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 This is to avoid the risk of out of date printed versions of the document.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

CATEGORY:	Policy
CLASSIFICATION:	Information Governance
PURPOSE:	To ensure that data subject rights under all applicable data protection laws are respected and that Brunelcare acts in accordance with such laws.
CONTROLLED DOCUMENT NUMBER:	BC/IG/012
VERSION NUMBER:	002
CONTROLLED DOCUMENT SENIOR LEADERSHIP TEAM LEAD:	Director of Corporate Services
CONTROLLED DOCUMENT AUTHOR:	GDPR Advisor – July 2024 (V001)
APPROVED BY:	SLT - V001 Director of Corporate Services (V002)
APPROVED ON:	V001- July 2024
IMPLEMENTED ON:	V001 - July 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: July 2027
ASSOCIATED DOCUMENTS:	Brunelcare DSAR Procedure
Essential Reading for: **Information for:**	Trustees and all colleagues

Document Consultation and Review Process

Groups/Individuals who have overseen the development of this Policy:	**GDPR Advisor** **Governance Team**
Groups/Individuals Consulted:	**SLT**

Document version control:

Date	version	Amendments made	Amendments Approved by
July 2024	V001	New policy – previous DPO had guidance in place but not a policy	SLT
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:	July 2024
Date Published on the Hub:	V002 – September 2025
Does it need to be published on website:	Yes

CONTENTS

1. POLICY STATEMENT

1.1 Brunelcare processes large amounts of data about a variety of people including applicants for and residents of our homes, and those who wish to receive or are receiving care services. Brunelcare is also an employer and therefore process personal data about our staff and individuals who work for us, as well as applicants and other business contacts.

1.2 Brunelcare will comply with Data Protection Laws (DP Laws) regarding Data Subject Rights including in relation to notifying data subjects of their rights, how it receives and processes requests, and in responding to such a request. In all cases, processing data including the handling of requests will be in accordance with Data Protection Laws.

1.3 This Policy is focused on Data Subject Access Requests (DSARs), which is the majority of requests, but we will apply the policy to any and all Data Subject Rights requests in compliance with the law:

1.2.1 where Brunelcare is the data controller of the data, when determining the purpose and the means (the 'why' and the 'how') of any processing, we will comply with all obligations set for controllers in DP Laws regarding DSARs, including consideration of the request and our rights in relation to it, and

1.2.2 where Brunelcare is the processor of information on behalf of another controller, we will respond to the exercise of a DSAR in accordance with the DP Law and our contract with the controller, who will usually be the party who will reply to the individual who made the request (data subject).

1.3 This policy sets out how Brunelcare will seek to enable and support individuals (data subjects) to exercise their rights in accordance with the legislation.

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 The Data Protection Act (DPA) 2018 and the UK General Data Protection Regulations (UK GDPR) sets out eight rights, that individuals can exercise in terms of their personal information. The legislation gives individuals the following rights:

i. the right to be provided with specified information about the processing of their personal data ('the right to be informed');

ii. the right to access their personal data and certain supplementary information ('the right of access', sometimes known as 'Data Subject Access');

iii. the right to have their personal data rectified, if it is inaccurate or incomplete ('the right of rectification');

iv. the right to have, in certain circumstances, their personal data deleted or removed ('the right of erasure', sometimes knowns as 'the right to be forgotten');

v. the right, in certain circumstances, to restrict the processing of their personal data ('the right to restrict processing');

vi. the right, in certain circumstances, to move personal data the individual has provided to another organisation ('the right of data portability');

vii. the right, in certain circumstances, to object to the processing of their personal data and, potentially, require Brunelcare to stop processing that data ('the right to object'); and

viii. the right, in relevant circumstances, to not be subject to decision making based solely on automated processing ('Rights related to automated decision making, including profiling').

Related Legislation

The EU General Data Protection Regulation, 2016/679.

The UK Data Protection Act 2018.

The UK-adopted version of the EU GDPR, which took effect from 1 January 2021.

Aims of the Policy

2.2 This policy sets out how we will enable and support individuals (data subjects) to exercise their rights in accordance with the legislation

2.3 It sets out our commitment to ensure that:

i. all data subject rights requests are responded to in a person centre manner and according to the values of transparency and integrity;

ii. all personal data is processed fairly and lawfully and in accordance with data subjects' rights;

iii. that everyone working for the Charity or on our behalf to comply with this policy when dealing with data subject rights; and

iv. the approach that we will routinely take when responding to requests is clearly set out, including setting out in general terms any exemptions in the DPA we are likely to apply when responding to requests.

3. SCOPE OF THE POLICY

3.1 This policy applies to all DSAR requests that we receive.

3.2 Apart from requests made on behalf of individuals (data subjects) by an agent acting for that data subject, this policy does not cover requests for personal data made by third parties under the Freedom of Information Act or, as a Third Party Disclosure Request where a legitimate legal basis has been cited for the release of personal information.

3.3 The Freedom of Information Act does not apply to Brunelcare, but Third-Party Disclosure Requests are addressed in our 'Data Sharing Policy'.

4. DEFINITIONS

4.1 For the purposes of this policy, the definitions set out in the GDPR have been adopted, unless otherwise stated.

- *Data Controller:* A 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.

- *Data Processor:* An individual or legal person, public authority, agency or other body (other than an employee of the data controller) who processes the data on behalf of the data controller.
- *Data Protection Legislation:* The UK General Data Protection Regulation (UK GDPR) together with the Data Protection Act 2018 (the Data protection legislation) governs the processing of personal data. The data protection legislation requires that personal data including special categories of personal data, which are regarded as more sensitive, must be processed by data controllers in accordance with the data protection principles set out in the UK GDPR.

- *Data Subject:* Any living individual who is the subject of personal data.
- *EU GDPR*: The EU General Data Protection Regulation, 2016/679.
- *GDPR:* 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:* 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.
- *Processing:* 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'.
- *Special categories:* Special category personal data comprises information relating to a data subject, that reveals or is concerned with the data subjects: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data (where used for identification purposes); physical or mental health or conditions; Sexual life or sexual orientation Information about the commission of offences or criminal proceedings is also regarded as sensitive under data protection legislation and we handle such information commensurately.
- *UK DPA:* the UK Data Protection Act 2018.
- *UK GDPR:* the UK-adopted version of the EU GDPR, which took effect from 1 January 2021 as a result of Brexit.

5. THE KEY PRINCIPLES AND REQUIREMENTS

Details of how to make a request

5.1 We will publish information about how people can exercise their data subject rights on our website, including details of reasonable

adjustments that we can offer to ensure that these rights are accessible to all.

Confirmation of request and identity

5.2 The Corporate Services Team (CS Team) will normally ask applicants to provide written confirmation of their request via email or letter. This is because of the requirement to be satisfied of the applicant's identity and for audit purposes.

5.3 The CS Team can accept data subject rights requests by telephone however; these may be subject to further identity checks. In any circumstance, we reserve the right to make identity checks as deemed necessary.

5.4 The CS Team will not usually progress a subject rights request until it has received the requester's:

i. full name;
ii. previous name(s) (if applicable);
iii. address and/or email address;
iv. date of birth; and
v. authorisation to communicate with a third party (if applicable).

5.5. Depending on the circumstances, the team may ask the applicant (or their representative) for further proof of identity or Authority to Act.

5.6 Where the team is otherwise satisfied as to the identity of the person making the request, it may elect to waive the requirement for the applicant to provide proof of identity.

When third parties act for the data subject

5.7 If a DSAR is exercised on behalf of the data subject by a third party (such as the data subject's lawyer), we shall also satisfy ourselves as to the identity of that third party and their authority to act for the data subject. However, it is the third party's responsibility to provide evidence of their authority, such as a written authority to make the request or a power of attorney.

5.8 If we feel the data subject may not understand what information may be disclosed to the third party they have authorised, we shall send the response directly to the data subject instead.

Individuals under the age of 18

5.9 A person under the age of 18 (a child) has the same rights over their personal data as an adult. Personal data about a young person is still their personal data and it is the child that can exercise the DSAR. Given that children merit specific protection, any information and communication addressed to a person under 18 shall be in such a clear and plain language that the child can easily understand.

5.10 In certain cases, the child's rights may be exercised by a person with parental responsibility for the individual or other authority.

Clarifying the request

5.11 Where we have a large amount of information relating to the applicant or a request is unclear, the CS Team may ask the applicant to clarify what specific information that they are looking for. The CS Team will send clarifying correspondence to the applicant as soon as possible following receipt of the request.

Timescale for compliance

5.12 The CS Team must log the date that the request was received, and the applicant's identity confirmed. The date that a request becomes active will be the date that a valid request is made (i.e. subject to clarification and identity checks).

5.13 The CS Team will aim to deal with all requests promptly and to respond within one month. Where this is not possible the team must within one month tell the applicant:

i. that they are extending the response time for up to two months and the reasons why, or;

ii. why they have decided not to respond to the request and that they can complain to the ICO or seek a judicial remedy.

5.14 The time limit to comply is calculated from the day the request is received (whether it is a working day or not) until the corresponding calendar date in the next month. If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. If the corresponding date falls on a weekend or a public holiday, we have until the next working day to respond.

5.15 The CS Team will monitor the time taken to comply with requests and report to the Data Protection Officer on compliance.

5.16 If a decision to decline the request is made, we must explain to the data subject why we are not taking action in response to their request, informing them of their right to complain to the supervisory authority and to a judicial remedy.

Multiple requests and additional copies

5.17 If multiple or subsequent requests are unfounded or excessive (in particular because of their repetitive character), we may either:

i. charge a reasonable fee; or

ii. refuse to act on the request.

5.18 In deciding whether multiple requests are excessive or made at unreasonable intervals, the CS Team will consider:

i. the nature of the data, including whether it is particularly sensitive;

ii. the purposes of the processing, including whether it is likely to cause a detriment to the applicant;

iii. the frequency with which the data is altered, including whether the data is likely to have changed or been altered since the previous request;

iv. the time that has elapsed since the previous request;

v. the volume of information or investigation involved;

vi. any reasons given by the applicant for wanting the same information or, making the same request again; and

vii. whether information requested under the right of access would be disclosable through other routes.

5.19 The CS Team will keep a record of their decision-making and respond to any requests by the applicant for a review of their decision.

Searching for personal data

5.20 The CS Team will undertake a reasonable and proportionate search for the personal data pertaining to a request in conjunction with relevant staff.

5.21 A record of any search parameters and strategy used will be clearly recorded in every case.

Amending data that is the subject of a request

5.22 It is a criminal offence for staff to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure or accurate response to a person who has made a data subject rights request unless:

i. the data would have been amended in any event; and/or

ii. There is a reasonable belief that the individual is not entitled to receive the requested information in line with a valid exemption under the DPA.

5.23 We will consider the data held at the time a request was received. However, in many cases routine use of the data may result in it being amended while the request is being dealt with. We may therefore consider the information we hold as at the date of the response, even if this is different to that held when the request was received. It is however important to note that for some data subject rights requests, we sometimes need to alter or erase data to comply with the request itself, this applies to the rights of erasure and rectification.

Review of the information

5.24 Once the relevant information has been located, the CS Team will review the data prior to making a decision as to which data subject right has been exercised and will decide whether any exemptions apply or, if there are legitimate reasons why we are unable to action a request.

5.25 With regards specifically to the right of access, the subject access right is to information (i.e. personal data) and not to documentation.

Accordingly, the CS Team may extract the applicant's personal data from documentation or redact information, which is not the applicant's personal data when preparing our response. Where appropriate, the CS Team may provide relevant contextual information to assist the applicant.

5.26 For complex requests the Director of Corporate Services and/or the Company Secretary will review the information prior to making a decision. In the most sensitive cases, further escalation and review may be necessary.

Exemptions

5.27 The DPA and UK GDPR set out a number of exemptions which may apply to data subject rights requests. We may be exempt from complying (in full or in part) with a request if:

i. the information sought is classed as 'third party data' meaning that it is information about other individuals and not the requester;
ii. we do not have the consent to release third party information, and it is not reasonable in the circumstances to disclose the data;
iii. the disclosure of information or, granting an individual's request would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders;
iv. the disclosure of information or, granting an individual's request would prejudice the functions of a regulator;
v. the information contains legally privileged personal data;
vi. disclosure of information or, granting an individual's request would be likely to prejudice our negotiations with the data subject;
vii. we are asked to erase data which we are required to process in order to comply with a legal obligation, for the performance a task carried out in the public interest or for reasons of public interest;
viii. there is another applicable exemption in the DPA or, UK GDPR.

Other reasons we may refuse a request

5.28 There are other reasons beyond the above exemptions which may result in us refusing a request in part or in full. In terms of the data subject rights of erasure, rectification, restriction of processing and objection, there are often legitimate reasons why we are unable to action the requested outcome. We're required by law to publish and retain certain personal information; therefore, this can result in us being unable to meet desired outcomes.

Response

5.29 The CG Team will usually respond to requests by email unless this is not possible or, another contact method has been specified by a

requester. The team will take appropriate security measures to protect the response from unauthorised disclosure in accordance with Brunelcare's 'Information Classification Policy'.

5.30 Our responses to data subject rights requests will contain the following information:

i. a summary of the request;

ii. our decision as to disclosure or, whether we are granting or refusing a request;

iii. clear reasons for any redactions, exemptions or, our reasons for refusing to grant a request. We will cite relevant sections of the DPA and UK GDPR in these circumstances;

iv. any information we need to send to comply with a request will be attached;

v. information about how an Internal Review can be requested along with contact details for the Information Commissioners Office (ICO);

vi. supplementary information about the way we process personal data.

5.31 All communications with data subjects on DSARs must be '*in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child*' (Article 12, GDPR). The information shall be provided in writing, or by other means including, where appropriate, electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

Audit and record keeping

5.32 The CG Team will maintain records of:

i. the requests we receive; the 'raw' products of any searches undertaken and the strategy used;

ii. a master copy of any information about the applicant which we have collated to comply with a request along with a record of any exemptions applied;

iii. any correspondence with the applicant, including our final response;

iv. any advice received or records prepared during the course of handling the request.

Internal Reviews and the Information Commissioner's Office (ICO)

5.33 We will, where appropriate, voluntarily review responses that applicants are not happy with, so as to resolve any complaint or dispute in a proportionate manner. This is called an Internal Review.

5.34 Complaints about responses should be referred to the Director of Corporate Services.

5.35 If the Director of Corporate Services has been involved in making decisions on disclosure of information, the Internal Review will be managed by a member of the Executive Team.

5.36 Additionally, individuals have a right to request that the Information Commissioner Office make an assessment of compliance with the requirements of the data protection legislation.

Fees

5.37 All the information is to be provided free-of-charge unless we can demonstrate that the requests from a data subject are '*manifestly unfounded or excessive*', in particular because of their repetitive character, in which case we as controller may either:

- charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested; or

- refuse to act on the request.

Breach

5.38 If you become aware of a breach of this policy, you must report it promptly to the Director of Corporate Services, or the Company Secretary.

6. ROLES AND RESPONSIBILITIES

6.1 Brunelcare's Data Protection Officer (DPO) will monitor compliance with this policy and provide advice on responding to data subject rights requests.

6.2 The Corporate ServicesTeam is responsible for managing all responses to data subject rights requests within organisational and statutory deadlines.

6.3 All colleagues are responsible for:

i. Identifying data subject rights requests.

ii. Referring data subject rights requests immediately to the Corporate Services Team by forwarding to dataprotection@brunelcare.org.uk.

iii. Co-operating with and assisting the Corporate Services Team to coordinate responses to requests.

6.4 We will provide staff with appropriate training/guidance so that they are able to comply with their responsibilities under this policy.

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 Charity will establish effective arrangements for communicating the requirements of this policy. This will include:

i. All new starters being briefed on the requirements of this policy as part of their induction to Brunelcare.
ii. 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 his policy will be reconsidered against any legislative changes and reviewed at least every three years.