Policy Name: **CCTV Surveillance Policy**

Policy Summary…

This policy outlines the guidelines for the use, management, and operation of Closed-Circuit Television (CCTV) systems within Midland Heart.

Midland Heart uses CCTV camera surveillance for the following purposes:

- To enhance the security and safety of residents, staff, and property within Midland Heart's housing estates and offices.
- For the detection and prevention of crime.
- For the detection and prevention of anti-social behaviour (ASB).
- To protect physical assets and Midland Heart properties from damage or misuse.
- To provide support for investigations into incidents or disputes by capturing relevant images.
- To investigate health and safety and breaches of Code of Conduct within communal offices space.

It applies to ….

This policy applies to all staff, residents, visitors, and contractors in respect of CCTV camera surveillance systems installed and operated by Midland Heart within residential buildings, offices, communal areas, and external premises. It describes what CCTV systems may be used for, how they are to be specified, installed, maintained, operated and any associated responsibilities. It also sets out how long images will be securely stored and rights to access recorded data and images.

Our Policy…

Midland Heart is committed to ensuring the safety, security and wellbeing of our residents, staff, visitors, and contractors. As part of this commitment, we use CCTV systems to monitor and protect our facilities, property, and assets, as well as assist in the investigation of incidents within our housing estates. We recognise the importance of respecting individuals' privacy rights by maintaining transparency and regulatory compliance in our monitoring activities.

Policy Principles

- CCTV systems will be used for the purposes outlined in this policy and in compliance with applicable laws and regulations.
- Surveillance will be conducted in a manner that safeguards the privacy and dignity of individuals. This will be achieved by:
    - Access to CCTV footage will be restricted to authorised personnel for legitimate purposes only.
    - Recorded footage will be securely stored, retained, and disposed of in accordance with data protection requirements.
    - Signs will usually be prominently displayed in areas covered by CCTV to inform of its presence, where the situation and circumstances demand it.

Impact Assessments…

Data Protection:

Midland Heart's policies and procedures are developed in line with our Data Protection policy and associated procedures, in order to comply with legal obligations.

Storage and retention of images

- All images will be retained and securely stored in an encrypted format, to prevent unauthorised access for a period of no longer than 31 days from the date of recording. After which, images will be automatically overwritten, unless required for ongoing investigations or legal proceedings. (Schemes with localised independent CCTV systems may have shorter retention periods, which will be dependent on operational equipment's memory capacity).
- In instances where an image is required to be held more than the 31-day retention period, the CCTV Manager will be responsible for authorising such requests. Retention of images will then be reviewed monthly and any not required for evidential purposes, will be permanently deleted.

Requests for copies of images captured on cameras

Internal

Access to CCTV footage is restricted to authorised personnel only. Authorisation for access to CCTV footage will be granted based on job role and necessity, as determined by CCTV Manager.

Right to access

- Requests for access to CCTV footage must be submitted in writing to the Data Protection team. They should include details such as the date, time, and location of the incident or event being investigated, as well as a lawful reason for the request.
- Requests made by individuals for access to footage containing their own personal data must comply with data protection regulations and may require additional verification of identity.

Third parties

- Requests for disclosure of CCTV footage to external parties, such as the police or other authorities with the power to prosecute, for example customs and exercise, or trading standards, can be made.
- Disclosure of CCTV footage to third parties will only be made in accordance with applicable laws and regulations.

Rapid deployment cameras

- Rapid deployment cameras offer a versatile solution for temporary surveillance needs, providing quick and flexible installation in various locations and situations.
- They can be deployed rapidly to monitor specific areas, deter criminal activity, and assist in matters of health and safety. Midland Heart may use rapid deployment cameras to provide temporary security solutions or to assist in its investigations where traditional CCTV systems may be impractical or unavailable.

Body worn video cameras

Body Worn Video Equipment (BWV) is used to reduce risks to personnel and to collect evidence. Midland Heart may use BWV with both audio and visual recording capabilities. Midland Heart employees may request the use of BWV, however, the decision to deploy this equipment rests with line managers.

- All personnel issued with body-worn video cameras will receive training on the proper use, maintenance, and handling of the devices.
- Staff should exercise discretion and judgement when recording sensitive or private information, such as conversations with victims or witnesses, and should respect individuals' privacy rights.
- Where practical, individuals will be informed of the presence of body-worn video cameras and the recording of their interactions with Midland Heart staff.

Fleet vehicle dashcams

Commercial fleet vehicles will contain dashcams and vehicle tracking systems. Dashcams are used to support in retrospective accident investigations, and this is supported with the use of tracking systems that monitor the location of the vehicle and provide useful data leading up to an accident occurring, such as vehicle speeds. Dashcam footage will be used solely for this purpose, and they do not record sound which is disabled. Footage is maintained for up to 48 hours then overridden automatically due to the data capacity of built in SD cards within dashcam devices.

Covert monitoring

Midland Heart will not engage in covert monitoring or covert surveillance (i.e. where individuals are unaware of its occurrence), except under exceptional circumstances. Such instances may arise when there is credible suspicions of criminal activity or serious malpractice or ASB, and following careful consideration, it is determined that no less intrusive methods can address the issue.

Any request for the use of covert monitoring must be approved by the Director of Housing in writing, specifying the scope, duration, justification, and limitations on covert monitoring activities.

Private cameras operated by customers

Midland Heart may permit tenants to install private CCTV systems for personal security providing that they inform Midland Heart of their intention and obtain written consent. Tenants must ensure their systems comply with privacy laws and do not interfere with common areas. Midland Heart is not liable for private CCTV image or audio capture, data storage, maintenance or footage.

The siting, placement, and installation of CCTV cameras

CCTV cameras (including Rapid Deployment Cameras) will be strategically positioned to cover areas where there is a legitimate need for surveillance, such as entrances, exits, car parks, communal spaces, and other vulnerable areas.

- Cameras will not be placed in areas where individuals have a reasonable expectation of privacy such as private property, restrooms, or other sensitive areas.
- They must be clearly visible and identifiable using appropriate signage, advising of the presence of surveillance and the purpose of CCTV monitoring.
- Practical and technical constraints will be taken into consideration such as lighting conditions and line of sight.

- The siting and operation of CCTV camera placement will be monitored to ensure compliance with this policy, relevant laws, and regulations, and to address any concerns or complaints from stakeholders promptly and appropriately.
- The rationale, decision-making process, and outcomes of CCTV camera siting decisions, including any risk assessments, consultations, and mitigation measures implemented will be documented, and records maintained.

Monitoring

Monitoring will require regular oversight, assessment, and enforcement to ensure compliance with established guidelines, legal requirements, and organisational objectives. This will include:

- Scheduled periodic reviews of the CCTV policy to identify any areas for improvement or corrective action.
- Conducting audits of CCTV practices and procedures to verify adherence to the policy's guidelines and protocols.
- Monitor CCTV systems to confirm proper functioning and capability.
- Monitoring access to CCTV footage to ensure authorised access only, establishing incident response protocols for addressing breaches related to CCTV surveillance.
- Providing ongoing training and awareness programs for personnel involved in CCTV operations.

Ensuring we are doing what we say…

Responsibilities

Data Protection Officer	• Compliance with data protection laws and regulations, including conducting Data Privacy Impact Assessments (DPIA), monitoring data processing activities, and providing guidance on data protection issues related to CCTV operations.
CCTV Manager	• Development, implementation, and maintenance of the CCTV policy. • Implementing security measures to protect CCTV data from unauthorised access or disclosure. • Organising and delivering training programs and awareness initiatives related to CCTV operations and data protection requirements. • Developing training materials and resources for CCTV Operators, security personnel, and other relevant staff. • Conducting regular training sessions to ensure personnel are proficient in CCTV monitoring techniques, incident response procedures, and data protection principles. • Raising awareness among staff and tenants about the presence and purpose of CCTV surveillance and their rights regarding their personal data. • Monitoring and ensuring compliance with the CCTV policy, data protection laws, and relevant regulations. • Conducting regular audits and assessments of CCTV operations to identify non-compliance or areas for improvement. • Investigating complaints or incidents related to CCTV surveillance and implementing corrective actions as necessary.
CCTV Operatives	• Monitoring live CCTV feeds, reviewing recorded footage, and identifying security or safety incidents. • Monitoring designated areas for suspicious activities, unauthorised access, or safety hazards. • Reporting incidents to appropriate departments or authorities and following established procedures. • Maintaining accurate records of CCTV monitoring activities, including incident logs and footage archives. • Responding to security incidents identified through CCTV surveillance. • Collaborating with authorities and 3rd party contractors, by monitoring and responding to security threats in real-time. Providing support during incident investigations by retrieving and preserving CCTV footage as evidence.
Supplier - Total	• Technical management and administration of the CCTV system.

Integrated solutions (TIS)	• Installing, configuring, and maintaining CCTV cameras, recording equipment, and associated hardware and software. • Monitoring system performance and troubleshooting technical issues. • Ensuring proper installation and positioning of CCTV cameras to maximize coverage and effectiveness. • Conducting routine inspections and maintenance of CCTV equipment to prevent malfunctions or failures.
Midland Heart employees	• Respecting the privacy rights of others and refraining from actions that may compromise the security or integrity of CCTV operations. • Reporting any concerns or incidents related to CCTV surveillance to CCTV manager or Data Protection Officer in accordance with established procedures. • All staff are responsible for complying with this policy. Any staff found to be abusing images and sound monitoring will be subject to investigation and disciplinary action.

Measures and Reporting

The following key performance indicators (KPIs) will be used to evaluate the effectiveness of this CCTV policy:

- **Privacy Compliance** - Measure compliance with privacy regulations and guidelines governing the use of CCTV surveillance, such as posting signage, and restricting access to recorded footage. Regular audits and assessments can ensure that the CCTV policy aligns with legal requirements and respects individual privacy rights.

- **Data Security** - Evaluate the security measures in place to protect CCTV footage from unauthorised access, tampering, or misuse. This includes encryption, access controls, secure storage, and auditing procedures to safeguard sensitive information and maintain data integrity.

- **Training and Awareness** - Assess the effectiveness of training programs and awareness initiatives aimed at educating personnel and stakeholders about the CCTV policy, procedures, and best practices.

- **Feedback and Satisfaction** – Welcome feedback from employees, residents, visitors, and other stakeholders about their perceptions of the CCTV system's effectiveness, impact on safety and security, and satisfaction with its implementation.

Explaining technical terms…

DPA18	Data Protection Act 2018
CCTV	Closed-Circuit Television
DPO	Data Protection Officer
ICO	Information Commissioner's Office
PIA	Privacy Impact Assessment
BWV	Body Worn Video
RDC	Rapid Deployment Camera
SAR	Subject Access Request
TIS	Midland Heart CCTV supplier
SIA	Security Industry Authority

Related Law & Regulations…

Legislation/Regulation	Relevance to This Policy
General Data Protection Regulation (GDPR)	Lawful basis for processing, transparency, data minimisation, security measures, retention period and individual rights.
Data Protection Act 2018	Data protection principles, lawful basis for processing, rights of data subjects, Data protection Impact Assessments (DPIA's), Data Protection Officer (DPO), security measures and data breach reporting.
Surveillance Cameras Code of Practice for England and Wales	Purpose and justification, Principles of surveillance, legal compliance, Data protection and Privacy, Operational requirements and review and accountability.
ICO guidance on Video Surveillance	Legal compliance, transparency and accountability, purpose limitation, data minimization, individual rights, retention period and security measures.
ICO Guidance on Data protection and employment. Monitoring workers	Legal compliance, lawful basis for processing, transparency and accountability, necessity and proportionality, data minimization, individual rights and retention periods.
ICO Data sharing code of Practice	Lawful basis for sharing, transparency and accountability, data minimization, security measures, data retention and disposal and data sharing agreements.
ICO Individual rights (including SARs)	Access rights, rectification and erasure, restriction of processing, objection to processing, data portability and Subject Access Requests (SARs).