

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 This is to avoid the risk of out of date printed versions of the document.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

## SURVEILLANCE AND CCTV POLICY

<b>CATEGORY:</b>	Policy
<b>CLASSIFICATION:</b>	Information Governance
<b>PURPOSE:</b>	To set out Brunelcare's policy regarding the use of surveillance and CCTV across all settings
<b>CONTROLLED DOCUMENT NUMBER:</b>	BC/IG/006 (replaces IS007)
<b>VERSION NUMBER:</b>	V003
<b>CONTROLLED DOCUMENT SENIOR LEADERSHIP TEAM LEAD:</b>	Director of Corporate Services
<b>CONTROLLED DOCUMENT AUTHOR:</b>	Director of Corporate Services
<b>APPROVED BY:</b>	Senior Leadership Team
<b>APPROVED ON:</b>	22 March 2023
<b>IMPLEMENTED ON:</b>	28 April 2023
<b>REVIEW PERIOD:</b>	Every 3 years - unless legislation or best practice changes
<b>REVIEW DATE:</b>	Latest Review Date: July 2025 – to reflect new Executive Team Structure Next full review date March 2028
<b>ASSOCIATED DOCUMENTS:</b>	Data Protection Policy Privacy and Confidentiality Policy Anti-social Behaviour and hate Crime Policy Data Subject Access Request Policy and Procedure Managing Comments, Concerns, Complaints and Compliments Policy and Procedure Personal Data Assessments and Privacy Notices Threat and Security Risk Assessments Image Tracking Register
<b>Essential Reading for:</b>	All Trustees and employees (colleagues)

<b>Information for:</b>	Customers
-------------------------	-----------

#### Document Consultation and Review Process

<b>Groups/Individuals who have overseen the development of this Policy:</b>	Corporate Governance Team, Senior Leadership Team (V001)
---	--

#### Document version control:

Date	Version	Amendments made	Amendments Approved by
March 2023	V002	Policy fully reviewed in line with legislative and best practice requirements. Updated to new agreed controlled documents policy format.	SLT
July 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:

<b>Date added to Register:</b>	March 2023
<b>Date published on the Hub:</b>	March 2023 (V003) August 2025 (V003)
<b>Does it need to be published on website:</b>	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 .....	6
4. DEFINITIONS .....	6
5. KEY PRINCIPLES AND REQUIREMENTS .....	7
6. ROLES AND RESPONSIBILITIES .....	14
7. EQUALITY AND DATA PROTECTION .....	15
8. IMPLEMENTATION AND TRAINING .....	16
9. MONITORING AND REVIEW .....	16
APPENDIX A .....	17

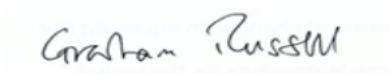
## 1. POLICY STATEMENT

- 1.1 Brunelcare owns and operates CCTV at various premises, including offices, residential properties and community facilities. The organisation does this for the purpose of enhancing security where it is considered there may be a risk of crime or a potential threat to the health, safety and well-being of individuals; and to assist in the prevention and detection of criminal or anti-social behaviour.
- 1.2 Brunelcare acknowledges the obligations it incurs in operating such systems and the rights and freedoms of those whose images may be captured. Brunelcare is committed to operating them fairly and within the law at all times and in particular will comply with the requirements of the UK General Data Protection Regulation (UK GDPR) and UK Data Protection Act 2018 (the DPA 2018).
- 1.3 This policy governs Brunelcare's approach to installing and operating CCTV and other forms of surveillance systems and handling the information obtained. It is underpinned by the following key principles:
  - 1.3.1 Brunelcare's practice will at all times follow applicable legislation and guidance in relation to data protection and surveillance technology.
  - 1.3.2 Surveillance systems will only be installed where it is considered a necessary and proportionate way to deal with issues or to protect the safety and security of those using or supplying Brunelcare's services.
  - 1.3.2 Systems will only be installed with due consideration to all alternative options.
  - 1.3.3 All surveillance equipment will be planned, designed and installed in a way that ensures minimal intrusion of privacy.
  - 1.3.4 Systems will be appropriately specified and professionally installed, having due regard to appropriate technical and legal advice and other relevant guidance.
  - 1.3.5 Appropriate technical and organisational measures will be employed to ensure the security of the organisation's systems and personal data, including relevant controls to govern access to and use of images.
  - 1.3.6 Appropriate measures will be taken to provide clear and accessible privacy information to individuals whose personal data is processed by systems.
  - 1.3.7 When installing surveillance systems inside, this will only be operated in areas which are communal such as receptions, entrances, corridors and dining areas.
  - 1.3.8 Surveillance technology operated by Brunelcare will not be placed in private areas such as private offices, bedrooms, staff rooms, changing rooms, or toilets unless, in exceptional circumstances, this is deemed necessary for the investigation of a serious crime or where there is a serious risk to health and safety or to the operation of the organisation. In such cases surveillance will not be installed without the express authorisation of the Chief Executive Officer, the Director of Corporate Services and the organisation's Data

Protection Officer in line with appropriate legislation and guidance. The Information Commissioner's Office will also be consulted in such situations.

- 1.3.9 Brunelcare will not put in place or use newly recognised technology, such as facial or gait recognition, Automatic Number Plate Recognition (ANPR), or thermal imaging without first conducting a full Data Protection Impact Assessment and seeking the approval of senior management.
- 1.4 This policy will be supplemented by comprehensive procedures, which provide detailed operational guidance on the installation, operation, use and maintenance of our systems.
- 1.5 Brunelcare recognises the increasing popularity of personal household surveillance systems and that tenants or residents may wish to install these in their homes. Without exception, Brunelcare shall not accept any responsibility for such installations or liability for the images they capture. Domestic use of surveillance systems, and the footage captured by them, is exempt from the UK GDPR, as long as use is purely for personal and household purposes.

**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 sets out how Brunelcare implements, manages and maintains surveillance systems in a way that is consistent with current legislation and best practice.
- 2.2 This policy ensures ongoing compliance with relevant data protection legislation and ensures the privacy rights of all those using the organisation's services (including employees (colleagues) and volunteers) are protected.

### **Relevant Legislation and Guidance**

[Data Protection Act 2018](#)

[Retained Regulation \(EU\) 2016/679 \(UK GDPR\)](#)

[Criminal Procedure and Investigations Act 1996](#)

[Protection of Freedoms Act 2012](#)

[Human Rights Act 1998](#)

[Regulation of Investigatory Powers Act 2000](#)

[Mental Capacity Act 2005](#)

[Home Office Surveillance Camera Code of Practice 2021](#)

[CQC guidance for providers of health and social care on using surveillance in care services](#)

[Surveillance Camera Commissioner's "Passport to Compliance" Guidance](#)

[European Data Protection Board's "Guidelines 3/2019 on processing of personal data through video devices \(Version 2.1 February 2020\)"](#)

***Note: Brunelcare is not a relevant authority in relation to the Freedom of Information Act 2000 (FOIA) or the Private Security Industry Act 2001. This means that Brunelcare does not have to obtain any necessary licences for the operation of CCTV cameras from the Security Industry Authority (SIA) or any other regulatory body.***

***Brunelcare is not a relevant authority with regards to the Protection of Freedoms Act 2012 (POFA), but as a data controller we are encouraged to follow the POFA code of practice.***

### 3. SCOPE OF THE POLICY

- 3.1 This policy applies to all colleagues, customers, visitors, suppliers and contractors of Brunelcare whether permanent or temporary.
- 3.2 This policy covers the use of all surveillance technology (including CCTV) which records identifiable images of people whilst on Brunelcare's premises.
- 3.3 This policy will not cover the use of conventional cameras or surveillance used for artistic, administrative, educational or research purposes. Nor does it cover mobile video systems such as body worn video or dashboard-mounted cameras.
- 3.4 Where used, CCTV will be used to:
  - detect, investigate and prevent anti-social behaviour;
  - obtain evidence to support tenancy enforcement action (where appropriate); and
  - assist the police, local authority and any other organisation in combatting anti-social behaviour.

### 4. DEFINITIONS

- 4.1 '***Overt surveillance***' is surveillance that is carried out in the full knowledge of individuals using the service, colleagues and the public who may be recorded through the system being used. This is what is covered by the term '***surveillance***' within this policy unless otherwise stated. Surveillance in most circumstances will refer to Closed Circuit Television systems (CCTV).

- 4.2 'Covert surveillance' is surveillance that is carried out secretly and without the knowledge of those being recorded (e.g. through a hidden camera). The Regulations of Investigatory Powers Act 2000 (RIPA) govern the use of covert surveillance to ensure that it is used only when necessary, reasonable and proportionate. Whilst it does not apply to charities, the organisation will follow RIPA as closely as possible when using covert surveillance techniques in appropriate cases. Brunelcare will only use 'directed surveillance' in exceptional circumstances.

'Directed surveillance' is surveillance which meets the following conditions:

- It is covert but not intrusive (i.e. it does not intrude into anything taking place in any private residential premises or any private vehicle).
  - It is conducted for the purpose of a specific investigation.
  - It is likely to result in the obtaining of private information about a person.
  - It is conducted other than by way of an immediate response to events or circumstances. To conduct directed surveillance, the following criteria will need to be satisfied:
    - It is for one of the following purposes: preventing or detecting anti-social behaviour, in the interests of public safety, or for the protection of public health.
    - It is necessary because other forms of information gathering have proved impossible or impractical.
    - It is proportionate in that the level of intrusion is outweighed by the need for the evidence to be obtained by the surveillance.
- 4.3 A 'data protection impact assessment (DPIA)' is an assessment used to determine the impact on privacy through the implementation and installation of a system (in this case a DPIA would be conducted to assess the appropriateness and impact of a surveillance system being installed).

## 5. KEY PRINCIPLES AND REQUIREMENTS

### Setting Out Reasons for installing CCTV and Surveillance systems

- 5.1 Brunelcare recognises that using CCTV and other surveillance systems can be privacy intrusive. As such it will not install systems as a routine response to incidents of a criminal or anti-social nature. Notwithstanding this, it is acknowledged that there is potential value of these systems as both a deterrent and a means of detection. All potential installations will be considered on a case by case basis. In doing so the aim will be to demonstrate that installation is a justified, proportionate and effective solution to an identified problem or risk.
- 5.2 Prior to taking steps to implement surveillance equipment, an assessment will be undertaken to identify the purpose for which the surveillance is being used, including what is hoped to be achieved by using the surveillance equipment. Consideration will always be given to whether the aims of the surveillance can be achieved in a way that is less intrusive to the privacy of individuals.

- 5.3 The reasons for installing surveillance equipment may be, but are not limited to: the prevention of crime and disorder, the apprehension and prosecution of suspected offenders or to provide evidence of misconduct, health and safety interests of colleagues and the public, the protection of public health/property and assets, monitoring security of the organisation's buildings, assisting in the identification of actions that may result in disciplinary proceedings against colleagues for serious misconduct and identifying the causes of unwitnessed falls and incidents
- 5.4 Once the purpose has been identified it will be considered whether this is legitimate under data protection legislation (see further the organisation's Data Protection Policy). This ensures the reason for surveillance is reasonable, lawful and appropriate. Where surveillance is implemented for one identified purpose, the information collected through this will not then be used for another purpose. Therefore, during the initial assessment of reasons for the surveillance, all legitimate reasons will be considered.
- 5.5 Within, or around, a care environment it is recognised that surveillance technology will likely collect certain forms of sensitive personal information and therefore extra conditions will be met under data protection legislation to protect this data.
- 5.6 Where the implementation of surveillance equipment is planned, a full Data Protection Impact Assessment (DPIA) will be completed in consultation with the Corporate Services Team and the organisation's Data Protection Officer.
- 5.7 The DPIA will be reviewed on a regular basis to ensure that the surveillance in place still meets its identified and agreed aims and whether any additional steps or amendments to the DPIA need to be undertaken.
- 5.8 The Corporate Services Team will maintain a register of DPIAs as a record of decision making, and installation authorisation and review. In the interests of transparency, the register and individual DPIAs shall be made publicly available on request. In setting out the reasons for surveillance, records will set out the purpose for using surveillance, initial assessments undertaken, the DPIA and what alternatives to surveillance have been considered.
- 5.9 Where a high-risk to individuals is identified following the DPIA and mitigating actions put in place, the Information Commissioner's Office will be consulted. In these instances, no surveillance will be undertaken until such consultation and sign-off has taken place.
- 5.10 For every surveillance system put in place, the checklist at Appendix A, also see below, will be completed and reviewed on an annual basis. This checklist is based on the Information Commissioner's Office checklist available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance/checklist-for-limited-cctv-systems/>

### **Consulting Individuals and Consent**

- 5.11 Wherever practicable, individuals who will be subject to or effected by surveillance will be consulted. This includes individuals using the organisation's services, the organisation's colleagues and visitors to the organisation's services.



- 5.12 Consultation will not be seen as a single or one-off exercise and will be repeated at different stages. Consultation will be held when it is first considered whether surveillance will be used, when detailed proposals have been made and from time-to-time when the surveillance is being used so that any ongoing concerns can be addressed and the impact of the surveillance reviewed.
- 5.13 When consultation is undertaken, people will be told the purpose for which the surveillance is being considered, what type of surveillance is being considered, where it would be used, what information will be collected from the surveillance, where and how the information will be stored, who will have access to the information and how long it will be stored for. Any responses and concerns raised will be recorded and responded to where appropriate.
- 5.14 Where consent is required for the surveillance to legally take place this will be recorded on an informed and individual basis. No-one will be disadvantaged should they refuse to provide consent.
- 5.15 Where individuals lack capacity to consent, the organisation's Mental Capacity and Deprivation of Liberty Safeguards Policy will be followed with all best interest decisions appropriately recorded.
- 5.16 In some situations it will not be possible to consult people (e.g. where covert surveillance is required to investigate abuse concerns). This will be in very limited situations and the Corporate Services Team and Data Protection Officer will be consulted throughout. Where this is necessary this will be recorded and a clear justification set out.

### **System Specification and Installation**

- 5.17 Brunelcare will procure and site systems in accordance with an agreed standard specification, which reflects recommended practices and incorporates privacy by design features. Relevant criteria will include, but not be limited to ensuring that:
- 5.17.1 personal data can be easily located and extracted;
  - 5.17.2 images are of an appropriate quality, relevant to their purpose;
  - 5.17.3 the date and time images are captured is easily identifiable;
  - 5.17.4 unnecessary images are not viewed or recorded;
  - 5.17.5 relevant retention periods can be complied with;
  - 5.17.6 image only systems are installed, which have no sound recording capability, as standard;
  - 5.17.7 cameras are sited to ensure only areas of interest are subject to surveillance and to minimise viewing areas not relevant to the purposes the system was installed for, with due regard given to planning permission requirements as necessary;
  - 5.17.8 cameras are sited to ensure they can produce good quality images taking into account the environment where located;
  - 5.17.9 cameras and equipment are sited in secure locations and are protected from unauthorised access and possible vandalism.

- 5.18 Brunelcare will engage the services of specialist contractors, in accordance with relevant procurement procedures, to advise on technical specifications and system configuration and design; and to carry out installation and maintenance. Such contractors will be required to demonstrate the appropriate credentials, expertise, and understanding of Brunelcare's data requirements and general data protection requirements.
- 5.19 Brunelcare will maintain a register of all system installations, detailing location and installation date, relevant technical specifications and system design features.

### Protecting Privacy

- 5.20 Surveillance will be used in a way that always protects people with dignity and respect.
- 5.21 Only those requiring access to the information collected through surveillance will be provided with access. A list will be kept and maintained of all of those with access to data collected from each individual surveillance asset.
- 5.22 Ways to lessen the impact on people's privacy will be considered through the decision to use surveillance. This may include: considering the position or cameras/microphones to only capture what is necessary, whether surveillance could only be used at certain times of the day (i.e. when the risks identified are most prevalent), finding ways to gather the information that does not identify people (e.g. sensors rather than video technology) or whether it would be possible to allow colleagues or people using the service to turn off the surveillance equipment at certain times.
- 5.23 Care will be taken not to record sensitive information (e.g. intimate care).
- 5.24 Audio will only be recorded where there is a clearly stated, recorded and legitimate reason for doing so, recognising that audio is more invasive than images only.
- 5.25 A record will be kept of all privacy concerns that were considered during the decision to implement surveillance technology and the actions taken to lessen any privacy impacts. This will also record any concerns that were considered but were not able to be addressed.

### Accessing Surveillance Recordings and Use of Images

- 5.26 Access to all equipment and images will be strictly controlled. Appropriate security measures will be in place to ensure entry to physical locations where data is held is limited to authorised personnel. Brunelcare will have in place a written data processing agreement with these surveillance contractors, where used, which is legally compliant and clearly defines obligations, responsibilities and liabilities.
- 5.27 Specialist contractors, appointed by Brunelcare, will be responsible for setting and maintaining relevant technical security controls for each system, including passwords or access codes and for maintaining physical and digital access logs.
- 5.28 Clear standards and procedures will be put in place for when people ask to access recordings. This will ensure appropriate steps are taken to protect the privacy of those captured in recordings and that the information shared is done so in an appropriate format.

- 5.29 As with any other requests for data, the organisation's Data Subject Access Request Policy will be followed at all times.
- 5.30 Where an individual makes a Subject Access Request and surveillance recordings are requested, the person making the request will be asked to provide, as appropriate for the situation: the date, time and location where they believe they were recorded by the organisation's surveillance systems, two or more photographs so that they can be identified within surveillance images (front and side view) and proof of identity such as a passport or driving licence containing a photograph. This will allow the organisation to satisfy itself as to the identity of the person making the request and locate the requested information.
- 5.31 Where surveillance data includes information regarding third parties not subject to the access request received, a review will be taken on a case-by-case basis to determine whether, and to what extent, the information relating to third parties will be redacted prior to the information being shared. In light of this it may be appropriate not to share the requested images to protect the privacy of third parties. It may be the case that only still images will be provided or a written statement on what information can be seen through the footage.
- 5.32 Where a request is received to access recordings this will be shared with the organisation's Data Protection Officer and Corporate Governance Team. This will occur with all requests whether the request has come from a private individual or a body such as adults safeguarding, CQC, the Police or the Coroner.
- 5.33 Where colleagues access surveillance recordings for an illegitimate reason or where they should not have access to recordings, appropriate disciplinary action will be taken.
- 5.34 Where surveillance systems are connected to the internet or enable remote viewing, appropriate safeguards will be maintained to ensure the security and integrity of the data and to prevent any illegitimate access or tampering.
- 5.35 All information gathered through surveillance will be kept secure at all times. The organisation's Data Retention and Disposal Policy makes clear how long surveillance recordings are kept for and how these will ultimately be securely destroyed at the end of the prescribed retention period.
- 5.36 Surveillance evidence will only be used against colleagues in disciplinary proceedings where such evidence tends to show, in the reasonable belief of the organisation, that the colleague may be guilty of serious misconduct. The colleague will be given the opportunity to review and respond to the images in these circumstances. The organisation's Disciplinary Policy will be followed at all times.
- 5.37 Where images have been extracted from surveillance recordings, any removal media (e.g. USB drives or DVDs) will be held according to the organisation's Data Retention and Disposal Policy, and access and security of the data will be maintained in line with data held within surveillance systems in line with the requirements within this policy.
- 5.38 Where a third party company handles or stores information gathered through the organisation's surveillance systems on the organisation's behalf, contracts agreed with

such third parties will outline clear rules of data processing, including use, access, retention and destruction.

- 5.39 Where the installation of surveillance may constitute a deprivation of liberty (see the organisation's Mental Capacity and Deprivation of Liberty Safeguards Policy) this will be reviewed to consider whether an authorisation is required.
- 5.40 All individuals and colleagues, when joining or visiting the service will be made aware that surveillance equipment is in place. Privacy Notices will be provided where appropriate and available on the organisation's website.
- 5.41 Appropriate signage will be put in place to advise individuals that recording equipment is in use and provide reasons as to why this is in place (e.g. the prevention of crime) and who to contact should any concerns be raised. This signage will be positioned in an area visible by all about to enter the service or areas which are subject to surveillance.
- 5.42 Where surveillance cameras are situated outside of the organisation's premises, these will be positioned to ensure they do not capture images of public spaces or other private property. These cameras will only focus on the external areas of the organisation's premises.
- 5.43 Where it is determined that a surveillance system is no longer required, appropriate steps will be taken to promptly remove the identified equipment. This process will involve the removal of all cameras, associated equipment and signage.

### **Equipment and Training**

- 5.44 Any surveillance equipment implemented will be fit for purpose and appropriate for the reason to which surveillance will be implemented.
- 5.45 Surveillance equipment will, where possible, be capable of collecting metadata (e.g. the time, date and location of the recording).
- 5.46 Surveillance equipment will maintain appropriate levels of data encryption standards at all times, with software updated and patched where required.
- 5.47 All surveillance equipment will be maintained and cleaned. It will be ensured that its placement and use will not pose a health and safety risk.
- 5.48 Surveillance equipment will be kept in a locked office to prevent unauthorised access. Systems supporting the surveillance equipment will be password protected with only those with a legitimate and lawful need to access this information allowed access to the surveillance system and this password.
- 5.49 All colleagues involved in the operating of surveillance systems, and the handling of information gathered through surveillance systems, will be appropriately trained.
- 5.50 The organisation's Managing Comments, Concerns, Complaints and Compliments Policy will deal with any complaints or concerns raised regarding surveillance undertaken by the organisation.

### **Private Surveillance in Care Settings**

- 5.51 The organisation recognises that there will be times when the family or representatives of a person being supported may have concerns about the care a loved one is receiving and use hidden (covert) cameras and/or microphones to give themselves reassurance.
- 5.52 Those concerned about the care their loved one is receiving will be encouraged to raise and discuss their concerns with the Manager of the service prior to installing surveillance equipment. The interests of the person receiving care will be put first in all situations.
- 5.53 Where private surveillance equipment is discovered, the care and support received by the person will not be prejudiced in any way. The same standard of care and support will be provided at all times and the person or their family will not be put at a disadvantage due to this.
- 5.54 Where private surveillance is discovered, the effect this will have on others using the service and their privacy rights will be considered as well as the privacy rights of colleagues providing care.
- 5.55 Where private surveillance equipment is discovered it may be the case that it would be appropriate to switch off the surveillance equipment and remove this from the service. The equipment will be kept in a safe place for the owner to collect. At no point will the equipment be deliberately damaged or any of the recordings deleted.
- 5.56 There may be situations where the installation of covert surveillance equipment breaches a contract of service. Where this is the case this will be discussed with all of those involved to resolve the situation.
- 5.57 The reasons behind the perceived need to install covert surveillance equipment will be investigated and dealt with in line with the organisation's Managing Comments, Concerns, Complaints and Compliments Policy

### **Private Surveillance in Housing Settings**

- 5.58 It is recognised that there may be instances where a tenant may wish to install personal household surveillance equipment within, or on the outside of, their home (e.g. video doorbells).
- 5.59 Such personal surveillance will be permitted provided that the installation of equipment does not impact the structural integrity of the property and that the area recorded does not include public areas or infringe the privacy of other tenants (e.g. look into their property). Tenants are responsible for ensuring private surveillance is compliant with data protection legislation.
- 5.60 Where it is discovered that surveillance equipment has been installed that breaches the tenant's tenancy agreement or is not in compliance with point 5.59 above, steps will be taken to seek removal of the surveillance equipment from the tenant's premises to protect the privacy rights of other tenants.

- 5.61 The organisation will not accept any responsibility for private surveillance installations or the images they capture.

## **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, including in data protection and the use of surveillance equipment.
- 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. This includes the use and management of surveillance equipment.

### **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. This includes legislation and best practice related to surveillance systems.

### **Director of Corporate Services**

- 6.6 The Director of Corporate Services has been delegated responsibility for ensuring organisational compliance with the Data Protection Act 2018, and is supported by the Data Protection Officer.
- 6.7 The Director of Corporate Services is responsible for ensuring that any substantive changes made to the policy will be communicated to all relevant personnel.

### **Data Protection Officer**

- 6.8 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. The DPO can be contacted at [dataprotection@brunelcare.org.uk](mailto:dataprotection@brunelcare.org.uk).
- 6.9 The DPO is responsible for monitoring progress and advising the organisation on implementation of this policy, acting as primary contact on any CCTV and surveillance related queries and approving responses to requests of access to surveillance data.
- 6.10 The DPO is responsible for monitoring the completion of all mandatory data protection training for all colleagues (including specialised training for those using and maintaining surveillance equipment) and ensuring access to further guidance and support.

- 6.11 The DPO will conduct regular assurance activity to monitor and assess new processing of personal data. This will include data processed through surveillance systems. The DPO will be able to advise on the completion and review of Data Protection Impact Assessments as required by this policy.
- 6.12 The DPO is the first point of contact for the regulatory authorities and for individuals whose data is processed through surveillance technology (colleagues, customers etc.).

#### **Senior Information Risk Owner (SIRO)**

- 6.13 The SIRO owns the overall risk arising from the processing of personal data by Brunelcare.

#### **Managers**

- 6.14 Managers of services where surveillance technology is used will be familiar with this policy and its contents, including the steps that need to be taken regarding surveillance technology on a day-to-day basis.
- 6.15 Managers are responsible for ensuring colleagues within their service adhere to this policy and complete appropriate training.

#### **Colleagues**

- 6.16 All colleagues have individual responsibility for complying with this policy and following accompanying guidance.
- 6.17 All colleagues will undertake relevant data protection training alongside any other training that shall be deemed as mandatory. This will be particularly the case for colleagues involved in the use and maintenance of surveillance systems.
- 6.18 Where colleagues suspect, or are made aware, of covert surveillance technology being in place within a service they have a responsibility to report this to their line manager so that any concerns can be addressed and appropriate action taken.

### **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 it holds, and to provide and protect all such data.

- 7.3 Brunelcare is dedicated to safeguarding the personal information under the organisation'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 organisation's practice related to data protection is set out in Brunelcare's Data Protection Policy.
- 7.4 It is recognised that processing of surveillance 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 All colleagues will receive data protection training on induction and on an ongoing basis to ensure this knowledge remains up-to-date with any new data protection principles shared.
- 8.2 Colleagues involved in the use, installation and access of surveillance equipment and recordings will be trained in its use.
- 8.3 Implementation and ongoing compliance to this policy will be monitored by the organisation's Data Protection Officer and Corporate Services Team.

## **9. MONITORING AND REVIEW**

- 9.1 As stated above, where surveillance technology has been put in place, the ongoing need for this, as well as its continued appropriateness, will be reviewed on an annual basis and recorded.
- 9.2 This policy will be reviewed on a three-yearly basis or sooner based on changes to legislation and guidance or where the author deems it required.



**Information Commissioner's Office Checklist for Limited CCTV Systems**

Location of Surveillance:	
Date Checklist Completed:	
Person Completing Checklist:	
Signed:	

This CCTV system and the images produced by it are controlled by:

Brunelcare, Saffron Gardens, Prospect Place, Whitehall, Bristol BS5 9FF (registered charity number: 201555 / registered company number: 601847)

who is responsible for how the system is used under the UK GDPR and Data Protection Act 2018.

We, Brunelcare, have considered the need for using CCTV and have decided it is necessary for the prevention and detection of crime and for protecting the safety of individuals, or the security of premises. We will not use the system for any incompatible purposes and we conduct regular reviews of our use of CCTV to ensure that it is still necessary and proportionate.

	Checked (date)	By	Date of next review
If our system is processing footage of identifiable individuals and is processing personal data, we have registered as a controller and submitted a relevant data protection fee to the Information Commissioner's Office (ICO). We have also recorded the next renewal date.			
There is a named individual who is responsible for the operation of the system.			
Prior to processing we have clearly defined the problem we are trying to address. We regularly review our decision to use a surveillance system.			
We have identified and documented an appropriate lawful basis for using the system, taking into consideration Article(s) 6, 9 and 10 of the UK GDPR and relevant Schedules of the DPA 2018.			

	Checked (date)	By	Date of next review
Our system produces clear images which we can easily disclose to authorised third parties. For example when law enforcement bodies (usually the police) require access to investigate a crime.			
We have positioned cameras in a way to avoid any unintentional capture of private land or individuals not visiting the premises.			
There are visible signs showing that CCTV is in operation. Contact details are displayed on the sign(s) if it is not obvious who is responsible for the system.			
We securely store images from this system for a defined period and only a limited number of authorised individuals may have access to them.			
Our organisation knows how to respond to individuals making requests for copies of their own images, or for images to be erased or restricted. If unsure the controller knows to seek advice and guidance from the Information Commissioner's Office (ICO) as soon as a request is made.			