



Basketball Ireland CCTV Policy – Updated [March 2025]

1. Introduction

Basketball Ireland (BI) uses Closed Circuit Television (CCTV) systems for **security, safety, and crime prevention** in its facilities. This policy ensures that all CCTV usage complies with the **General Data Protection Regulation (GDPR) (EU) 2016/679** and the **Data Protection Act 2018 (Ireland)**.

2. Purpose of CCTV Usage

The purpose of CCTV within BI facilities is to:

- ✓ Ensure the **safety of players, staff, and visitors**.
- ✓ Prevent and detect **unauthorised access, vandalism, or criminal activity**.
- ✓ Protect BI property and assets.
- ✓ Support the investigation of security incidents.

CCTV will **not** be used for:

- ✗ Monitoring employee performance.
 - ✗ Surveilling private areas such as restrooms or changing rooms.
-

3. Lawful Basis for CCTV Processing

The legal basis for BI's use of CCTV is **Legitimate Interest (Article 6(1)(f) GDPR)**. BI has conducted a **Legitimate Interest Assessment (LIA)** to ensure CCTV use is:

- ✓ Necessary for BI's security and safety objectives.
- ✓ Proportionate to the risks being managed.
- ✓ Balanced against the privacy rights of individuals.

A **Data Protection Impact Assessment (DPIA)** is conducted where cameras may have a **high risk of capturing personal data**.

4. Notification & Signage

- ✓ **Clear, visible signage** is placed at all monitored locations.
- ✓ Signs inform individuals that CCTV is in operation and include:
 - The purpose of CCTV use.
 - BI's contact details for **Subject Access Requests (SARs)**.
 - A reference to where this policy can be accessed.

(See Appendix 1 for Locations of Camera Network).



5. CCTV Footage Storage & Retention

- ✓ CCTV footage is stored securely and retained for a maximum of **30 days** unless required for an investigation.
 - ✓ The **retention period is justified** based on security needs, ensuring footage is available for incident reviews while avoiding excessive data storage.
 - ✓ After **30 days**, footage is permanently deleted unless required for **ongoing investigations or legal proceedings**.
-

6. Access to CCTV Footage

- ✓ **Restricted Access:** Only authorised BI personnel have access to CCTV footage, including:
 - Compliance & Safeguarding Manager.
 - Facility & Security Manager.
 - ✓ Third-party security contractors with access must sign a **Data Processing Agreement (DPA)** ensuring GDPR compliance.
 - ✓ **Access Log:** Any access to CCTV footage is logged, recording:
 - Date & time of access.
 - Name of person accessing.
 - Reason for access.
-

7. Subject Access Requests (SARs)

- Individuals **have the right** to request access to their CCTV footage under GDPR.
- ✓ Requests must be made in writing to **[BI Data Protection Officer Contact]**.
 - ✓ BI will respond within **30 days**, subject to:
 - The request not infringing on **another person's privacy**.
 - The footage still being available (within the **30-day retention period**).
-

8. Data Security & Breach Handling

- ✓ **CCTV data is encrypted and stored in a restricted-access system.**
- ✓ Any **unauthorised access or data breach** will be handled under BI's **Data Breach Response Plan**.
- ✓ If a breach occurs, BI will:
 - Assess the impact.
 - Notify affected individuals **if required by GDPR**.
 - Report to the **Data Protection Commission (DPC) within 72 hours** if significant.

9. Disclosure of CCTV Footage

✓ CCTV footage will only be shared with:

- Law enforcement (e.g., Gardaí) upon formal request.
 - Legal representatives involved in **ongoing legal cases**.
 - ✓ Requests from external parties **must be legally justified** and approved by BI's **Compliance Officer & Data Protection Officer**.
-

10. Governance & Policy Review

✓ This policy is reviewed **annually** by BI's **Data Protection Officer & Compliance Team**.

✓ Updates will be made in response to:

- **Changes in GDPR or Irish Data Protection Law**.
 - **New security risks** identified in BI facilities.
-

11. Contact Information

For any questions about this policy or to submit a **Subject Access Request (SAR)**, please contact:

✉ **BI Compliance Manager** – rwall@ireland.basketball

☎ **BI Office** - **+353 (1) 459 0211**

Summary of Key Updates in This Version:

- ✓ **Updated GDPR Compliance** – Now explicitly references the **Data Protection Act 2018 & GDPR**.
 - ✓ **Justification for CCTV Use** – Confirms BI has conducted a **Legitimate Interest Assessment (LIA)**.
 - ✓ **Detailed Retention & Access Logs** – Introduces a **30-day storage policy with an access log requirement**.
 - ✓ **Stronger Data Breach Procedures** – Aligns with BI's **Data Breach Response Plan**.
 - ✓ **Governance & Annual Review Commitment** – Ensures the policy evolves with data protection laws.
-

Final Assessment:

- ✓ This updated policy ensures **full GDPR compliance** and **clarity on access, retention, and disclosure**.
- ✓ It **strengthens BI's legal position** by justifying CCTV use with **LIA and security risk assessments**.
- ✓ **Clearer processes for SARs, security breaches, and policy reviews** improve governance.



Appendix 1: The CCTV network for BI is located in the following areas:

External:

- Front x 3 (Main entrance)
- Rear of building x 2 (Car park)
- Left Side of building
- Right Side of building

Internal Ground Floor:

- Reception
- Shop
- Rear Hallway
- Main Hallway

Basketball Arena:

- Left Front
- Right Front

Internal Upper Floor:

- Hospitality
- Lobby
- Main Office

There are 16 cameras in total. 5 are external, while 9 are internally placed. Cameras will be positioned so that they cannot capture non-relevant images in their vicinity (for example neighbouring private property, or passers-by).