

Surveillance Policy

CP025 Common Policies

August 2024

**Contents**

[1 Introduction 2](#_Toc173242351)

[2 Scope and Purpose 2](#_Toc173242352)

[3 Definitions 3](#_Toc173242353)

[4 Closed Circuit Television (CCTV) 4](#_Toc173242354)

[5 Surveillance Equipment Installed or Provided by individuals or Relatives 7](#_Toc173242357)

[6 Smart Devices (Care Homes) 10](#_Toc173242361)

[7 Roles and Responsibilities 10](#_Toc173242362)

[8 Training and Monitoring 13](#_Toc173242363)

[9 Communication and Dissemination 14](#_Toc173242364)

[10 Equality Impact Assessment (EIA) 14](#_Toc173242365)

[11 Resources 14](#_Toc173242366)

[12 Version Control 15](#_Toc173242367)

1. Introduction
   1. This policy details the requirements in respect of CCTV and other forms of surveillance under the UK GDPR and the Human Rights Act. MHA will maintain the confidentiality and integrity of images captured by its systems.
   2. The monitoring, recording, holding, and processing of images of distinguishable individuals constitutes personal data as defined by the Data Protection Act Legislation.
   3. MHA will only facilitate the operation of CCTV at specific locations where it is deemed necessary to do so and where there is a clear justification for its operation. This must be discussed and logged with the Data Protection Officer (DPO).
2. Scope and Purpose
   1. This policy provides a framework for systems managed by MHA, and for those being considered by family or friends of people supported in MHA’s services, to protect people captured on camera at our services including colleagues, volunteers, visitors, and contractors.
   2. This policy document has been developed to comply with relevant legislation and guidance:
   * Information Commissioner’s Office (ICO) – The ICO suggests that a Data Protection Impact Assessment (DPIA) is required, as CCTV is likely to result in a high risk to people.
   * Care Quality Commission (CQC) Under sections 62 and 63 of the Health and Social Care Act, inspectors have powers to view, copy or seize CCTV recordings.
   * Wales - A decision to use CCTV must be consistent with the Statutory Guidance that accompanies Regulation 44 of the Regulated Services (Service Providers and Responsible Individuals) (Wales) Regulations 2017.
   * Human Rights Act (1998) - the Act protects an individual’s right to a private and family life. The effect of the Act is consistent with the Data Protection Act, in that use of surveillance cameras has to be justifiable.
   * Data Protection Legislation – controls how personal information is used by organisations, businesses, or the government.
   1. This policy must be applied in conjunction with MHA’s data protection policies.
3. Definitions

| Term | Definition |
| --- | --- |
| **CCTV Camera** | CCTV cameras are usually wired and need a constant power source. They capture and record live images at a specific a location. |
| **Data Protection Officer (DPO)** | This term means an individual or entities whose role it is to  assist the controller, to monitor internal compliance, inform and  advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority. |
| **Data Protection Legislation** | This includes: the UK General Data Protection Regulations (UK GDPR), the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications Regulations (PECR) as updated from time to time. |
| **Data Subject** | An identifiable living person. For MHA this is past & present, living: colleagues, residents, family members and supporters or any person for whom MHA processed or has processed personal data. |
| **Information Commissioner’s Office (ICO):** | The ICO is the UK's independent body set up to  uphold information rights. The ICO has both responsibility for ensuring the UK GDPR (and other legislation/regulations) are upheld, as well as responding to concerns from data subjects. |
| **Personal Data** | Any information identifying a data subject or information relating to a data subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. |
| **Smart Devices** | A smart device is an electronic device, generally connected to other devices or networks via different wireless protocols (such as Bluetooth, Wi-Fi or 5G) that can operate, to some extent interactively and autonomously. Some types of smart devices are smartphones, laptops, tablets, smart speakers, and smartwatches. |
| **Surveillance** | Observation of a place, person or group, or ongoing activity in order to gather information. |
| **Surveillance Camera** | Surveillance cameras are wireless and can run on batteries or solar panels, which means they don’t require wires. They can easily be moved or fixed to moving items, e.g. people. They can capture and record live images of at various locations. |

1. Closed Circuit Television (CCTV)
   * 1. In order to protect vehicles, property and people using our services (including all visitors), MHA use CCTV systems on some of our properties. Where installed they have to comply with MHA’s requirements as detailed in the Data Protection Policy.
     2. To comply with Data Protection Legislation MHA completes a Data Protection Impact Assessment (DPIA) covering the use of CCTV, as they are deemed to be a high risk to the rights and freedoms of individuals. Internal systems are only considered for a specific purpose and period due to their invasion of privacy, a DPIA must be completed. If CCTV is being considered, changes to coverage is being considered, a system is being replaced or removed the DPO must be consulted.
     3. The DPIA concludes that all CCTV systems must:
2. Only use the system for crime prevention and detection - i.e. Not watching colleagues unless it relates to a crime.
3. Make sure the cameras only cover MHA property - i.e. Not roads, paths, or property outside our boundaries.
4. Have signs (yellow with CCTV image in a triangle) in visible location stating:
   * Methodist Homes is the Data Controller. It is acceptable to have Methodist Homes (MHA) but not just MHA.
   * The system is used for crime detection and prevention.
   * The contact telephone number is 01332 221888.
5. Be password protected with need-to-know access.
6. Have monitors turned off when not being used.
7. Record with a quality such that faces and vehicle registration numbers can be identified – day and night.
8. Ideally, have a process for extracting sections of the recording with all personal data not relating to the data subject being blurred - e.g. Other faces, children, vehicle registration numbers. If the system cannot do this MHA must arrange for the process to be done by a third-party.
9. Have recording restricted to a rolling 30 days.
10. Have a document detailing:
    * The roles authorised to access it (e.g. Manager, deputy, admin, maintenance) – ensuring only these roles currently have access,
    * How the password is set and changed, and how the system is used (including exporting footage/photos and blurring/deleting faces and registration numbers).
      1. For more information on completing a Data Processing Impact Assessment refer to MHA’s Data Protection Policy.

Storing and Viewing CCTV images

* + 1. Recorded material must be stored in a way that maintains the integrity and security of the information. This is to ensure that the rights of individuals are protected, and that the information can be used effectively for its intended purpose.
    2. Recording units should be kept in a secure, lockable office/room. The system must be password protected to prevent unauthorised access.
    3. Viewing live images should be restricted to authorised team members where it is necessary for them to see it, for the purpose of crime prevention and safety. Recorded images should also be viewed in a restricted area, such as a designated secure office.

Disclosure

* + 1. Disclosure of information from surveillance systems must be controlled and consistent with the purpose of crime prevention and detection, for which the system was established. It is always acceptable to disclose information to law enforcement agencies once they have provided an official request form, failure to do so, would be likely to prejudice the prevention and detection of crime.
    2. The Data Protection Officer must be notified when CCTV images have been requested by a law enforcement authority and be provided with the requesting email and official request form.
    3. In some limited circumstances it may be appropriate to release information to a third party, where their needs outweigh those of the individuals whose information is recorded. In these circumstances, the Data Protection Officer should be consulted prior to images being released to said third parties.

1. Surveillance Equipment Installed or Provided by individuals or Relatives
   * 1. MHA hopes that no person, relative, representative or colleague will experience reasonable cause for suspicion of harm that requires surveillance evidence to deny or confirm the occurrence of abuse. MHA work in partnership with people to resolve and reassure their concerns.
     2. There is a danger that hidden surveillance undermines appropriate and existing pathways of raising concerns and limits our ability to address those concerns and improve the support provided, since it risks limited dialogue about concerns.
     3. The introduction of covert or overt surveillance, by individuals or their relatives, creates a number of data protection concerns. Most of all, the use of such equipment, particularly in bedrooms, can impact on an individual’s right to privacy and dignity.
     4. Cameras installed by individuals (as opposed to organisations) on their own property for “domestic purposes” i.e., for an individual’s own “personal, family or household affairs” is not a breach of the Data Protection Legislation. But Data Protection Legislation may require them to follow certain rules, see the ICO’s page on [Domestic CCTV Systems](https://ico.org.uk/for-the-public/domestic-cctv-systems/).
     5. The CQC guidance states that if providers discover that relatives have installed hidden cameras, they need to take steps to investigate and understand the concerns that have prompted this. They should also make an assessment of the privacy impact of the cameras before discussing their continued use.

Care Homes – Procedures

* + 1. An individual must make a formal request to install a smart device, which has the capacity to capture audio or visual recordings. Refer to guidance on smart devices in section 6.
    2. A relative cannot request on behalf of a family member. If a person lacks capacity, the request must come from a Lasting Power of Attorney for health and welfare (Mental Capacity Act, 2005), detailing why this would be in the individual’s best interests.
    3. The manager must arrange a meeting accompanied by a note taker to discuss the person’s request, and explore if there is another way to resolution, providing the CQC Guidance information (link in the resources section) to consider - it may be useful to have a copy on display in the foyer.
    4. Should surveillance equipment be discovered in an individual’s bedroom, apartment or communal area, the team must notify the Manager as a matter of urgency.
    5. Managers can decide to turn off surveillance equipment or remove it from an individual’s room, keeping it safe until it can be returned to its owner. However, under no circumstances should this equipment be deliberately damaged or removed with the intention of not returning it. Neither should recordings be deleted.
    6. Consideration should also be given to whether the use of the equipment is intruding on the privacy or rights of others.
    7. The Manager should discuss the equipment with the individual or their relatives, to determine whether they have any cause for concern. Any concerns should be investigated in accordance with MHA’s Complaints Procedures.

Retirement Living - Procedures

* + 1. Tenants and Leaseholders are at liberty to do as they wish in their own environment as long as it doesn’t breach the Data Protection Legislation. However, unless cameras are installed in a secure way, it may be possible for third parties to access images of vulnerable people and misuse the images, potentially rendering the person even more vulnerable. If surveillance is installed, it is the person’s sole responsibility to ensure that the equipment is technologically secure.
    2. If a surveillance device is located in an individual’s apartment where MHA colleagues provide support, the relevant manager must discuss with the individual or their relatives, raise their concerns and review the situation to protect MHA colleagues.
    3. Any concerns raised by individuals, or their relatives should be investigated in accordance with MHA’s Complaints Procedures.

Use of Surveillance Equipment (all services)

* + 1. If smart devices or similar equipment are deemed appropriate the following must be discussed and agreed with the individual or their legal representative:
  + They are responsible for the purchase, installation, and maintenance of the equipment including PAT testing where applicable.
  + There must be an obvious notice informing others that the equipment is in use.
  + They have to comply with relevant legislation, advice from the ICO, and codes of practice.
  + The equipment can only be used for the purpose and time agreed.
  + They may only use the equipment in their room or flat - no intimate care may be filmed or recorded, and no other persons may be filmed or recorded.
  + They are responsible for the security and storage of the equipment which must not jeopardise MHA’s business continuity – i.e., the footage is not for use on social media sites and there must be no risk that others may ‘hack’ into the footage.
    1. If the person still wishes to proceed, the manager will discuss whether permission is to be granted with the area manager.
    2. If the above cannot be guaranteed, permission may be refused. The manager needs to be vigilant that there may be a risk of an attempt to use covert or hidden surveillance - which is not desirable.
    3. Any equipment a person may choose to use, is their property and must be returned to them, it cannot be interfered with or destroyed by MHA staff.

1. Smart Devices (Care Homes)
   1. Smart devices provide many benefits to individuals and their families. It enables them to maintain contact, enhancing an individual’s wellbeing.
   2. Individuals and their families will be supported to use smart devices within their bedrooms. However, the intended use of the device must be discussed with the manager before installing in accordance with the procedures for the use of surveillance equipment (section 5.4)
   3. Any smart device which records or transmits live video images, voice recordings or which automatically answers video calls will be disabled by the team whilst they are providing support or if they are disturbing the individual and causing distress.
   4. Team members will also need to be informed of the intended use of these type of devices, and how they can be turned off or disable during care. Appropriate signage should be displayed to inform people that this type of device is in use.
2. Roles and Responsibilities

| Role | Responsibilities |
| --- | --- |
| **Chief Executive Officer (CEO)** | * Overall responsibility for strategic and operational management, including ensuring that MHA’s policies comply with all legal, statutory, and good practice guidance requirements. |
| **Executive Leadership Team** | * The Executive Leadership Team (ELT) are ultimately responsible for ensuring all team members comply with this policy and understand the need to implement appropriate practices, processes, controls, and training to ensure that compliance with the requirements of the UK GDPR is achieved and maintained. |
| **Managers** | * Effectively and professionally engage with relatives or individuals who request the installation of surveillance equipment. * Comply with all relevant MHA policies and procedures i.e., data protection and complaints. * Escalate concerns and seek advice from senior managers. * Complete the annual Data Protection Audit. * Ensure that their team are aware of the information security policies, procedures, and user obligations applicable to their area of work. * Ensuring colleagues have appropriate training for the systems they are using. * Ensuring that any CCTV image requests are reported to the Data Protection Officer. |
| **MHA Colleagues and Volunteers** | * All colleagues must understand and comply with the procedures within this policy document. * Report any concerns regarding surveillance to their respective manager without delay. |
| **Data Protection Officer (DPO)** | MHA will ensure that there is always one person with overall responsibility for data protection, the DPO.  The DPO will:   * Implement policies and procedures to embed the data protection principles and the rights of Data Subjects. * Ensure data protection training is provided to all colleagues and provide additional guidance and support as required or requested. * Keep records as required by the data protection legislation. * Risk assess each breach/incident and log with the ICO, as necessary. * Inform the Board of breaches or incidents that are reportable to the ICO. |
| **Caldicott Guardian** | The **Senior Nurse Advisor** is the Caldicott Guardian for MHA. The Caldicott Guardian will:   * Work alongside the DPO to make sure that the personal information about people who use MHAs services is used legally, ethically, and appropriately and that confidentiality is maintained in relation to the storage, management and sharing of this information. * Provide leadership and informed guidance on complex matters involving confidentiality and information sharing regarding personal information for MHA’s residents. * Play a key role in ensuring that MHA satisfies the highest practical standards for handling the information of people receiving care and support from MHA. * Apply the eight Caldicott Guardian Principles * Act as the conscience of MHA, providing impartial and independent advice. * Represent and champion information governance requirements and issues at senior management team and board level where appropriate, being and integral part of the overall information governance framework. * Play a key role in advising and ensuring that the Caldicott Principles are applied in digital and paperless systems. |

1. Training and Monitoring
   1. All colleagues must complete the following within three months of commencement of employment and annually thereafter, achieving a “pass” grade:
   * Confidentiality and Information Handling
   * Cyber Security Awareness
   1. Best practice guidance dictates that annual audits should be completed to ensure that the CCTV system is only used in line with this and associated policy documents. Data Protection Annual Audit Form must be completed annually for all services.
   2. Managers and senior colleagues will monitor the application of this policy via audit and observation.
   3. Identified risks, incidents or events relating to the content and procedures within this policy will be monitored through MHA’s Governance framework.
2. Communication and Dissemination
   1. This policy is disseminated and implemented within all MHA services through MHA’s channels of communication.
   2. Each colleague’s line manager must ensure that all teams are aware of their roles, responsibilities.
   3. This policy will be available to the people we support and their representatives in alternate formats, as required.
   4. Queries and issues relating to this policy should be referred to the Standards and Policy Team [policies@mha.org.uk](mailto:policies@mha.org.uk).
3. Equality Impact Assessment (EIA)
   1. MHA aim to design and implement policy documents that meet the diverse needs of our service, population, and workforce, ensuring that none are placed at a disadvantage over others.
   2. It reflects the provisions of the Equality Act 2010 and promotes equal opportunities for all
   3. This document has been assessed to ensure that no one receives less favourable treatment on the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy, and maternity.
4. Resources
   1. MHA policy documents, procedures, and guidance
   * Complaints Policy
   * Consent Policy
   * Data Protection Policy
   * Information Governance Policy
   * Mental Capacity and Deprivation of Liberty Safeguards
   * Whistleblowing Policy
   1. External Resources
   * [Care Quality Commission (CQC) Using cameras or other recording equipment to check somebody's care](https://www.cqc.org.uk/contact-us/report-concern/using-cameras-or-other-recording-equipment-check-somebodys-care)
   * [The Regulation and Inspection of Social Care (Wales) Act 2016 - Statutory Guidance](https://www.gov.wales/sites/default/files/publications/2024-03/guidance-for-care-home-and-domiciliary-suppliers-2024.pdf)
   * [CQC - How we check the use of surveillance](https://www.cqc.org.uk/guidance-providers/all-services/how-we-check-use-surveillance)
   * [ICO Data Protection Impact Assessments](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/)
   * [ICO - CCTV and video surveillance guidance](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/)
   * [The Data Protection Act 2018](https://www.gov.uk/data-protection)
   * [Human Rights Act 1998](https://www.legislation.gov.uk/ukpga/1998/42/contents)
5. Version Control

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Version Date | Revision Description / Summary of Changes | Author and Review Panel | Next Review Date |
| 11 | August 2024 | * Compliance review, transferred to standard policy template * Revised sections to include smart devices. * Procedures updated for surveillance equipment * External resource links updated | Head of Standards & Policy  Data Protection Officer  Head of Quality Improvement    Senior Nurse Advisor  Safeguarding Lead | November 2026 |