

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 This is to avoid the risk of out of date printed versions of the document.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

PERSONAL DATA BREACH POLICY

CATEGORY:	Policy
CLASSIFICATION:	Information Governance
PURPOSE:	To set out the principles and approach for a personal data breach
CONTROLLED DOCUMENT NUMBER:	BC/IG/010 (<i>replaces BC/IG/008 - Identifying and Reporting an Information Governance Incident</i>)
VERSION NUMBER:	V002
CONTROLLED DOCUMENT SENIOR LEADERSHIP TEAM LEAD:	Director of Corporate Services
CONTROLLED DOCUMENT AUTHOR:	Director of Corporate Services
APPROVED BY:	Board
APPROVED ON:	V001 - 18 September 2024
IMPLEMENTED ON:	1 October 2024
REVIEW PERIOD:	Every three years – unless legislative, best practice or changes to internal roles and responsibilities
REVIEW DATE:	Reviewed in September 2025 – to reflect new Executive Team Structure Next full review: September 2027
ASSOCIATED DOCUMENTS:	Data Protection Policy Personal Data Breach Procedure
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
September 2024	V002	Fully updated policy following data protection review	Board - 18 September 2024
August 2025	VOO3	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:	1 October 2024
Date Published on Hub:	V001- 1 October 2024 V002 – September 2025
Does it need to be published on website:	No

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.

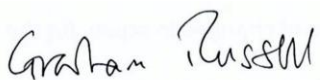
CONTENTS

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	13
7. EQUALITY AND DATA PROTECTION	13
8. IMPLEMENTATION AND TRAINING	14
9. MONITORING AND REVIEW	14

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, 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

Goldsworthy
Chair of the Board



Oona

Chief Executive Officer

2. AIM OF THE POLICY AND RELATED LEGISLATION

- 2.1 The purpose of this policy is to set out a Personal Data Breach response plan to protect individuals and their personal data, and to enhance Brunelcare's compliance with applicable data protection laws ('**DP Laws**'), in particular the GDPR.

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 any suspected or actual Personal Data Breach relating to any Information processed by Brunelcare and, as appropriate, those acting on its behalf.
- 3.2 Please refer to all other relevant policies, in particular the Supplier Policy, the Data Protection Policy, the Information Security Breach Policy, and the Transfer of Information Policy, and the Personal Data Breach Procedure, issued under this policy.

4. DEFINITIONS

- 4.1 *Art 29 WP* means the Article 29 Working Party, the EU body composed predominantly of a representative of the data protection regulator of each EU country, replaced in May 2018 by the European Data Protection Board (*EDPB*).
- 4.2 *EU GDPR* means the EU General Data Protection Regulation, 2016/679.
- 4.3 *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.
- 4.4 *Information* means any data and information in any format and on any medium, whether verbal, soft copy, hard copy or otherwise.
- 4.5 *Personal Data Breach* or *PD Breach* means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

- 4.5.1 *destruction* of personal data is where the data no longer exists, or no longer exists in a form that is of any use to the controller;
- 4.5.2 *damage* is where personal data has been altered, corrupted, or is no longer complete;
- 4.5.3 *loss* of personal data is where the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession; and
- 4.5.4 *unauthorised* or *unlawful* processing may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR.
- 4.6 *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' (EU GDPR). 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.
- 4.7 *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

Legal Context

- 5.1 The GDPR sets out obligations on controllers to respond appropriately to PD Breaches and make any required notifications to regulators and data subjects. Other laws around the world, particularly laws of many States in the USA, contain similar provisions. This policy is drafted for compliance with the GDPR. In the event of any PD Breach we will consider whether:
 - 5.1.1 any other law of the UK, EU, or any law of another jurisdiction, is applicable and, if so, the required steps for compliance; and
 - 5.1.2 we have any other legal or other obligation (such as under confidentiality and other agreements with third parties and legal, medical, or professional notification duties under other applicable regimes) to notify any person of any PD Breach, including police, insurers, banks and credit card companies.
- 5.2 Other UK and EU laws which include notification requirements:
 - 5.2.1 trust service providers must notify their supervisory body (the UK ICO in the UK) of a security breach (Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market ('**eIDAS**');
 - 5.2.2 operators of essential services and for digital service providers have notification obligations under Directive (EU) 2016/1148 concerning measures for a high

common level of security of network and information systems across the Union ('**NIS Directive**') and

- 5.2.3 providers of communication service providers must notify security breaches to the competent national authorities (again the UK ICO in the UK) within the context of Directive 2002/58/EC37 ('**ePrivacy Directive**'), Directive 2009/136/EC ('**Citizens' Rights Directive**') and Regulation 611/2013 ('**Breach Notification Regulation**').

Quotations are from the Art 29 WP *Guidelines on Personal data breach notification under Regulation 2016/679* WP250rev01 adopted 6 February 2018 unless otherwise stated.

The Policy

- 5.3 We will take all commercially reasonable and appropriate measures to minimise or negate both the likelihood of a Personal Data Breach and the severity of the risk to individuals should a PD Breach occur. These measures include implementation of our Information Security Policy, Encryption Policy and Business Continuity & Disaster Recovery Plan. For example:
 - 5.3.1 encryption and pseudonymisation address the risk from a 'Confidentiality Breach', where there is an unauthorised or accidental disclosure of, or access to, personal data;
 - 5.3.2 effective backups address the risk from an 'Availability Breach', where there is an accidental or unauthorised loss of access to, or destruction of, personal data; and
 - 5.3.3 secure log files and least-privilege access address the risk from an 'Integrity Breach', where there is an unauthorised or accidental alteration of personal data.
- 5.4 Should we suspect a PD Breach, we will promptly implement the response plan set out in this policy and related procedure to:
 - 5.4.1 detect a suspected or actual PD Breach and confirm if a PD Breach has occurred,
 - 5.4.2 escalate a suspected or actual PD Breach to the relevant stakeholders,
 - 5.4.3 contain the breach and prevent recurrence,
 - 5.4.4 assess the risk to individuals,
 - 5.4.5 determine whether notification to the regulator or individuals is necessary and make any required notification, and
 - 5.4.6 document the breach throughout, including timings, actions taken, and lessons learned. The PD Breach Report must be completed for each reported suspected or actual PD Breach and will help guide you through the process.

- 5.5 Where we are joint controllers with another person, we will have a written arrangement with that joint controller as to our respective obligations in responding to PD Breaches and we will follow that arrangement regarding any PD Breach.
- 5.6 Not every security incident or information security breach need also be a PD Breach. If no personal data is involved, it will not be a PD Breach, however, the Information Security Breach Policy must still be followed. If a PD Breach is suspected, or occurs, then this policy will also apply and take precedence.

Detection

- 5.7 As the UK ICO notes, a PD Breach can happen for a number of reasons, examples of which are:
- 5.7.1 loss or theft of data or equipment on which data is stored
 - 5.7.2 inappropriate access controls allowing unauthorised use
 - 5.7.3 equipment failure
 - 5.7.4 human error
 - 5.7.5 unforeseen circumstances such as a fire or flood
 - 5.7.6 hacking attack
 - 5.7.7 'blagging' offences where information is obtained by deceiving the organisation who holds it.
- 5.8 We will implement appropriate internal processes to be able to detect and address a Personal Data Breach. Operationally, we will maintain training and awareness in relation to this policy, highlighting the importance of detection and escalation of suspected Personal Data Breaches, including responding to any reports of the same from customers or any other source. We will also consider use, if and as appropriate, of technical measures such as data flow and log analysers to identify irregularities in data processing.

Escalation and Leadership

- 5.9 If any person suspects a PD Breach has occurred, they must immediately notify the Director of Corporate Services by email as set out below and verbally through a face-to-face or telephone conversation. The Corporate Services Team will start an online breach record using Keepabl, our tool for breach management. Relevant contact details are:

Person	Phone	Email
Director of Corporate Services	07773 641352	dataprotection@brunelcare.org.uk
Data Protection Officer	07745 880105	clare@cpdataprotection.com
Head of Digital Services	07825 302790	joel.buchan@brunelcare.org.uk

- 5.10 The Director of Corporate Services will take the lead in responding to a PD Breach and may delegate operational management of particular breaches as appropriate. The Director of Corporate Services will ensure that sufficient resources are available to respond to the PD Breach.
- 5.11 The Director of Corporate Services, or their respective delegate, will liaise at all times with the DPO in the management of the PD Breach and implementation of this policy and the Information Security Breach Policy.

Containment and Recovery

- 5.12 The PD Breach must be rapidly contained, where possible in liaison with the Head of Digital Services. However, such liaison may not be appropriate or possible in order to effect immediate measures to rectify the breach as quickly as reasonably possible (such as recalling an email or retrieving a package).
- 5.13 Additional measures may be necessary to prevent recurrence of the breach, some of which may be taken rapidly (such as disabling certain users' access or changing passwords) and some may require more time to implement, in which case we will consider what interim measures may be deployed to address the risk in the meantime.
- 5.14 Measures to contain the PD Breach will directly impact the assessment of the risk to data subjects and those measures that most reduce that risk must be prioritised. Examples are given in the PD Breach Procedure, issued under this policy.

Assessing the Risk to Individuals

- 5.15 In case of a PD Breach, the Director of Corporate Services, or their delegate, will assess whether there is any likely risk to the rights and freedoms of individuals.
- 5.16 Risks include physical, material or non-material damage such as an individual's loss of control over their personal data, limitation of their rights, discrimination, identity theft, fraud, financial loss, damage to reputation, loss of confidentiality and significant economic or social disadvantage.
- 5.17 Guidance on assessing the risk to individuals is set out in the PD Breach Procedure, issued under this policy. As an example of different levels of risk from similar breaches the Art 29 WP notes:

'In the context of a hospital, if critical medical data about patients are unavailable, even temporarily, this could present a risk to individuals' rights and freedoms; for example, operations may be cancelled and lives put at risk. Conversely, in the case of a media company's systems being unavailable for several hours (e.g. due to a power outage), if that company is then prevented from sending newsletters to its subscribers, this is unlikely to present a risk to individuals' rights and freedoms.'

Notification and Communication

- 5.18 The PD Breach Procedure contains further guidance on when notifications and communications are - and are not - necessary under GDPR and how to make them if required. In summary, our notification obligations under the GDPR are driven by the assessment of the risk to the rights and freedoms of individuals.

5.18.1 *Where there is no likely risk:*

No notification is required, either to regulators or data subjects.

5.18.2 *Where there is a likely risk:*

We will need to notify the UK ICO (our 'competent supervisory authority') without undue delay and no later than 72 hours of becoming aware of the PD Breach. This notification will be performed by the Director of Corporate Services or their delegate.

Where, and to the extent that, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5.18.3 *Where there is a likely high risk:*

We will need to notify the UK ICO (our 'competent supervisory authority') as above and the affected data subjects (individuals) without undue delay from becoming aware of the PD Breach. Again, this communication will be performed by the Director of Corporate Services or their delegate.

- 5.19 We will consider the urgency of notification to data subjects in each case:

5.19.1 if there is an immediate threat of identity theft, or if special categories of personal data are disclosed online, notification to data subjects might even take place before notifying the supervisory authority; however

5.19.2 there may be reasons connected to law enforcement that require notification to data subjects to happen only after liaison with the UK ICO and other relevant authorities.

'Aware'

- 5.22 We will be 'aware' of a PD Breach when we have 'a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised'. While we may undertake a short period of investigation to establish whether or not a PD Breach has in fact occurred and, during that period of investigation we may not be regarded as being 'aware', that initial investigation should happen as soon as possible and cannot be for an extended period.

- 5.21 The Art 29 WP gives examples, including:

5.21.1 'A third party informs a controller that they have accidentally received the personal data of one of its customers and provides evidence of the unauthorised disclosure. As the controller has been presented with clear

evidence of a confidentiality breach then there can be no doubt that it has become “aware”.’

5.21.2 ‘A controller detects that there has been a possible intrusion into its network. The controller checks its systems to establish whether personal data held on that system has been compromised and confirms this is the case. Once again, as the controller now has clear evidence of a breach there can be no doubt that it has become “aware”.’

5.21.3 ‘A cybercriminal contacts the controller after having hacked its system in order to ask for a ransom. In that case, after checking its system to confirm it has been attacked the controller has clear evidence that a breach has occurred and there is no doubt that it has become aware.’

5.22 The GDPR places a direct obligation on our processors to notify us without undue delay on becoming aware of a PD Breach. However, as regulators may consider us to be ‘aware’ once our processor is aware of a breach, our agreements with processors will specify this obligation.

Records

5.23 The Corporate Services Team shall record all relevant information regarding the suspected or actual PD Breach in the PD Breach Report for each reported suspected or actual PD Breach and update the PD Breach Log.

Approved Codes of Conduct and Certifications

5.24 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 the security requirements in the GDPR. If necessary or appropriate, Brunelcare will review such codes and certification mechanisms for relevance and fit for our operations.

Breach

5.25 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 and Digital Services Team at joel.buchan@brunelcare.org.uk.

Enforcement

5.26 All Brunelcare colleagues bear responsibility for their own compliance with this policy. Breach of this policy is ground for disciplinary proceedings against an colleagues, 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

5.27 The Director of Corporate Services 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.

Colleagues

- 6.11 All colleagues have individual responsibility for complying with this policy and following accompanying guidance.
- 6.12 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 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.

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 commission reviews where the Policy has not been adhered to identify any lessons learnt and advise on changes to systems and processes as appropriate.
- 9.3 This policy will be reconsidered against any legislative changes and reviewed at least every three years.