Byram House

CCTV AND SECURITY POLICY

Date: May 2026

CCTV AND SECURITY POLICY

Contents

1. Introduction to the Policy

This policy sets out the framework, principles, and procedures that **Byram House** follows regarding the use of CCTV and other security monitoring systems (including door chimes) to protect children, staff, visitors, and property. The policy applies to all staff, agency workers, volunteers, and contractors working at Byram House, whether at 62 Deighton Road, 66 Deighton Road, or elsewhere.

The Home is Byram House, which comprises the two residences at 62 Deighton Road and 66 Deighton Road. This policy applies equally across both residences.

Current position: Byram House **does not currently use** any CCTV cameras in or around the property. A location-specific risk assessment has not provided evidence that CCTV is needed at this time. However, this position is reviewed regularly, and this policy sets out the detailed procedures that will be followed **should CCTV be implemented in the future**. The policy also covers **door chimes** currently in use on main exits.

The objectives of this policy are to:

- Comply with all relevant legislation, including the **Data Protection Act 2018**, the **UK General Data Protection Regulation (UK GDPR)**, the **Protection of Freedoms Act 2012** (Part 2 – Codes of Practice for Surveillance Cameras), and the **Human Rights Act 1998** (Article 8 – right to private life).
- Ensure that any future use of CCTV is justified, proportionate, and transparent, with appropriate safeguards for privacy.
- Provide clear guidance on system management, data retention (maximum 30 days), sharing of images, subject access requests, and complaints.
- Ensure that door chimes (currently in use) are managed appropriately as a security measure.

The home will treat all CCTV images and related data as **data protected** under the Data Protection Act 2018 and UK GDPR.

2. How this Policy Benefits the Home

This CCTV and Security Policy benefits Byram House in the following ways:

- **Legal Compliance** – It ensures that if CCTV is installed, the home will comply with the **Data Protection Act 2018**, **UK GDPR**, the **Protection of Freedoms Act 2012** (surveillance camera code of practice), and **ICO guidance** on CCTV. It also addresses the lawful basis for processing, transparency, data minimisation, and retention.
- **Privacy Protection** – It mandates that any CCTV system will be designed to avoid intrusion into adjacent private property and will only cover areas justified by risk assessment. Children, staff, and visitors will be informed through signage.
- **Risk-Based Approach** – It requires a full checklist and risk assessment before installation, reviewed annually. The current decision not to use CCTV is based on a risk assessment, and this will be kept under review.
- **Data Security** – It sets out strict access controls (only identified staff), daily efficiency checks, logging of access, secure storage of evidential downloads (sealed, witnessed, signed), and automatic deletion after 30 days.
- **Accountability** – It establishes a System Administrator, access logs, and a clear procedure for releasing images to police or other authorities (only where lawful, with recorded justification).
- **Subject Access Rights** – It informs data subjects of their right to request copies of their own CCTV images and the process for doing so.
- **Door Chimes** – It clarifies the purpose of door chimes (monitor activity, deter unwanted visitors) as a current security measure distinct from CCTV.
- **Inspection Readiness** – The **Social Care Common Inspection Framework (SCCIF) 2026** expects appropriate security and privacy practices. This policy demonstrates the home's commitment.

3. Definitions & Legislation

3.1 Definitions

Term	Definition
Home	Byram House, the children's home registered with Ofsted, comprising two residences at 62 Deighton Road and 66 Deighton Road.
Company	IMS Care LTD, the registered provider and legal entity responsible for operating Byram House.
Byram House	The name used throughout this policy to refer to the home and its staff.
CCTV	Closed-circuit television – a system of cameras used to monitor activities for security or safety purposes.
Data Controller	The entity that determines the purposes and means of processing personal data (Byram House / IMS Care LTD).
Data Processor	A person or organisation that processes data on behalf of the data controller (e.g., a CCTV maintenance contractor).
Personal Data	Any information relating to an identified or identifiable living individual (e.g., a recorded image of a person).
Lawful Basis	A legal reason for processing personal data under UK GDPR (e.g., legitimate interests, legal obligation, public task).
System Administrator	The designated staff member(s) responsible for day-to-day management of the CCTV system.

Door Chime	An audible alert (often a bell or electronic tone) triggered when a door is opened, used to monitor entry/exit. Not a recording device.
Retention Period	The length of time CCTV images are kept before automatic deletion (30 days for Byram House).
Subject Access Request (SAR)	A request by an individual for access to their personal data (including CCTV images).

3.2 Key Legislation and Statutory Guidance

Legislation / Guidance	Key Provisions	Relevance to this Policy
Data Protection Act 2018 (DPA 2018)	Implements the UK GDPR. Sets out data protection principles (lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality).	CCTV images are personal data. The home must comply with all principles when processing them.
UK General Data Protection Regulation (UK GDPR)	Requires a lawful basis for processing (Article 6). For special category data (e.g., health information captured unintentionally), Article 9 conditions apply.	The home's lawful basis for CCTV is likely **legitimate interests** (Article 6(1)(f)) – the need to protect children, staff, and property.
Protection of Freedoms Act 2012 (Part 2)	Requires surveillance camera systems to comply with a statutory code of practice (prepared by the Surveillance Camera	The home must ensure any CCTV system complies with the 12 guiding principles (e.g., use only where

	Commissioner). The code includes the "surveillance camera principles".	necessary, transparent, effective, accountable).
Surveillance Camera Code of Practice (Home Office, 2013, updated 2022)	Provides detailed guidance on the use of CCTV by local authorities and other relevant authorities. While not legally binding on private children's homes, it represents best practice.	Byram House will adopt the principles as best practice: proportionate, transparent, accountable, with clear retention and access policies.
Human Rights Act 1998	Article 8 – right to respect for private and family life, home, and correspondence. Any interference must be lawful, necessary, and proportionate.	CCTV that intrudes on private spaces (e.g., bedrooms, bathrooms) would breach Article 8. The home will not install cameras in such areas.
Children's Homes (England) Regulations 2015	Regulation 12 – Statement of Purpose; Regulation 34 – policies for protection of children; Quality Standards.	The home must have policies for safety and privacy. This policy supports that.
Social Care Common Inspection Framework (SCCIF) for Children's Homes 2026	Effective 1 April 2026. Focuses on children's lived experience and privacy.	Inspectors will evaluate whether any surveillance respects children's dignity and privacy.
Working Together to Safeguard Children 2026	Safeguarding includes protecting children from harm; appropriate monitoring may be justified.	Where CCTV is used for safeguarding (e.g., to prevent absconding), it must be proportionate and risk-assessed.

4. The Policy

4.1 Statement of Intent

Byram House will treat any CCTV system and all information, documents, and recordings as **data protected** under the Data Protection Act 2018 and UK GDPR.

The purposes of any future CCTV system are:

- To protect children, staff, and visitors.
- To increase personal safety and reduce the fear of crime.
- To protect buildings and assets.
- To protect the personal property of children, staff, and visitors (without prejudice).
- To support the police in preventing and detecting crime.
- To assist in identifying, apprehending, and prosecuting offenders.
- To assist in managing the premises (including grounds).
- For medical needs of children (e.g., monitoring for seizures where specifically risk-assessed and agreed in a care plan).

The system will be designed to **deny observation of adjacent private property**. Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

Transparency: All children, adults, and visitors will be informed (by clear signage at entrances) if any CCTV is installed and operating. The home will also explain the purpose, lawful basis, and retention period in a privacy notice.

4.2 Current Position (No CCTV) and Review Process

- **As of the date of this policy (March 2026), Byram House does not operate any CCTV cameras** in or around 62 or 66 Deighton Road.
- This decision is based on a **location-specific risk assessment** that did not identify evidence of need.
- The Registered Manager will **review the risk assessment annually**, or sooner if:
    - There is a serious incident (e.g., break-in, assault, missing child) that might justify CCTV.
    - A child with specific vulnerabilities (e.g., frequent absconding, high risk of exploitation) is admitted, and CCTV is considered as a safeguarding measure.
    - There are changes to the physical environment or local crime rates.
- If the risk assessment determines that CCTV is justified, the home will follow the procedures in sections 4.3–4.9 before any installation, including completing a **CCTV checklist and Data Protection Impact Assessment (DPIA)** .

4.3 Justification for CCTV (if installed in the future)

Before installing any CCTV system, the Registered Manager will:

1. **Complete a CCTV checklist and risk assessment** (template available from the ICO or internal documents). This will consider:
    - The specific problem or risk to be addressed.
    - Whether CCTV is proportionate and the least intrusive means.
    - Alternative measures (e.g., improved lighting, door chimes, increased staffing) considered and rejected.
    - The areas to be covered (excluding private spaces like bedrooms, bathrooms, and any area where children would reasonably expect privacy).
2. **Conduct a Data Protection Impact Assessment (DPIA)** where the processing is likely to result in a high risk to individuals (e.g., covering areas where children spend significant time). The DPIA will be reviewed by the Responsible Individual.
3. **Consult with staff, children, and placing authorities** (where appropriate) before installation.

4. **Display clear signage** at all entrances and within the area covered, explaining:
    - The purpose of CCTV.
    - The data controller (Byram House / IMS Care LTD).
    - The lawful basis (legitimate interests).
    - Contact details for enquiries (Registered Manager).
    - Retention period (30 days).
    - Right to access images (Subject Access Request).

The checklist and risk assessment will be re-visited **annually** to ensure the ongoing appropriateness of the system.

4.4 System Management (Administrator, Daily Checks, Access Logs)

System Administrator: The Registered Manager (or a deputy nominated by them) will act as the System Administrator.

Operational control:

- The CCTV system will be in constant operation (24/7) if installed.
- Management day-to-day will be by the service locally, acting in accordance with this policy.
- Access to the system (viewing images, downloading) is restricted to **identified members of staff** whose roles require it (e.g., Registered Manager, Deputy, Responsible Individual). A list of authorised staff will be kept.

Daily checks: The home will check daily:

- That the equipment is properly recording (e.g., time/date stamp correct).
- That all cameras are functional (no obstructions, no damage).
- That the hard drive is recording and not full.

Access log: Details of any system access (viewing, downloading, deleting) will be recorded in the home's log book, including:

- Date and time of access.
- Name of person accessing.
- Purpose of access (e.g., “investigating missing child incident”, “responding to police request”).
- What was viewed or downloaded.

4.5 Data Retention and Destruction

- All CCTV data will be stored for a **maximum of 30 days**, after which it will be **automatically deleted / overwritten** (unless required for an ongoing investigation or evidential purposes).
- Where images are required for an investigation (e.g., police request, safeguarding enquiry), they will be downloaded and stored as per section 4.7 (Image Downloading Procedure). The retained copy will be kept only for as long as necessary for the legal purpose.
- The home will not retain images beyond 30 days for routine monitoring.

4.6 Sharing CCTV Images (Lawful Disclosure)

The home does not share CCTV images with any third party without **lawful authority** or the **consent of the data subject** (unless consent is not required by law).

Disclosure may be made without consent where:

- It is required by law (e.g., court order, statutory duty).
- It is necessary for the prevention or detection of serious crime (shared with police).
- It is necessary for safeguarding a child (shared with local authority, safeguarding partners, Ofsted).
- It is necessary for the prevention or detection of a health and safety risk.

Recipients may include:

- Police forces, courts, tribunals.
- Local authorities (children's services, safeguarding teams).
- Regulatory bodies (Ofsted, CQC).
- Health authorities (where images show a medical emergency).
- Professional legal advisors (where the home is involved in legal proceedings).

All disclosures must be:

- Recorded in the access log.
- Justified in writing (lawful basis and necessity).
- Limited to the minimum necessary (e.g., blurring non-relevant individuals where possible).

The home will not share images with the media, commercial organisations, or the general public.

4.7 Image Downloading Procedure (Evidential Integrity)

Where images are required as evidence (e.g., for police investigation, court proceedings), the following procedure will be followed to preserve evidential integrity:

1. **Prepare download media** (e.g., USB stick, external hard drive) – each media must be identified by a unique mark (e.g., numbered label).
2. **Clean the media** of any previous recordings (format or erase).
3. **Download the relevant images** by an authorised person (System Administrator).
4. **Seal the media** in an evidence bag (or sealed envelope). The seal must be witnessed by a second authorised staff member.
5. Both witnesses sign and date the seal. The bag is labelled with:
    - The date and time of download.
    - The unique mark of the media.
    - The location and camera number.

    - The name of the person who downloaded.
6. **Store the sealed bag** in a separate **secure evidence store** (e.g., locked cabinet, safe) accessible only to the Registered Manager and Responsible Individual.
7. **Record the release** of the download media to the police or other authorised recipient in the access log. The recipient signs for receipt.

Viewing by police without downloading: If police wish to view images on site (without taking a copy), this must be recorded in writing, including the officers' names, badge numbers, time, and purpose.

Court production: When a court requires a downloaded media, it will be produced from the secure evidence store, complete in its sealed bag. The chain of custody must be documented.

4.8 Data Subject Access Requests (SARs)

Under the Data Protection Act 2018 and UK GDPR, individuals have the right to access their own personal data, including CCTV images.

Procedure for handling SARs:

- A request may be made verbally or in writing to the Registered Manager.
- The home will respond **within one month** (30 calendar days) of receipt.
- To protect privacy, the home may require proof of identity before releasing images.
- Images will be provided in a commonly used electronic format (e.g., video file, still image).
- If the images contain data about other identifiable individuals, the home will **redact** (blur) those individuals' faces before release, unless the other individuals consent.
- Requests that are manifestly unfounded or excessive may be refused or charged a reasonable fee (the home will follow ICO guidance).

Fees: For subsequent copies of the same data, a reasonable fee may be charged (currently up to £10 for CCTV stills). The home will inform the requester in advance.

4.9 Complaints and Monitoring

- **Performance monitoring** – Random operating checks (including compliance with this policy) may be carried out by the Responsible Individual or external auditor.
- Any **complaint** in relation to the CCTV system (or alleged misuse) should be addressed to the Registered Manager in the first instance. If unresolved, it may be escalated to the Responsible Individual or the Information Commissioner's Office (ICO).
- The home will investigate all complaints promptly (within 10 working days) and respond in writing.

4.10 Door Chimes (Current Security Measure)

- **Door chimes** are located on the main exits of the home (both 62 and 66 Deighton Road) and are currently operational.
- The main purpose of door chimes is to **monitor activity** coming into and leaving the home and to act as a **deterrent to unwanted visitors**.
- Door chimes are **not recording devices** – they do not capture, store, or share images or audio recordings. They simply produce an audible alert when a door is opened.
- Staff are trained to respond to the chime (e.g., check who is entering/exiting, ensure children are safe).
- Door chimes are not considered high-risk under data protection law. However, the home will ensure that they are not used in a way that intrudes on privacy (e.g., chimes in bathrooms are not installed).
- The home will review the continued use of door chimes as part of the annual risk assessment (section 4.2).

5. How the Home Trains its Staff About this Policy

Byram House provides structured training to ensure all staff understand and can implement this CCTV and Security Policy effectively.

Training Element	Frequency	Method / Content
Induction	Upon appointment	Face-to-face training covering: current policy (no CCTV currently), legal framework (DPA 2018, UK GDPR, Protection of Freedoms Act), lawful basis for CCTV (legitimate interests), privacy and signage requirements, retention (30 days), access controls, door chimes, subject access requests, and the dual-site operation (62 & 66 Deighton Road).
Annual refresher	Every 12 months	Classroom or virtual session covering updates to legislation (ICO guidance, SCCIF 2026), any changes in the home's CCTV status (if installed), and refresher on lawful disclosure.
System Administrator training	For designated senior staff (if CCTV installed)	Specific training on daily checks, access logging, downloading procedures (evidential integrity), handling police requests, and SARs.
Data protection and SARs	At induction and biennially	Training on handling subject access requests, redaction techniques, and ICO reporting obligations.
Door chime operation	At induction	Practical training on responding to door chimes, recording unusual activity, and maintenance checks.

Staff are required to:

- Read and sign this policy annually.
- Complete all mandatory training.
- Never attempt to install, modify, or download from a CCTV system unless authorised.
- Report any suspected misuse of CCTV or door chimes to the Registered Manager immediately.

6. Related Policies and Guidance

This policy must be read in conjunction with:

- Data Protection Policy (including privacy notices)
- Safeguarding Policy
- Health and Safety Policy
- Whistleblowing Policy
- Complaints Policy
- Children's Homes (England) Regulations 2015
- Working Together to Safeguard Children 2026
- Social Care Common Inspection Framework (SCCIF) for Children's Homes 2026
- ICO guidance: "In the picture: A data protection code of practice for surveillance cameras and personal information"
- Protection of Freedoms Act 2012 (Part 2) – Surveillance Camera Code of Practice

7. Policy Approval and Review Details

Byram House

Policy Name	CCTV AND SECURITY POLICY	
Home	Byram House	
Reviewed by	Danyaal Iqbal / Mustafa Amin	Deputy Manager / Registered Manager
Approved by	Stacey Wagstaffe	Responsible Individual
Date	May 2026	