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 This is to avoid the risk of out of date printed versions of the document.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

PRIVACY AND CONFIDENTIALITY POLICY / PROCEDURE

CATEGORY:	Policy & Procedure
CLASSIFICATION:	Information Governance
PURPOSE:	To set out Brunelcare's approach to the management of privacy and confidentiality
CONTROLLED DOCUMENT NUMBER:	BC/IG/007 (replaces BC/CG/020)
VERSION NUMBER:	V003
CONTROLLED DOCUMENT EXEC TEAM LEAD:	Director of Corporate Services
CONTROLLED DOCUMENT AUTHOR:	Director of Corporate Services
APPROVED BY:	Senior Leadership Team
APPROVED ON:	22 March 2023
IMPLEMENTED ON:	28 April 2023
REVIEW PERIOD:	Every 3 years - unless changes to legislation, best practice or internal roles and responsibilities
REVIEW DATE:	Reviewed in September 2025 – to reflect new Executive Team Structure Next full review: March 2026
ASSOCIATED DOCUMENTS:	Computer Users Code of Practice Clear Desk, Clear Screen Policy Data Protection Policy
Essential Reading for:	Trustees, all colleagues and contract staff.

Document Consultation and Review Process

Groups/Individuals who have overseen the development of this Policy:	Corporate Governance Team, Senior Leadership Team

Document version control:

Date	Version	Amendments made	Amendments Approved by
March 2022	V002	Policy fully reviewed in line with legislative and best practice requirements. Updated to new agreed controlled documents policy format.	SLT
March 2023	V002	Policy reviewed - no amends made	SLT
September 2025	V003	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:	**March 2023 – V002**
Date Published on the Hub:	**March 2023 – V002** **September 2025 - V003**
Does it need to be published on website:	**Yes**

CONTENTS

1. POLICY STATEMENT 4

2. AIM OF THE POLICY AND RELATED LEGISLATION 4

3. SCOPE OF THE POLICY 5

4. DEFINITIONS 5

5. KEY PRINCIPLES AND REQUIREMENTS 5

6. ROLES AND RESPONSIBILITIES 9

7. EQUALITY AND DATA PROTECTION 10

8. IMPLEMENTATION AND TRAINING 11

9. MONITORING AND REVIEW 11

Appendix A 12

1. POLICY STATEMENT

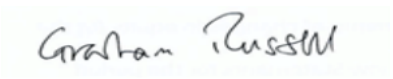
1.1 Brunelcare commits to the highest levels of care for customers and colleagues. This includes their personal data.

1.2 All colleagues are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and data protection legislation – the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA2018).

1.3 It is important that Brunelcare protects and safeguards person-identifiable and confidential business information that it gathers, creates processes and discloses data in order to comply with the law, relevant regulatory body requirements and to provide assurance to customers.

1.4 This policy sets out the requirements placed on employees (colleagues) when sharing information within Brunelcare and between partnering organisations.

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 purpose of this Policy is to lay down the principles that must be observed by all who work for Brunelcare and have access to person-identifiable information or confidential information. All colleagues need to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

Legislative and Legal requirements:

- Anonymisation: Code of Practice
- The Information Governance Review
- Computer Misuse Act 1990
- Data Protection Act 2018
- Care Act 2014
- Health and Social Care Act 2008 (Regulated Activities)Regulations 2014
- Mental Capacity Act 2005
- Freedom of Information Act 2000
- Human Rights Act 1998
- Access to Health Records 1990

3. SCOPE OF THE POLICY

3.1 All colleagues, trustees and volunteers are within the scope of this policy without limitation.

4. DEFINITIONS

4.1 '*Person-identifiable information*' is anything that contains the means to identify a person (e.g. name, address, postcode, date of birth, health information) and must not be stored on removable media unless it is encrypted as per current Charity requirements and policies.

4.2 Confidential information within the care setting is commonly thought of as health information; however, it can also include information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including customer health information, colleague records and occupational health records. This policy also covers Brunelcare confidential business information.

4.3 Information can relate to customers and colleagues (including temporary staff), however stored. Information may be held on paper, CD/DVD, USB sticks, computer files or print-outs, laptops, palmtops, mobile phones, digital cameras or even heard by word of mouth.

5. KEY PRINCIPLES AND REQUIREMENTS

5.1 All colleagues must ensure that the following principles are adhered to:

5.1.1 Person-identifiable or confidential information will be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of.

5.1.2 Access to person-identifiable or confidential information will only be given on a need to know basis.

5.1.3 Disclosure of person-identifiable or confidential information will be limited to that purpose for which it is required.

5.1.4 Recipients of disclosed information will respect that it has been given to them in confidence.

5.1.5 If the decision is taken to disclose information, that decision will be justified and documented.

5.1.6 Any concerns about disclosure of information will be discussed with the colleague's Line Manager or the Corporate Services Team.

5.2 Brunelcare is responsible for protecting all the information it holds and must always be able to justify any decision to share information.

5.3 Person-identifiable information, wherever appropriate and in line with the data protection principles stated in the Charity's Data Protection Policy, will be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data in line with the ICO's Anonymisation Code of Practice.

5.4 Access to rooms and offices where terminals are present, or person-identifiable or confidential information is stored will be controlled. Doors will be locked with keys, keypads or accessed by swipe card. In mixed office environments measures will be in place to prevent oversight of person-identifiable information by unauthorised parties.

5.5 All colleagueswill keep a clear desk in line with the Charity's Clear Desk, Clear Screen Policy. In particular, all records containing person-identifiable or confidential information will be stored in recognised filing and storage places that are appropriately locked.

5.6 Unwanted printouts containing person-identifiable or confidential information will be put into a confidential waste bin. Discs, tapes, printouts and email messages must not be left lying around but be filed and locked away when not in use.

5.7 Brunelcare's Contract of Employment includes a commitment to confidentiality. Breaches of confidentiality may be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal.

Disclosing Personal/Confidential Information

5.8 To ensure that information is only shared with the appropriate people in appropriate circumstances, care will be taken to check that the requesting party has a legal basis for access to the information before it is released.

5.9 It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed.

5.10 Information may be disclosed:

5.10.1 When effectively anonymised in accordance with the Information Commissioner's Office Anonymisation Code of Practice (https://ico.org.uk/).

5.10.2 When the information is required by law or under a court order. In this situation colleagues will contact the Corporate Services Team and Data Protection Officer by emailing dataprotection@brunelcare.org.uk. The Corporate Services Team will consult the Data Protection Officer (DPO) before advising.

5.10.3 Where disclosure can be justified for another purpose, this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In this situation colleagues will contact the Corporate Services Team and Data Protection Officer by emailing dataprotection@brunelcare.org.uk. The Corporate Services Team will consult the Data Protection Officer (DPO) before advising.

5.10.4 For any proposed routine disclosures of personal/confidential information, please consult the Corporate Services Team to assess requirements for new processes and to understand whether a Data Protection Impact Assessment needs to be undertaken.

5.11 If colleagues have any concerns about disclosing information, they will contact the Corporate Services Team and Data Protection Officer by emailing dataprotection@brunelcare.org.uk. The Corporate Services Team will then consult the DPO if necessary, before advising. Care must be taken in transferring information to ensure that the method used is as secure as it can be. Data sharing agreements provide a way to formalise arrangements between organisations. For further information on Data Sharing Agreements contact the Corporate Services Team.

5.12 Colleagues must ensure that appropriate standards and safeguards are in place to protect against inappropriate disclosures of confidential personal data.

5.13 When transferring customer information or other confidential information by email, services or methods that meet Brunelcare encryption standards must be used. Emails between Brunelcare Mail accounts meet this requirement (brunelcare.org.uk to brunelcare.org.uk). Where an email needs to be shared outside of the Charity's domain, colleagues will consult the Corporate Services Team and the Data Protection Officer for advice.

5.14 It is not permitted to include confidential or sensitive information in the body of an email. When emailing to addresses other than to a Brunelcare address, the information must be sent as an encrypted attachment using the appropriate system.

5.15 Sending information via email to customers is permissible, provided the risks of using unencrypted email have been explained to them, they have given their consent, or the information does not constitute person-identifiable or confidential information.

Working Away from the Office Environment

5.16 There will be times when colleagues may need to work from another location or whilst travelling. This means that these colleagues may need to carry Brunelcare

information with them which could be confidential in nature (e.g. on a laptop, USB stick or paper documents). The Charity's Smartphone and Mobile Device Policy will be followed at all times.

5.17 Taking home/removing paper documents that contain person-identifiable or confidential information from Brunelcare premises is discouraged.

5.18 To ensure safety of confidential information, colleagues must keep them on their person at all times whilst travelling and ensure that they are kept in a secure place if they take them home or to another location. Confidential information must be safeguarded at all times and kept in lockable locations.

5.19 When working away from Brunelcare locations,colleagues must ensure that their working practice complies with Brunelcare's policies and procedures. Any electronic removable media must be encrypted as per the current requirements.

5.20 Colleagues must minimise the amount of person-identifiable information that is taken away from Brunelcare premises.

5.21 If colleagues need to carry person-identifiable or confidential information they must ensure the following:

- Any personal information is in a sealed non-transparent container (i.e. windowless envelope, suitable bag, etc.) prior to being taken out of Brunelcare buildings.
- Confidential information is kept out of sight whilst being transported.

5.22 If colleagues need to take person-identifiable or confidential information home, they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or have any access to the information. It is particularly important that confidential information in any form is not left unattended at any time, for example in a car.

5.23 Colleagues will not forward any person-identifiable or confidential information via email to their home email account. Colleagues will not use or store person-identifiable or confidential information on a privately-owned computer or device unless this has been authorised as per the Charity's Bring Your Own Device Policy.

Carelessness

5.24 All colleagues have a legal duty of confidence to keep person-identifiable or confidential information private and not to divulge information accidentally. Colleagues may be held personally liable for a breach of confidence and must not:

- Talk about person-identifiable or confidential information in public places or where they can be overheard;
- Leave any person-identifiable or confidential information lying around unattended, this includes telephone messages, computer printouts, faxes and other documents;

- Leave a computer terminal logged on to a system where person-identifiable or confidential information can be accessed, unattended.

5.25 Steps must be taken to ensure physical safety and security of person-identifiable, or business confidential information held in paper format and on computers.

5.26 Passwords must be kept secure and must not be disclosed to unauthorised persons. Colleagues must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. Allowing another person to use your password to access the network, may constitute a disciplinary offence.

Abuse of Privilege

5.27 It is strictly forbidden for colleagues to knowingly browse, search for or look at any personal or confidential information about themselves without a legitimate purpose, unless through established self-service mechanisms where such access is permitted (e.g. viewing your employment record). Under no circumstances should colleagues access records about their own family, friends or other persons without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and may be an offence under the Data Protection Act 2018.

5.28 When dealing with person-identifiable or confidential information of any nature, colleagues must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of Brunelcare.

5.29 If colleagues have concerns about this issue they should discuss it with their Line Manager, Corporate Services Team or the DPO.

Confidentiality Audits

5.30 Good practice requires that all organisations that handle person-identifiable or confidential information put in place processes to highlight actual or potential confidentiality breaches in their systems, alongside procedures to evaluate the effectiveness of controls within these systems. This function will be coordinated by the Corporate Services Team through a programme of audits.

6. ROLES AND RESPONSIBILITIES

Board

6.1 It is the Board's responsibility to ensure that robust policies are in place to protect privacy and confidentiality.

Executive Team

6.2 The Executive Team has responsibility for ensuring that Brunelcare policies comply with all legal, statutory and good practice guidance requirements.

6.3 The Executive Team will role model the behaviours they expect to see under this policy, namely keeping private and confidential information secure whether that be in paper, digital or verbal format.

Director of Corporate Services

6.4 Responsibility for this policy has been delegated to the Director of Corporate Services who will keep this policy up to date, ensure that it is communicated effectively and implement adequate monitoring to ensure the security of private and confidential information.

6.5 The Director of Corporate Services is responsible for providing advice on request to any colleague on the issues covered within this policy and ensuring that training is provided for all colleagues to further their understanding of the principles and their application.

6.6 The Director of Corporate Services is responsible for ensuring that the contracts of all colleagues (permanent and temporary) are compliant with the requirements of the policy and that confidentiality is included in corporate inductions for all colleagues.

Data Protection Officer (DPO)

6.7 The DPO provides advice to the organisation and all of its colleagues on data protection issues which can include confidentiality issues which will be reviewed in collaboration with the Director of Corporate Services, as appropriate, to ensure the organisation's compliance with data protection law.

Line Managers

6.8 Line Managers are responsible for making themselves aware of the contents of this policy and to role model the behaviours they expect to see under this policy.

6.9 Line Managers will ensure that confidential information is kept secure whether that be in paper, digital or verbal format. Line Managers will ensure that their team members are aware of their responsibilities under this policy.

6.10 Line Managers are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. They must ensure that any breaches of the policy are reported, investigated and acted upon via Brunelcare’s policies.

All Colleagues

6.11 Confidentiality is an obligation for all colleagues. There is a Confidentiality clause in the contract of employment and it is mandatory to participate in induction, training and awareness raising sessions carried out to inform and update colleagues on confidentiality issues.

6.12 Any breach of confidentiality, inappropriate use of health data, colleague records or business sensitive/confidential information, or abuse of computer systems is a disciplinary offence, which could result in dismissal or termination of employment

contract. Any incidents must be reported to an appropriate line manager and documented fully.

7. EQUALITY AND DATA PROTECTION

Equality and Diversity

7.1 Brunelcare seeks to embed an environment where all clients, visitors and colleagues are treated as individuals, fairly and in a consistent way. The Charity works 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 it holds, and to provide and protect all such data.

7.3 Brunelcare is dedicated to safeguarding the personal information under the Charity's control and in maintaining a system that meets our obligations under the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018. The Charity's practice related to data protection is set out in Brunelcare's Data Protection Policy.

8. IMPLEMENTATION AND TRAINING

8.1 This policy will be made available to all colleagues via the Brunelcare intranet site. Managers will ensure that all team members are aware of their obligations under this policy.

8.2 Formal training will be provided via the Brunelcare e-learning platform.

9. MONITORING AND REVIEW

9.1 Compliance with the policies and procedures laid down in this document will be monitored by the Corporate Services Team and may be subject to external audit.

9.2 The Director of Corporate Services is responsible for the monitoring, revision and updating of this document every two years, or sooner if the need arises.

Appendix A

Confidentiality Do and Do Nots

Do:

- Safeguard the confidentiality of all person-identifiable or confidential information that you come into contact with. This is a statutory obligation on everyone working on or behalf of Brunelcare.
- Clear your desk at the end of each day, keeping all non-digital records containing person-identifiable or confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.
- Switch off computers with access to person-identifiable or business confidential information, or put them into a password protected mode, if you leave your desk for any length of time.
- Ensure that you cannot be overheard when discussing confidential matters.
- Challenge and verify, where necessary, the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know.
- Share only the minimum information necessary.
- Transfer person-identifiable or confidential information securely, using approved systems, when necessary.
- Seek advice if you need to share customer/person-identifiable information without the consent of the customer/identifiable person's consent and record the decision and any action taken.
- Report any actual or suspected breaches of confidentiality.
- Participate in induction, training and awareness raising sessions on confidentiality issues.

Do Not

- Share passwords or leave them lying around for others to see.
- Share information without the consent of the person to which the information relates, unless there are statutory grounds to do so.
- Use person-identifiable information unless absolutely necessary and anonymise the information where possible.
- Collect, hold or process more information than you need, and do not keep it for longer than necessary