CCTV and Monitoring Policy

Policy Sponsor	Senior Information Risk Owner
Policy Owner	Data Protection Officer
Date Approved	31 August 2025
Date for review	31 August 2028
Distribution	Unrestricted; Internal and External Use
Date EIA completed	July 2025

1. Purpose

The purpose of this policy is to outline Barnardo's position on the use of CCTV, video recording and other monitoring activities across the Charity. Barnardo's is committed to the effective and conscientious use of recording and monitoring devices to deliver excellent services and protect its colleagues, service-users and property.

Why does this policy matter?

- Barnardo's has legal obligations regarding responsibly capturing images, video and audio of individuals. The UK's data protection regulator, the ICO, can impose fines and other sanctions on Barnardo's if it fails to comply with its legal obligations for recorded monitoring
- Barnardo's values its colleagues, supporters and service-users and needs to ensure that these individuals, and their personal data, are safe. To do this, it is important for Barnardo's to ensure that data gathered by monitoring devices is regulated effectively.

2. Scope

This policy covers all matters relating to the use of monitoring devices for the purposes of improving our services to vulnerable children and for organisational effectiveness, as well as improving the safety of Barnardo's colleagues, premises and service-users.

Monitoring devices constitute any devices that capture live or stored audio, images or video data. Examples of this include, but are not limited to:

- CCTV on Barnardo's premises
- Recording used during counselling sessions at a therapeutic intervention
- Supporter relations calls that are recorded for training, monitoring and auditing purposes
- Smart doorbells and entry systems
- A recorded video conference or meeting
- TV recording for publicity purposes
- The use of movement detectors and auditory devices
- Internal monitoring devices
- AI notetaking and transcription tools

The policy covers the justifications for using monitoring devices, and installing equipment conscientiously, mitigating the intrusiveness of monitoring equipment, securely storing data, sharing captured images, video or audio, inspecting installed monitoring devices, and deleting data responsibly. Adherence to this policy should be considered in conjunction with Barnardo's other statutory and regulatory requirements.

3. Policy

It is crucial that any use of recorded monitoring across Barnardo's justifies the capturing of individuals' personal data and is a proportionate response to the issue. Barnardo's considers it justified to use recorded monitoring if, and only if, it meets at least one of the following criteria:

- The improvement of security to Barnardo's premises and property
- Aiding in preventing, detecting or prosecuting criminal acts
- Greatly improving the welfare or safety of Barnardo's service-users and staff
- Visitor screening
- Assisting in the resolution of disputes which arise during disciplinary or grievance proceedings
- Aiding the defence of any civil litigation, including employment tribunal proceedings
- The improvement of the personal safety of colleagues, visitors and other members of the public and to act as a deterrent against crime
- Improvement to the effectiveness and efficiency of day-to-day operations
- Archiving and preservation of meetings and discussions

If one of these criteria are met, then the installation of recorded monitoring needs to still be shown to be a proportional response to a perceived risk. It will be the responsibility of any colleague considering the use of recorded monitoring to ensure that other less-intrusive attempts that don't require monitoring have been made to resolve the problem, where appropriate.

Example: Installing additional lighting in a car park that has had numerous thefts may result in the same outcome as costly and intrusive CCTV devices.

Barnardo's carefully assesses the intrusiveness of monitoring devices and will not approve their use where they pose an undue risk to individual privacy. This includes any form of surveillance involving children or young people in foster placements, as well as the installation of cameras in private or sensitive areas such as toilets, changing rooms, and spaces designated for prayer or reflection.

Call and meeting recording or transcription

Barnardo's regularly records telephone conversations, meetings and uses AI notetaking and transcription tools with supporters, colleagues, volunteers and members of the public. The calls are used to keep a record of customer needs, and additionally for training, monitoring, work efficiency, future reference and auditing purposes. Due to the sensitive nature of these calls and meetings, Barnardo's retains this data in line with its retention schedules. Additionally, calls are securely stored via protected software and are accessed on a need-to-know basis. Calls outside the scope of supporter relations and marketing services should not be recorded without prior consent from all parties involved. When recording meetings, notice of the recording will be provided at the start of the meeting. Speakers and attendees should be informed of how recordings will be stored, used, or shared.

Installation

During the installation of monitoring devices, colleagues should consider how the intrusiveness of devices can be mitigated as effectively as possible, for example, continuous and real time recording should be avoided where appropriate and cameras placed to avoid irrelevant recordings of the public. All devices that have been installed by Barnardo's for the purposes of monitoring should be explicitly labelled with clear signage on the premises or done orally in some circumstances. Signage should include basic details such as Barnardo's logo, website, telephone number, and an email contact. Where monitoring devices are used the subject must be informed or their parent/carer if they don't have the capacity to understand.

All monitoring devices that retain audio or visual data should be capable of storing and transferring information onto Barnardo's electronic systems securely. Barnardo's ensures that all data captured in this way can be easily transferred to third parties, who would have the authority to act upon it.

Responsibility for monitoring and securing the data captured by Barnardo's monitoring devices is always clearly identified. Responsible individuals ensure that viewing areas are appropriately secure and can only be accessed by a limited number of colleagues on a need to see or hear basis. Data should be encrypted and password protected.

Sharing data with third parties

There are cases when data from the monitoring devices will need to be shared with a third party.

Data may only be disclosed to third parties for specific reasons:

- **Police investigations**
- **Safeguarding concerns**
- **Purposes for which the recording device was originally installed**

Any sharing of such data must have the appropriate level of approval and comply with Barnardo's Policy on Information Sharing.

Requests from individuals (DSARs):
If someone makes a request to access monitoring footage in which they appear (a Data Subject Access Request), Barnardo's will consider the request in line with data protection law. CCTV recordings are personal data when an individual can be identified.

If the footage also shows other people and it is not possible to blur or redact their identities (which is often the case), consideration should be given to whether it is appropriate to seek consent from those individuals before sharing. If consent cannot be obtained, or if redaction is not possible, we may instead offer the requester an opportunity to view the footage in person rather than receive a copy.

If neither option is suitable, we will assess whether a legal exemption applies, for example, if sharing the footage would inappropriately reveal personal information about someone else. Each request will be carefully reviewed on a case-by-case basis, balancing the requester's rights with the rights and privacy of others.

Third Party Monitoring

Where monitoring devices are operated by third parties (e.g., landlords or foster carers), a formal assessment must be carried out to determine appropriate arrangements for data usage, secure storage, and timely deletion. This assessment should ensure compliance with relevant data protection legislation and align with Barnardo's standards on privacy and safeguarding.

Retention and deletion

Barnardo's retains and disposes of CCTV and monitoring data in accordance with its Records Management, Retention and Disposal Policy - Inside Barnardo's and Retention schedule.

Covert monitoring

Barnardo's should not engage in covert monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or extremely serious malpractice (eg, gross misconduct or practices that jeopardise the safety of others) is taking place and, after suitable consideration, Barnardo's reasonably believe there is no less intrusive way to tackle the issue.

Where the use of covert monitoring is justified, it will only be carried out with the express authorisation of the Head of Retail Operations. Prior to engaging in covert monitoring, Barnardo's will conduct a Privacy Impact Assessment. The Privacy Impact Assessment will consider the nature of the problem that Barnardo's is trying to address at that time and whether the covert monitoring is likely to be an effective solution, or whether a better solution exists. The decision to carry out covert monitoring will be fully documented and will set out how the decision to use covert monitoring was reached and by whom. The risk of intrusion on innocent workers will always be a primary consideration in reaching any such decision.

Access to, and the disclosure of, covert monitoring recordings will be limited to authorised individuals only. Where covert monitoring takes place, it will only be carried out for a limited period

(up to a maximum of 2 weeks) that is consistent with the objectives of making the recording and will only relate to the specific suspected criminal or unauthorised activity.

Barnardo's uses an external vendor to undertake covert monitoring on its behalf. This vendor meets the security, due diligence and safeguarding criteria outlined in Barnardo's vendor risk assessment.

4. Definitions and Key Concepts

Closed-Circuit Television (CCTV) - A system of video cameras used to monitor and record activity in specific areas. Unlike broadcast television, CCTV signals are not openly transmitted but are restricted to authorised users

Smart Monitoring Devices - Devices connected to the internet, such as baby monitors, nanny cams, or home security systems. Often used in private settings, they may still collect personal data subject to data protection rules when used in work-related or shared environments.

Meeting Recording - refers to the practice of capturing audio and/or video of a meeting. This allows participants to review the discussion later, ensures accurate documentation, and can be useful for those who couldn't attend the meeting in real-time.

Video Doorbell (Smart Doorbell) - A doorbell equipped with a camera and microphone that can stream video to a smartphone or device. It records people approaching or ringing the door and may capture images/audio from public areas.

Audio Recording - Some monitoring devices capture not only video but also sound. Audio is considered more intrusive under data protection law and may require additional justification and safeguards.

Live Streaming - Broadcasting video/audio in real-time over the internet or an internal system. This poses heightened data protection and safeguarding risks if not properly secured.

Covert Surveillance - Recording individuals without their knowledge. This is only permitted in rare, exceptional circumstances (e.g. serious crime or safeguarding risk) and requires senior authorisation and legal oversight.

Geo-Location Tracking - Some monitoring devices (e.g. in vehicles or phones) may track an individual's location. This counts as personal data and must be handled carefully.

Transcription - is the process of converting spoken language into written text.

Redaction - The process of obscuring or removing personal data from footage before disclosure, e.g. blurring faces or masking audio.

5. Roles and Responsibilities

Roles	Responsibilities
Trustees	• Provide strategic oversight to ensure surveillance practices align with Barnardo's values, safeguarding commitments, and legal duties. • Endorse policies and ensure appropriate governance arrangements are in place. • Seek assurance that privacy and data protection risks are being effectively managed.
Policy Sponsor/Senior Information Risk Owner	• Act as the executive owner of this policy and champion for information risk management across Barnardo's. • Provide strategic leadership on the use of surveillance and monitoring technologies. • Ensure risks associated with the use of CCTV and monitoring devices are properly assessed, recorded, and mitigated.
Head of Information Governance and Data Protection Officer	• Provide expert advice on data protection, DPIAs, and the lawful use of monitoring technologies. • Approve or advise on high-risk uses of monitoring devices. • Oversee and support responses to Data Subject Access Requests (DSARs) and complaints involving recorded data. • Receive and act on reports of serious incidents or policy breaches involving recorded data. • Monitor compliance with this policy and escalate risks to the SIRO or senior leadership as needed. • Keep this policy under review and aligned with legal requirements and best practice.
All Managers	• Ensure this policy is implemented within their service or team. • Complete or oversee Data Protection Impact Assessments (DPIAs) before any new monitoring devices are introduced. • Make sure signage, privacy notices, and retention arrangements are in place.

	• Ensure colleagues and volunteers are trained and understand their responsibilities. • Report any risks, concerns, or incidents to the Information Governance team.
All trustees, colleagues and volunteers	• Follow this policy and relevant procedures when using or accessing CCTV or other monitoring devices. • Report any suspected misuse, data breach, or concern related to monitoring systems. • Do not use personal or unauthorised devices to record individuals without prior approval. • Always respect the privacy and dignity of individuals.
DDaT, Facilities Management/Properties Team	• Ensure technical controls are in place to support secure installation, access, and storage of recorded data. • Support procurement, installation, and maintenance of authorised CCTV systems. • Assist in enforcing data retention periods and access restrictions. • Work with Information Governance to ensure systems are compliant by design.

6. Associated Legislation, Guidance, References and Documents

All monitoring and surveillance activities must comply with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Human Rights Act 1998 (Article 8 – right to private and family life)
- Protection of Freedoms Act 2012 (Part 2 – for CCTV use in public places)
- Guidance on the use of domestic CCTV – GOV.UK (www.gov.uk)
- Domestic CCTV systems – guidance for people using CCTV | ICO
- Family Placement Surveillance & Monitoring Device Procedure and Guidance

7. Compliance and Oversight

In addition to the compliance and oversight arrangements set out under Roles and Responsibilities, the following applies:

- The Policy Owner will ensure that management information demonstrated adherence to and compliance with this policy is produced and provided to relevant parties as required.
- Departments and services where monitoring and surveillance devices exist will ensure local procedures are in place to demonstrate compliance with this policy.
- The Audit and Assurance team will periodically and independently review adherence to and compliance with this policy and associated procedures and processes across the Charity in line with their approved audit and inspection plans.

8. Equality Impact Statement

Barnardo's is committed to ensuring that the use of CCTV and monitoring technologies upholds the principles of equality, diversity, and inclusion. This policy has been assessed for its impact on individuals with protected characteristics under the Equality Act 2010. Monitoring practices are designed to be proportionate, non-discriminatory, and sensitive to the needs of vulnerable groups, including children and young people. Surveillance will not be used in private or sensitive areas, and all monitoring activities will be subject to assessment and regular review to ensure they do not inadvertently disadvantage or exclude any group.

9. Version History

Document History	Date	Author	Comments	Approval
1	25/03/19	Martine King	Awaiting approval	N/A
2	25/02/20	Martine King	Approved by SIRO	Yes
3	17/05/20	Marting King	Reviewed	N/A
4	21/06/21	Martine King	Updated	N/A
5	09/04/25	James Swarbrick	Updated to include AI, meetings, doorbell cameras	
6	23/07/25	Martine King	Updated roles and responsibilities, adding links to policy documents,	

			refreshed language and updated to reflect ICO guidance	