal data, such consent must be obtained in accordance with the requirements of DP Laws and Brunelcare's Consent Procedure, recorded appropriately and an appropriate mechanism for withdrawal provided.
- 5.11 Consent for data processing purposes is separate and different from consent for medical purposes.

Collection, Transparency & Purpose Limitation

- 5.12 Addressing the GDPR's 1st Principle (Lawfulness, fairness and transparency) and 2nd Principle (purpose limitation), Brunelcare shall provide the information required (in particular under Articles 13 and 14 of the GDPR) in a privacy

notice to data subjects at the appropriate time in order for processing of that personal data to be lawful, fair and transparent. The privacy notice will be delivered in a compliant manner for the particular context, whether by single notices, layered notices, tooltips and other suitable methods. Brunelcare shall ensure that the purposes are included in the information provided to data subjects and respected during processing.

Privacy by Design & Privacy by Default

- 5.13 Brunelcare shall adopt policies and procedures to implement privacy by design and privacy by default into its working practices as appropriate. Key areas include the design and use of technology, storage, security systems including access to data, and marketing. We will carry out DPIAs as appropriate. We will also consider the use of anonymisation and pseudonymisation as appropriate and will use encryption as set out in our Encryption Policy.
- 5.14 Access to personal or confidential information will only be granted on a need-to-know basis. Colleagues must only access the information necessary for the performance of their duties, and any disclosure must be justified, proportionate and documented.

HR

- 5.15 Brunelcare shall ensure that all processing of personal data concerning officers and colleagues is processed according to our HR Privacy Notice at all times. Background checks must not be carried out without consulting HR and criminal reference checks must not be carried out without consulting Legal and in accordance with our Sensitive Personal Data Policy.

Data Subject Rights

- 5.16 Data subjects – individuals about whom we process personal data - have several rights under the GDPR and other DP Laws. Brunelcare shall always respect data subjects' rights and their exercise of them in accordance with those laws and shall respond to the exercise of such rights in accordance with our Data Subject Rights Policy and related procedures.

Sensitive Data

- 5.17 Given its business, Brunelcare does process Special Categories of Personal Data, and data relating to criminal conviction and offences for legitimate business purposes. These types of personal data are given much higher protection under DP Laws and shall only be processed by or on behalf of Brunelcare in accordance with such requirements and obligations and our Sensitive Personal Data Policy.

Children's Data

- 5.18 Brunelcare does process personal data related to individuals under the age of 18. We shall consider age verification or gating techniques for our goods and services if and as appropriate or as required under DP Laws.

Financial Data

- 5.19 Brunelcare will comply with the PCI Data Security Standard ('**PCI DSS**') at all times when processing credit card data. The PCI DSS provides an actionable framework for developing a robust payment card data security process, including prevention, detection and appropriate reaction to security incidents.

Anonymisation

- 5.20 Where appropriate, Brunelcare shall consider anonymising personal data. As anonymised data is not personal data, the DP Laws do not apply to any processing of anonymised data. As a result, anonymisation should be considered throughout the data lifecycle although it may not be practical in many circumstances other than the end of a retention period, where personal data may be anonymised as opposed to securely deleted or destroyed under our Information Deletion & Destruction Policy. Any anonymisation carried out by or on behalf of Brunelcare must satisfy legal and regulatory requirements as well as any Anonymisation Procedure we have adopted at that time.

Pseudonymisation

- 5.21 Unlike anonymised data, pseudonymised data is still personal data as individuals can be re-identified by use of additional information, such as a lookup table linking individuals to alphanumeric identifiers. Brunelcare shall therefore protect, retain, delete and otherwise process pseudonymised data in the same way as other personal data.

However, pseudonymisation is an excellent tool to reduce risk in certain circumstances and is likely to be applicable on many more occasions throughout the data lifecycle than anonymisation. Brunelcare shall consider pseudonymisation when appropriate and any pseudonymisation carried out by or on behalf of Brunelcare must satisfy legal and regulatory requirements as well as any Pseudonymisation Procedure we have adopted at that time.

Marketing

- 5.22 All marketing activities must comply with our Privacy & Marketing Policy and all applicable laws at all times.

Use of processors

- 5.23 The choice and use of processors or sub-processors shall be in accordance with our Processor (Vendor) Policy.

Transfers

- 5.24 Transfers of personal data to third countries or international organisations shall only be carried out in accordance with our Transfers Policy.

Retention & End-of-Life

- 5.25 In accordance with our Retention Policy, Brunelcare shall first honour its legal obligations as to the period for which any particular personal data must be kept. Subject to any such legal obligation, we shall consider any exercise by a data subject of their rights in light of all relevant factors under DP Laws. At the end of the retention period for particular personal data, that personal data shall either be anonymized or securely deleted or destroyed under our Information Deletion & Destruction Policy.

Criminal offences

- 5.26 As well as the potential maximum fines in the EU / UK GDPRs of €20m / £17.5m or 4% of global turnover, whichever is higher, national laws typically set out criminal offences for certain processing of personal data contrary to that nation's DP Laws. Such offences typically include obtaining or sharing personal data unlawfully, causing personal data to be altered without authorisation, and re-identifying individuals without authorisation. Brunelcare will always have a lawful basis or lawful authorisation for its processing of personal data.

Approved Codes of Conduct & Certifications

- 5.27 The GDPR allows for approval of codes of conduct (Article 40) and certification mechanisms (Article 42). Adherence to an approved code or certification mechanism may be used as an element by which to demonstrate compliance with various requirements in the GDPR. If necessary or appropriate, Brunelcare will review such codes and certification mechanisms for relevance and fit for our operations.

Breach

- 5.28 If you become aware of a breach of this policy, you must report it promptly to the Director of Corporate Services at dataprotection@Brunelcare.org.uk.

Enforcement

- 5.29 All Brunelcare colleagues bear responsibility for their own compliance with this policy. Breach of this policy is ground for disciplinary proceedings against a colleague, which may result in disciplinary action including termination of employment. Breach of this policy by any non-employee such as a temporary worker, contractor or supplier may be a breach of their contract with Brunelcare and grounds for damages or termination.

6. ROLES AND RESPONSIBILITIES

Board

- 6.1 It is the responsibility of the Board to ensure that Brunelcare's policies and procedures reflect statutory requirements and best practice.

- 6.2 The Board has delegated oversight and monitoring of this policy to the Performance, Quality and Experience Committee.
- 6.3 Brunelcare is the data controller under data protection Legislation for the personal data it processes for its own purposes.
- 6.4 The CEO has overall responsibilities for compliance with data protection legislation as delegated by the Board.

Performance, Quality and Experience Committee

- 6.5 The Performance, Quality and Experience Committee is responsible for overseeing Brunelcare's arrangements for ensuring compliance with data protection legislation and information governance arrangements.

Director of Corporate Services

- 6.6 The-Director of Corporate Services has delegated responsibility to ensure that the Charity has robust data protection processes in place that comply with current legislation and best practice guidance.

Data Protection Officer

- 6.7 The Data Protection Officer (DPO) is primarily responsible for advising on and assessing Brunelcare's compliance with the DPA and UK GDPR and making recommendations to improve compliance.
- 6.8 The DPO is responsible for monitoring progress and advising the organisation on implementation of this policy, acting as primary contact on any data protection queries and approving responses to Right of Access requests (generally described in this document as '*Subject Access Requests*').
- 6.9 The DPO is responsible for monitoring the completion of all mandatory training for all colleagues (with special emphasis on colleagues handling personal data on a daily basis) and ensuring access to further guidance and support.

Colleagues

- 6.10 All colleagues have individual responsibility for complying with this policy and following accompanying guidance.
- 6.11 All colleagues will undertake relevant data protection training alongside any other training that shall be deemed as mandatory.

7. EQUALITY AND DATA PROTECTION

Equality and Diversity

- 7.1 Brunelcare seeks to embed an environment where all clients, visitors, colleagues, agency employees, contractors, consultants, trustees, volunteers and any other workers are treated as individuals, fairly and in a consistent

way. We work within the spirit and the practice of the Equality Act 2010 by promoting a culture of respect and dignity and actively challenging discrimination, should it ever arise. This Policy will be applied in a way that is consistent with these principles.

Data Protection

- 7.2 Brunelcare is committed to ensuring protection of all personal information that we hold, and to provide and protect all such data as laid out in this policy.
- 7.3 It is recognised that processing of personal data will involve the collection and sharing of sensitive personal information. Data protection obligations will therefore be followed at all times with information only shared with those that it is necessary to share this information with and in a secure manner.

8. IMPLEMENTATION AND TRAINING

- 8.1 Brunelcare will communicate the requirements of this policy. This will include:
- All new starters being briefed on the requirements of this policy as part of their induction to Brunelcare.
 - An annual reminder of the existence and importance of this policy via internal communication methods.
- 8.2 All colleagues will undertake mandatory training on information governance and security which they will re-take every year. In addition, all colleagues will be required to attend a more detailed data protection training protection training module as part of their induction.

9. MONITORING AND REVIEW

- 9.1 The implementation of this policy, and the effectiveness of the arrangements detailed within it, will be monitored by the-Director of Corporate Services.
- 9.2 The Performance, Quality and Experience Committee will be responsible for undertaking reviews of decision-making processes to ensure that the Policy is applied effectively and where further controls are required will advise accordingly.
- 9.3 The Performance, Quality and Experience Committee will commission reviews where the Policy has not been adhered to-identify any lessons learnt and advise on changes to systems and processes as appropriate.
- 9.4 This policy will be reconsidered against any legislative changes and reviewed at least every three years.