

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 This is to avoid the risk of out of date printed versions of the document.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.

Sensitive Personal Data Policy

CATEGORY:	Policy
CLASSIFICATION:	Information Governance
PURPOSE:	To set out the principles and approach regarding sensitive personal data
CONTROLLED DOCUMENT NUMBER:	BC/IG/015
VERSION NUMBER:	002
CONTROLLED DOCUMENT SENIOR LEADERSHIP TEAM LEAD:	Director of Corporate Services
CONTROLLED DOCUMENT AUTHOR:	Director of Corporate Services
APPROVED BY:	Board
APPROVED ON:	18 September 2025
IMPLEMENTED ON:	September 2025
REVIEW PERIOD:	Every 3 years - unless changes to legislation, best practice or internal roles and responsibilities
REVIEW DATE:	September 2028
ASSOCIATED DOCUMENTS:	Data Protection Policy Personal Data Breach 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
October 2024	V001	Drafted as part of full information governance policy review. Principles separated from earlier policy and procedure documents.	
August 2025	V002	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 (V002)
Date Published on the Hub:	September 2025 (V002)
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.

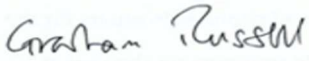
CONTENTS

1. POLICY STATEMENT	4
2. AIM OF THE POLICY AND RELATED LEGISLATION	5
3. SCOPE OF THE POLICY	5
4. DEFINITIONS	5
5. KEY PRINCIPLES AND REQUIREMENTS	6
6. ROLES AND RESPONSIBILITIES	14
7. EQUALITY AND DATA PROTECTION.....	16
8. IMPLEMENTATION AND TRAINING	17
9. MONITORING AND REVIEW	17

1. POLICY STATEMENT

- 1.1 To deliver its services safely and efficiently, Brunelcare needs to gather and use certain information about individuals, including customers, residents, tenants, suppliers, business contacts, employees (colleagues) and other individuals with whom the organisation has a relationship with or may need to contact.
- 1.2 Brunelcare is committed to ensuring that it complies fully with data protection legislation and 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 residents, tenants, customers, suppliers, colleagues, partners and regulators). 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.
- 1.3 The Board of Brunelcare will take steps to ensure that personal data is:
- processed fairly, lawfully and in a transparent manner;
 - used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes;
 - adequate, relevant, and limited to what is necessary;
 - accurate and, where necessary, up to date;
 - not kept for longer than necessary; and
 - kept safe and secure.
- 1.4 Brunelcare will make sure that it does not put individuals at risk because of processing their personal data. Failure to do so, can result in breach of legislation, reputational damage or financial implications due to fines. To meet our obligations, Brunelcare will put in place appropriate and effective measures to make sure compliance is maintained with DP laws.
- 1.5 This policy has been developed to achieve compliance with relevant legislation and national guidance and ensure compliance throughout the organisation.

Signed on behalf of Brunelcare:


Graham Russell
Chair of the Board


Oona Goldsworthy
Chief Executive

2. AIM OF THE POLICY AND RELATED LEGISLATION

- 2.1 This policy is to ensure that Brunelcare's processing of Special Categories of Personal Data ('**SCPD**') and personal data relating to criminal convictions and offences or related security measures ('**CCOPD**') and together '**sensitive personal data**') is in accordance with applicable data protection laws ('**DP Laws**').

Legislative and Legal requirements:

- [Data Protection Act 2018](#)
- [General Data Protection Regulation \(GDPR\) \(Regulation \(EU\) 2016/679\)](#)
- [UK General Data Protection Regulation \(UK GDPR\)](#)
- [Care Act 2014](#)
- [Health & Social Care Act 2008 \(Regulated Activities\) Regulations 2014](#)
- [Mental Capacity Act 2005](#)
- [Human Rights Act 1998](#)
- [Access to Health Records Act 1990](#)

3. SCOPE OF THE POLICY

- 3.1 This policy applies to all Brunelcare's officers and employees and, as appropriate, those operating on its behalf.

4. DEFINITIONS

- 4.1 In this policy, we use definitions from the GDPR unless otherwise stated.
- **CCOPD** means personal data relating to criminal convictions and offences.
 - **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.
- 4.2 **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'. While **personal data** is a defined term in EU and UK law, we use it here to also cover **personally identifiable information** as defined in US law, and other similar legal definitions.
- 4.3 **Special Categories of Personal Data** or **SCPD** 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.
- 4.4 **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 Brunelcare shall only process SCPD when it has a legal basis under Article 6 of the GDPR (see Brunelcare's Data Protection Policy) and a legal basis under Article 9(2) of the GDPR, namely one of the following:
- 5.1.1 the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where EU or Member State law if the EU GDPR applies (or UK law if the UK GDPR applies) provides that the prohibition on processing SCPD may not be lifted by the data subject;
 - 5.1.2 processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by EU or Member State law if the EU GDPR applies (or UK law if the UK GDPR applies) or a collective agreement pursuant to Member State law if the EU GDPR applies (or UK law if the UK GDPR applies) providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
 - 5.1.3 processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
 - 5.1.4 processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
 - 5.1.5 processing relates to personal data which are manifestly made public by the data subject;
 - 5.1.6 processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
 - 5.1.7 processing is necessary for reasons of substantial public interest, on the basis of EU or Member State law if the EU GDPR applies (or UK law if the UK GDPR applies) which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
 - 5.1.8 processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the colleague, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or Member State law if the EU GDPR applies (or UK law if the UK GDPR applies) or

pursuant to contract with a health professional and subject to the following conditions and safeguards.

- 5.1.9 SCPD may be processed for the purposes in this paragraph when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under EU or Member State law if the EU GDPR applies (or UK law if the UK GDPR applies) or rules established by national competent bodies or by another person also subject to an obligation of secrecy under EU or Member State law if the EU GDPR applies (or UK law if the UK GDPR applies) or rules established by national competent bodies;
- 5.1.10 processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or Member State law if the EU GDPR applies (or UK law if the UK GDPR applies) which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- 5.1.11 processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or Member State law if the EU GDPR applies (or UK law if the UK GDPR applies) which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
- 5.2 Under the UK Data Protection Act 2018 (**UK DPA 2018**), for the purposes of processing for health or social care purposes etc under Art 9(2)(h) of GDPR (point 5.1.8, above), the circumstances in which the processing of personal data is carried out subject to the conditions and safeguards referred to in Art 9(3) of GDPR (obligation of secrecy) include circumstances in which it is carried out:
- 5.2.1 by or under the responsibility of a health professional or a social work professional, or
- 5.2.2 by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.
- 5.3 Brunelcare shall ensure that any additional conditions set out in the DPA 2018 are met should we process SCPD and consult legal advice when in any doubt. In particular:
- 5.3.1 processing for the following purposes that is based on being authorised by, with a basis in, the law of the UK (or a part thereof), shall meet the relevant condition(s) in Schedule 1, Part 1 of the UK DPA 2018:
- employment, social security and social protection* in Art 9(2)(a),
 - health or social care in Art 9(2)(h),
 - public health in Art 9(2)(i), and
 - archiving, research and statistics in Art 9(2)(j).

5.3.2 processing for the substantial public interest purposes in Art 9(2)(g) set out below, with a basis in the law of the UK (or a part thereof), shall meet the relevant condition(s) in Schedule 1, Part 2 of the UK DPA 2018*:

- statutory and government purposes, administration of justice and parliamentary purposes, publication of legal judgments,
- equality of opportunity or treatment, racial and ethnic diversity at senior levels of organisations,
- preventing or detecting unlawful acts, protecting the public against dishonesty etc, regulatory requirements relating to unlawful acts and dishonesty etc, journalism etc in connection with unlawful acts and dishonesty etc, preventing fraud,
- suspicion of terrorist financing or money laundering,
- support for individuals with a particular disability or medical condition, counselling, safeguarding of children and of individuals at risk, safeguarding of economic well-being of certain individuals,
- insurance, occupational pensions,
- political parties, elected representatives responding to requests, disclosure to elected representatives, informing elected representatives about prisoners, and
- anti-doping in sport, or standards of behaviour in sport.

* Each of these processing activities are potentially Key Processing, requiring Key Measures, as defined below.

CCOPD

5.4 Brunelcare shall only process CCOPD under the control of official authority or when the processing is authorised by EU or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority – and there should typically be no reason for Brunelcare to keep such a register. It will be ensured that all envisaged processing of CCOPD is cleared with the Corporate Services Team, with legal advice sought at an early stage in the planning process.

5.5 CCOPD includes personal data relating to:

- the alleged commission of offences by the data subject, or
- proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

Where Brunelcare processes CCOPD on the basis of authorisation under the law of the UK (or a part thereof), we shall ensure that it meets a condition in Part 1, 2 or 3 of Schedule 1 of the UK DPA 2018. Conditions in Schedule 1, Part 3 include:

- consent,
- protecting individual's vital interests,
- processing by not-for-profit bodies,
- personal data which is manifestly made public by the data subject,
- legal claims and judicial acts,

- administration of accounts used in commission of indecency offences involving children*, and
- extension of conditions in Schedule 1, Part 2, referring to substantial public interest or insurance.

* This processing activity is potentially Key Processing, requiring Key Measures, as defined below.

5.6 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.

5.7 In addition, when Brunelcare, as controller, processes personal data, one of the 6 legal bases set out in Article 6 of the GDPR must apply to ensure lawful processing:

- 5.7.1 the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- 5.7.2 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;
- 5.7.3 the processing is necessary for compliance with a legal obligation to which the controller is subject;
- 5.7.4 the processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- 5.7.5 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;
- 5.7.6 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).

- 5.8 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'

- 5.9 While, in all cases, processing of personal data must be in accordance with applicable DP Laws:
- 5.9.1 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 employee relations, marketing and finance activities, and supplier management.
 - 5.9.2 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

- 5.10 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

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

Senior Sponsorship

- 5.12 The Director of Corporate Services has overall responsibility for establishing and maintaining the DPMS. Responsibility for the creation and maintenance (including appropriate periodic review) of this document, and related policies and procedures, shall be clearly set out in each such document.

Responsibilities

- 5.13 While senior sponsorship is set out above, we all have responsibilities to ensure we appropriately process and protect personal data in accordance with DP Laws and the DPMS, including (as appropriate to our roles) reporting personal data breaches, carrying out PIAs, carrying out due diligence on processors, and otherwise implementing privacy by design and privacy by default across Brunelcare's business. Line managers must ensure they are fully aware of the DPMS as it relates to their roles

as they are responsible for compliance by their direct reports and by suppliers for whom they are the lead manager.

Policies & Procedures

- 5.14 Brunelcare will establish and maintain appropriate policies to ensure compliance with applicable DP Laws across the data lifecycle, and appropriate procedures to ensure that the policies may be put into practice. Policies will address governance and risk across the personal data lifecycle from collection to destruction.

Training & Awareness

- 5.15 Brunelcare will train staff on the importance of data protection and aspects of this DPMS as appropriate to their role and level of seniority at on-boarding, on change of role and with refresher training sessions as appropriate.

Records

- 5.16 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

- 5.17 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.

Review

- 5.18 As appropriate, Brunelcare will review developments in DP Laws and codes of practice and practical changes in working patterns, assess the DPMS against any such development, and consider any required update to the DPMS.

Consent

- 5.19 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.

Collection, Transparency & Purpose Limitation

- 5.20 Addressing the GDPR's First Principle (Lawfulness, fairness and transparency) and Second 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

- 5.21 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 PIAs and DPIAs as appropriate and in accordance with our PIA & DPIA Policy. We will also consider the use of anonymisation and pseudonymisation as appropriate and will use encryption as set out in our Encryption Policy.

HR

- 5.22 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 advice and in accordance with our Sensitive Personal Data Policy.

Data Subject Rights

- 5.23 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

- 5.24 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

- 5.25 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

- 5.26 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

- 5.27 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

- 5.28 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.
- 5.29 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

- 5.30 All marketing activities must comply with our Privacy & Marketing Policy, its related procedure, and all applicable laws at all times.

Use of Processors

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

Transfers

- 5.32 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

- 5.33 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

- 5.34 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

- 5.35 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

- 5.36 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

- 5.37 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.

Ownership

- 5.38 The Director of Corporate Governance is responsible for maintaining this policy and related training and awareness programs.

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 organisation 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.
- 6.10 The DPO will conduct regular assurance activity to monitor and assess new processing of personal data. The DPO will also monitor and report on all data processor requirements (e.g. roles and responsibilities, notifications, data subject access requests).
- 6.11 The DPO is the first point of contact for the regulatory authorities and for individuals whose data is processed (colleagues, customers etc.).

Colleagues

- 6.13 All colleagues have individual responsibility for complying with this policy and following accompanying guidance.
- 6.14 All colleagues will undertake relevant data protection training alongside any other training that shall be deemed as mandatory.
- 6.15 Those working for or on behalf of Brunelcare will:
- 6.15.1 observe all forms of policy, guidance, codes of practice and procedures about the collection, sharing, handling and use of personal information;
 - 6.15.2 develop a comprehensive understanding of the purpose for which Brunelcare uses personal information;
 - 6.15.3 collect and process information in accordance with the purpose for which it is required to be used by Brunelcare to meet its statutory requirements and business needs;
 - 6.15.4 ensure personal information is destroyed when no longer required in line with the organisation's data retention schedules;
 - 6.15.5 upon receipt of a request by or on behalf of an individual for information held about them (Subject Access Request), refer requests to the Data Protection

Officer and Corporate Governance Team as quickly as possible so that the request can be acted on quickly and legal advice sought if required; and

- 6.15.6 understand that breaches of this policy may result in scrutiny by the Information Commissioner's Office (ICO) with the potential for fines to be levied and accompanying reputational damage. There is also the potential for misconduct action.

Other Roles

- 6.16 Specific roles are assigned throughout the organisation to manage personal data, its processing and the associated risks in terms of responsibilities, decision making and monitoring compliance:

- 6.16.1 *Caldicott Guardian*: a senior person within the organisation responsible for protecting the confidentiality of individual's health and care information and making sure this is used properly. The organisation needs to have a Caldicott Guardian due to the organisation providing services for the NHS/Local Authorities. The Caldicott Guardian ensures the organisation follows the 7 Caldicott principles related to personal information:

- Justify the purpose(s) of using confidential information.
- Only use it when absolutely necessary.
- Use the minimum that is required.
- Access should be on a strict need-to-know basis.
- Everyone must understand his or her responsibilities.
- Understand and comply with the law.
- The duty to share information can be as important as the duty to protect patient confidentiality.

The organisation's Director of Nursing and Care Services acts as the Caldicott Guardian.

- 6.16.2 The Corporate Services Team is responsible for issuing, reviewing and communicating corporate information management standards and procedures. The Team will also advise on compliance with data protection requirements.

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 The organisation will establish effective arrangements for communicating 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 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 This policy will be reconsidered against any legislative changes and reviewed on an annual basis