CCTV Policy

Document Control	
Document Title	CCTV Policy
Author	Head of IT, People & Change
Version	1.2
Release Date	March 2025
Next Review Date	March 2028
Document Type	Policy
Approved By	Executive Team

POLICY SUMMARY

Please note that where we use EPIC within this Policy, we refer to EPIC Limited.

This Policy sets out and outlines how EPIC may use and operate Closed Circuit Television (CCTV). The Policy applies to the use of CCTV at EPIC's office in Bentilee.

1. APPLICABILITY

1.1 The Policy applies to all employees of EPIC whether full-time, part-time, permanent, fixed-term or contracted as well as our Board, contractors and members of the public, including tenants who visit our office facilities.

2. INTRODUCTION

2.1 EPIC routinely captures images of people using Closed Circuit Television (CCTV) to provide a safe and secure environment for tenants, colleagues, and visitors, and also to prevent loss or damage to the company's property and to assist in the investigation of accidents, incidents, and near misses. EPIC shall only use CCTV where it is a proportionate and necessary measure to achieve a defined business objective.

2.2 This Policy sets out the accepted use and management of CCTV equipment in line with the Information Commissioner's CCTV Code of Practice to ensure that EPIC complies with data protection legislation.

2.3 We recognise that the images of individuals recorded by CCTV cameras are personal data which must be processed in accordance with data protection legislation. As a data controller, we have registered our use of CCTV with the Information Commissioner's Office (ICO) and seek to comply with its best practice suggestions.

3. CONTEXT

3.1 Closed Circuit Television (CCTV) can be a valuable resource in surveillance and security and is widely used in a range of premises and situations. However, because of the potentially sensitive nature of surveillance, there are codes, guidelines and legislation which must be complied with in order to operate a CCTV scheme legally and fairly.

3.2 The CCTV system in operation at EPIC is owned and operated by EPIC and the deployment is determined by the Executive Team in line with this Policy. The system comprises 11 fixed cameras and has sound-recording capability.

3.3 The CCTV is monitored from the server room located in EPIC's Ubberley Road office and is only accessible by specific members of the IT, People & Change team.

3.4 The introduction of, or changes to, CCTV monitoring will be agreed upon by the Executive Team and shared with staff and contractors.

4. STATEMENT OF INTENT

4.1 EPIC complies with the Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use. The checklist of operation (Appendix 1) is adapted from this document. Further information is available at: CCTV checklist report | ICO

4.2 CCTV warning signs will be clearly and prominently placed at all public entrances to EPIC buildings where CCTV is in operation, including the main staff and reception entrances and exterior walls, as coverage includes outdoor areas. Signs will contain details of the purpose for using CCTV (see Appendix 2).

4.3 The planning and design of the system has endeavoured to minimise any invasion of privacy and ensure that the CCTV will give maximum effectiveness and efficiency, but it is not possible to guarantee that the system will fully meet this brief or detect every single incident taking place in the areas of coverage.

4.4 CCTV data will not be used in any aspect of performance management, unless with the written consent of the employee concerned.

5. SITING THE CAMERAS

5.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed (described in section 2.1) and care will be taken to ensure that reasonable privacy expectations are not violated. EPIC will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act, cameras will be regularly checked to ensure they have not been moved or tampered with in any way.

5.2 EPIC will make every effort to position cameras so that their coverage is restricted to EPIC's office premises, which may include outdoor areas.

5.3 Only suitably competent contractors with the relevant knowledge and experience will be employed to install and maintain the equipment.

6. COVERT MONITORING

6.1 Covert monitoring should not normally be considered, and should only be used in exceptional circumstances, for example:

i) Where there is good cause to suspect that criminal activity or equivalent malpractice may constitute gross misconduct;

ii) Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

6.2 In these circumstances, authorisation must be obtained from the Chief Executive before allowing such an operation to take place. Unless the Chief Executive is instructed otherwise (e.g., in a police investigation), members of the Executive Team will be informed confidentially about any plans for covert monitoring.

6.3 Covert monitoring must cease following the completion of an investigation.

6.4 Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example, toilets.

7. STORAGE AND RETENTION OF CCTV IMAGES

7.1 Recorded data will not be retained for longer than is necessary to meet the purposes of recording them and will be deleted/erased appropriately and in line with approved procedures for EPIC as documented in Appendix 1. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

7.2 All retained data will be stored securely. Access will be limited to named staff only (see Appendix 1) whose access is authorised by the Head of IT, People & Change.

8. ACCESS TO CCTV IMAGES

8.1 Access to recorded images will be restricted to those staff authorised to view them and will not be made more widely available.

8.2 A list of staff authorised to view images from this CCTV system will be held by EPIC.

8.3 A log will be maintained of when CCTV footage is accessed and reviewed (name of reviewer, date & reason).

9. REVIEWING EFFECTIVENESS AND VIABILITY

9.1 Monthly reviews of all CCTV equipment take place to ensure that the system produces clear images that the law enforcement bodies (usually the police) can use to investigate crime and that these can easily be taken from the system when required.

9.2 Quarterly reviews are conducted to ensure that the use of CCTV continues to be the best solution and meets the requirements for which it was implemented.

10. SUBJECT ACCESS REQUESTS (SAR)

10.1 Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act.

10.2 All requests must be made in writing to the Head of IT, People & Change. Individuals submitting requests for access will have to provide sufficient information to enable the footage relating to them to be identified and isolated. For example, date, time, and location.

10.3 EPIC will respond to requests in line with Subject Access Request procedures and timescales.

10.4 At EPIC's discretion, a 'reasonable fee' for the administrative costs of complying with a request may be charged if the request is manifestly unfounded or excessive, or if an individual requests further copies of the images.

10.5 EPIC reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation. Where images of other individuals are on the CCTV footage, their permission will be sought before access is allowed. Where permission cannot be obtained, consideration should be given to hide or blur these individuals.

11. ACCESS TO AND DISCLOSURE OF IMAGES TO THIRD PARTIES

11.1 There will be no disclosure of recorded data to third parties other than authorised personnel such as the police and service providers to EPIC where these would reasonably need access to the data.

11.2 Requests should be made in writing to the Head of IT, People & Change.

11.3 The data may be used within EPIC's disciplinary and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures.

12. COMPLAINTS

12.1 Complaints and enquiries about the operation of CCTV within EPIC should be directed to the Head of IT, People & Change in the first instance.

12.2 Failure of authorised operators/staff to comply with the requirements of this Policy will lead to disciplinary action under EPIC's disciplinary procedure.

13. CCTV INSTALLED BY TENANTS

13.1 Whilst EPIC cannot reasonably withhold permission to allow a tenant to install CCTV at their home, they must be satisfied that the installation will be used for domestic purposes only. Guidance for the use of domestic CCTV is available HERE. The installation will be treated as an alteration to the property and the tenant will not be permitted to carry out the installation without prior written permission from EPIC and must be in accordance with EPIC's policy on alterations.

13.2 EPIC holds no responsibility to oversee or manage video doorbells (e.g., Ring Doorbell) that a tenant has installed themselves unless EPIC has provided/gifted the equipment to the tenant. The owner (e.g., tenant) of the equipment will be classified as the data controller and will retain all responsibility for GDPR compliance and related GDPR issues/concerns.

14. RESPONSIBILITIES

14.1 The roles and responsibilities of key stakeholders across EPIC are detailed below:

EPIC is responsible, as the Data Controller, for the way people's personal data is processed, and for dealing with the ICO as and when required. For clarity, "processing" means capturing, storing, copying, sharing, or deleting CCTV footage.

The Head of IT, People & Change is responsible for ensuring that only those whose role requires to have access to the CCTV systems and are able to produce images from this. They are also responsible for ensuring SAR requests in relation to CCTV are actioned within the relevant timescales.

The Chief Executive is the only person in the organisation who can authorise covert recordings and written authorisation should be obtained from them prior to any action being taken.

The Executive Team are responsible for making decisions in relation to the ongoing effectiveness of current CCTV installations and new installations.

15. BREACHES OF THIS POLICY

15.1 This Policy does not form part of any contract of employment or other contract to provide services, and we may amend it at any time.

15.2 A breach of this Policy may, in appropriate circumstances, be treated as a disciplinary matter. Following an investigation, a breach of this Policy may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

16. TRAINING

16.1 This Policy forms part of the standard induction for all new employees as detailed in Section 1. Applicability, and will be read within the induction period.

16.2 Regular training will be provided to all staff, through EPIC's annual learning and development plan, to ensure awareness of this Policy is maintained at all times.

17. DATA VALIDATION, REVIEW AND MONITORING

17.1 Overall responsibility for the monitoring and effectiveness of this Policy lies with the Head of IT, People & Change.

18. EQUALITY AND DIVERSITY IMPLICATIONS

18.1 An Equality Impact Assessment has been undertaken on this Policy and a copy can be obtained on request.

18.2 In carrying out our services, EPIC are committed to:

- Treating all customers and employees positively regardless of any personal characteristics including gender, age, ethnicity, disability, sexuality, gender reassignment or religion.
- Taking seriously all complaints and investigating and responding accordingly.
- Using plain language and providing information in other formats on request.

19. MONITORING / REVIEW

19.1 This Policy will be reviewed every three years. A review may be conducted earlier if there are significant changes to either legislation or EPIC's operating practices.

20. ASSOCIATED DOCUMENTS

- Data Protection Policy
- Disciplinary Policy

Appendix 1 – Checklist of Operation

EPIC's CCTV system and the images produced by it are controlled in line with our Policy; our Head of IT, People & Change will notify the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the Data Protection Act 1998).

EPIC has considered the need for using CCTV and has decided it is required for the prevention and detection of crime and for protecting the safety of users of the site. It will not be used for other purposes. We conduct a quarterly review of our use of CCTV.

Action	Date	Print & Signed	Review Date
Notification has been submitted to the Information Commissioner and the next renewal date recorded.			
The name of the individual responsible for the operation of the system is: • Elliot Clarke – IT Technician			
The reason for using CCTV has been clearly defined and installation/use of cameras is the best solution.			
The system is checked to verify it produces clear images which the law enforcement bodies (usually the police) can use to investigate crime; these can easily be taken from the system when required.			
Cameras have been sited so that they provide clear images and limit the opportunity to be tampered with.			
The potential impact on individuals' privacy has been identified and taken into account in the use of the system.			
Cameras are located in the following areas: • Outdoors – Reception Door • Outdoors – Front Carpark • Outdoors – Rear Carpark • Outdoors – Shipping Container • Outdoors – Left Side of the building front • Outdoors – Left Side of the building back • Indoors – Reception Doorway • Indoors – Reception Seating • Indoors – Behind reception • Indoors – Interview Room 1 • Indoors – Interview Room 2			

Cameras have been positioned to avoid intentionally capturing the images of persons not visiting the premises.			
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).			
Images from this CCTV system are securely stored, and access is limited to the following authorised persons: • Kelly Heath – Head of IT, People & Change • Elliot Clarke – IT Technician			
Recorded images will be deleted after 30 days unless they form part of an incident under investigation.			
Procedures are in place to respond to the police or individuals making requests for access to data held.			
Regular checks are carried out to ensure that the system is working properly and produces high-quality images.			

Appendix 2 – CCTV Signage

It is a requirement of the Data Protection Act 1998 to notify people entering a CCTV-protected area that the area is monitored by CCTV and that pictures are recorded.

EPIC is to ensure that this requirement is fulfilled.

The CCTV sign should include the following:

- That the area is covered by CCTV surveillance and pictures are recorded
- The purpose of using CCTV
- The name of the organisation
- The contact telephone number and email address of the system's operator
- The signage must include a pictorial image identical to the one shown below

Version Control

Date of Review	Reviewer	Version Number	Changes	Date of Next Review	Approved By
May 2023	HOBSS	1.0	New policy	May 2026	Exec Team
August 2023	HOBSS	1.1	Removal of IT & Change Manager role	May 2026	Exec Team
March 2025	HoIPC	1.2	General review	March 2028	Exec Team