



CLOSE CIRCUIT TELEVISION (CCTV) POLICY

1. INTRODUCTION

The safety and security of our staff, visitors, and premises are of paramount importance. As part of our commitment to maintaining a secure environment, we have implemented a Closed-Circuit Television (CCTV) system in the reception area at Ernest English House. This policy outlines the purpose, scope, and operational guidelines for the use of CCTV, ensuring compliance with the UK General Data Protection Regulation (UK GDPR) and other relevant legislation.

We recognise the importance of balancing security needs with the privacy rights of individuals. Therefore, this policy sets out clear procedures for the management of CCTV footage, including signage, data storage, access, and sharing protocols. It also ensures transparency and accountability in how surveillance is conducted and how data is handled.

2. RESPONSIBILITIES

- The Improving Lives Plymouth Strategy Delivery Group and Trustee Board will adopt and review the implementation of this policy.
- The Chief Executive retains overall responsibility for the implementation and review of this policy.
- Managers are responsible for the implementation of this policy within their project area.
- All staff and volunteers are required to adhere to the policy.
- The Data Protection Officer is responsible for ensuring that all processing of personal data captured by the CCTV system complies with the UK General Data Protection Regulation (UK GDPR). Their responsibilities include:
 1. Ensuring that the lawful basis for processing CCTV footage is clearly defined and documented.
 2. Responding to data subject rights requests, including access, rectification, and erasure of personal data where applicable.
 3. Maintaining records of processing activities related to CCTV, including the Legitimate Interests Assessment (LIA) and Data Protection Impact Assessment (DPIA).
 4. Overseeing compliance with data protection principles, including data minimisation, storage limitation, and security of processing.
 5. Coordinating with the IT Manager and other relevant personnel to ensure technical and organisational measures are in place to protect personal data.
- The IT Manager will oversee the technical implementation and maintenance of the CCTV system. Their responsibilities include:
 1. Ensuring secure configuration of the local hard drive and storage system.
 2. Implementing access controls and encryption where appropriate.
 3. Monitoring system integrity and performing regular audits.
 4. Supporting the Data Protection Officer in responding to data access requests and incidents.

5. Ensuring that the CCTV system remains compliant with UK GDPR and internal security policies.
6. Coordinating with external vendors or suppliers for hardware and software support as needed.

3. PURPOSE

This policy outlines the use of Closed-Circuit Television (CCTV) in the reception area to enhance security, deter crime, and ensure the safety of staff, visitors, and property.

4. AIMS

The aims of this CCTV policy are to:

- Enhance safety and security for staff, visitors, and volunteers by deterring and detecting criminal or anti-social behaviour.
- Protect property and assets belonging to the organisation and individuals within the reception area.
- Support incident investigations by providing visual and audio evidence where appropriate and lawful.
- Ensure compliance with the UK General Data Protection Regulation (UK GDPR) and other relevant legislation governing the use of surveillance systems.
- Promote transparency and accountability in the operation and management of CCTV systems.
- Safeguard individual privacy rights by ensuring that surveillance is proportionate, justified, and subject to appropriate controls.

5. SCOPE

The principles and standards described in this policy apply to all employees, volunteers and students of ILP.

6. LEGAL BASIS

Under Article 6 of the UK GDPR, the lawful basis for processing CCTV footage is legitimate interests specifically, the interest in maintaining a safe and secure environment. A Legitimate Interests Assessment (LIA) and Data Protection Impact Assessment (DPIA) will be conducted and documented prior to installation.

7. SIGNAGE AND TRANSPARENCY

Clear and visible signage will be placed at all entrances to the reception area, stating:

- CCTV is in operation.
- The purpose of surveillance (e.g., security and safety).
- Contact details for further information.

Signs will be readable and positioned before individuals enter the monitored area.

8. DATA STORAGE

Footage will be stored securely on a local hard drive with access restricted to authorised personnel only. Security measures such as password protection and encryption will be implemented. Footage will be retained for a maximum of 30 days, unless required for an ongoing investigation.

9. ACCESS AND SHARING

Individuals may request access to footage in which they appear. Requests must be responded to within one calendar month. **See Annexe 1**

Footage may be shared with law enforcement upon formal request. **See Annexe 2**

Sharing with third parties is prohibited unless legally required and compliant with data protection laws. **See Annexe 3**

10. STAFF TRAINING

All relevant staff will be trained on:

- The purpose and operation of the CCTV system.
- Data protection responsibilities.
- Handling subject access requests.

Policy Review

As part of the normal annual policy review process, the impact of this policy on staff, volunteers and people who use our services has been considered, ensuring its implementation does not discriminate against, or adversely affect anyone. We will ensure equal access to all our policies, including this one. We will assess capability to understand the policy and provide support when it is required.

In applying this policy, Improving Lives Plymouth will have due regard for the need to eliminate unlawful discrimination, promote equality of opportunity, and provide for good relations between people of diverse groups, in particular on the grounds of the following characteristics protected by the Equality Act (2010); age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, and sexual orientation, in addition to offending background, trade union membership, or any other personal characteristic. An Equality Impact Assessment is used for all policies and procedures.

SIGNED:



DATE: February 2026 REVIEW DATE: February 2027

Version Control/Change Log			
Version	Date	Author/s	Changes Made
1.0	January 2026	Lee Sewrey/George Dale/Ann-Marie Woolacott/Chris Burnett	Original Policy Adopted

Annexe 1 Process for Individual Access Requests (Subject Access Requests – SAR)

Purpose

To ensure individuals can access CCTV/recorded footage in which they appear, in compliance with data protection legislation.

Scope

Applies to all requests from individuals seeking copies of footage containing their personal data.

1.Receiving the Request

Requests must be submitted using [ILP's Subject Access Request Form](#) Requests will be automatically logged in the Access Request Register

2.Proof of Identification

To process a Subject Access Request, we must confirm the identity of:

1. The person making the request (the requester).
2. The person whose data is being requested (the data subject).

If they are requesting their own information:

- If we already store their personal email address in our client database, we can accept a photo of their driver's licence (provided we had this email address before their SAR request).
- Alternatively, they will need to visit one of our buildings so we can photocopy their driver's licence.
- If they do not have photo ID, we will require a recent utility bill (dated within the last three months) showing their name and address.

If they are requesting someone else's information:

they must provide proof of identity for both:

Themselves (the requester) – following the same requirements as above.

The data subject – a copy of their photo ID (e.g., driver's licence or passport) or, if unavailable, a recent utility bill with their name and address.

3.Footage Search

- a. IT Manager or Data Protection Officer locate relevant footage.
- b. Footage is reviewed with the requester, where appropriate to:
 - Confirm the individual appears.
 - Identify third parties present.

4.Redaction

Where other individuals appear, footage must be blurred or masked, or stills extracted instead of video.

5.Approval

The IT Manager or Data Protection Officer approve release.

6.Response

- a. Provide footage securely (encrypted link or physical media).
- b. Response must be completed within one calendar month.

7.Record Keeping

A record must be logged including date received, date fulfilled, what was provided and any refusal reason.

Refusal Criteria

Requests may be refused if:

- Disclosure would breach third-party privacy.
- Footage cannot be reasonably located.
- Request is unfounded or excessive.

Annexe 2 Process for Sharing Footage with Law Enforcement

Purpose

To define how footage is shared with police or regulators lawfully and securely.

Scope

Applies to all law enforcement requests.

1.Request Validation

Only accept a written request on official letterhead or email, or a legal order, warrant, court order with crime number reference).

2.Authorisation

Must be approved by the IT Manager and Data Protection Officer or a member of the Senior Manager Team.

3.Footage Extraction

Only extract minimum necessary footage avoiding unrelated or excessive timeframes.

4.Secure Transfer

- a. Use Encrypted USB or secure digital transfer.
- b. Never use personal email or messaging apps.

5.Documentation

Request recorded and held in GDPR records

This will Include Agency name, Officer name and badge number, legal basis and date and footage reference.

6.Retention

Keep a copy of the disclosed footage only if legally required.

Annexe 3 Process for Staff Access to Footage

Purpose

To prevent misuse, unauthorised viewing, or unlawful sharing of recorded footage.

Scope

Applies to all employees, volunteers' tenants and contractors

Access Rules

1. Authorised Roles Only

Access is restricted to:

- IT Manager
- Data Protection Officer.
- Senior Management/Chair of Trustees.

2. Permitted Reasons

Staff may only access footage for:

- Incident investigation.
- Health & safety review.
- Legal compliance.
- Subject access requests.

3. Prohibited Actions

Staff must not:

- View footage out of curiosity.
- Share via phone, social media, or email.
- Record screens or take photos.

4. Access and Logging

Every access must be requested from the IT Manager or Data Protection Officer using [ILP's Subject Access Request Form](#)

5. Training

All authorised users must complete:

- Annual data protection training.
- Adhere to ILP confidentiality policy.

6. Monitoring & Auditing

- Random audits conducted quarterly.
- Breaches treated as disciplinary offences.