



CCTV

1. Background

Closed-Circuit television (CCTV) is the use by Abbeyfield The Dales Ltd (ATD) of video cameras to transmit a signal covering specific public areas of offices, houses or the care homes, and of vehicles (via dashcam), to a place where the images can be confidentially viewed by designated individuals, on a set of monitors. Dashcam footage may also help in the case of road traffic incidents or other activities linked to staff when driving. This commitment to ensure the safety and security of individuals who receive and deliver services is based on the Mission Statement and Values of ATD.

As ATD is not a public authority identified by the Regulation of Investigatory Powers Act 2000, the provisions of that act do not apply. However, this policy draws on its provisions to direct best practice. Other legislation that has directed the drafting of this policy includes the Human Rights Act 1998 and the Protection of Freedoms Act 2012 as well as relevant guidance.

2. Objectives

Through the delivery of this policy, we aim to:

- To ensure our practice in the installation and use of CCTV operates in a way that enhances the quality of life for older people and enables safe services to be developed that meet the needs of future generations.
- To ensure that any CCTV system is correctly and efficiently installed and operated appropriately; and
- To ensure that ATD's use of Closed-Circuit Television (CCTV) adheres to the principles of the Data Protection Act 2018 (DPA), and any other relevant legislation.

Where CCTV is installed by ATD it is designed to:

- Capture images and sound.
- Ensure the safety of residents, visitors, volunteers, and staff.
- Assist in the prevention and detection of crime against both persons and property.
- Be reviewed as evidence if there are causes of concern raised.
- Ensure the security of property belonging to ATD and to residents, staff, volunteers, and visitors.
- Facilitate the identification, apprehension, and prosecution of offenders in relation to crime; and
- Assist in the prevention and detection of serious misconduct involving staff and volunteers.

3. Scope

This policy applies to the following groups, who are also likely to be the data subjects of any personal data captured by the CCTV system:

- All staff and volunteers working for ATD.
- Residents residing in ATD managed properties; and
- Visitors to ATD sites.

4. Policy (Applicable to all CCTV Monitoring)

4.1. Implementing CCTV

Where ATD believes that CCTV should be installed and used they will set out their case to the Chief Executive (CE) and apply for approval.

The following will be used to decide whether CCTV should be installed and operated:

- The purpose for using CCTV (What are the problems it is meant to address and what benefits will be gained?).
- Can CCTV realistically address these issues and deliver these benefits? Could less privacy intrusive solutions, such as improved lighting, achieve the same aims.
- Will the equipment/system being considered deliver the desired benefits now and in the future.
- What future demands may arise for wider use of the images recorded and how will these be addressed.
- What are the views of those who will most be under surveillance; and/or
- What can be done to reduce intrusion for those being monitored, particularly if concerns have been raised.

The decision to agree the use (or deny the request) will be made by the CE who will weigh all relevant factors, including those set out above, against the goal that the installation of CCTV is trying to achieve to reach a balanced and proportionate decision.

4.2. CCTV in Operation

ATD, where CCTV is in operation, will ensure:

- It is fairly and lawfully obtained, recorded and held.
- It is processed only for specified and limited purposes.
- It is adequate, relevant and not excessive.
- Not kept for longer than necessary and kept up to date.
- It is processed in accordance with individual's rights, that is, to be notified of the use of CCTV and supplied with relevant information if requested.
- It is stored in a secure manner.
- The Maintenance Manager will be responsible for overseeing that monitoring of all images is done in accordance with this policy and that suitable operation, backup, retention, destruction and maintenance of all storage media is conducted.
- Cameras are not hidden from view and appropriate steps are taken, e.g. by signing and displaying posters, to inform individuals of the presence of the system and who operates it (including contact details) always.
- To ensure privacy, cameras must be fixed and focussed on ATD property only, and be demonstrable upon request.
- Each use of CCTV will be regularly reviewed against all relevant factors including those listed at 4.1 above; and
- That CCTV equipment is regularly checked to confirm it is providing clear and useful images.

4.3. Compliance with data protection requirements

ATD's use of CCTV will comply with the DPA and the CCTV Code of Practice 2013 issued by the Information Commissioner.

4.4. Approval to use monitoring

Any request for approval to use CCTV Monitoring must be made by the unit Manager to the CE using Appendix 1 of this policy.

In addition to the considerations at 4.1 above, when deciding whether CCTV surveillance is necessary, **the CE** will consider:

- Whether another party, such as a person with law enforcement or investigatory powers (or their representative) should carry on the monitoring. (The CE must also consider whether it is lawful for ATD to allow the person to conduct the monitoring.).
- Whether it is necessary or appropriate, and feasible, to obtain the consent of person(s). For example: in relation to residents, CCTV to protect a resident may require the consent of the resident or that person's legally appointed representatives, and family members (unless family members are potentially subject to surveillance).
- Whether there is any other method of obtaining the information required or achieving the intended goal.
- The length of the duration of surveillance.
- The equipment needed to carry out the surveillance.
- The effect on the privacy of others; and
- Compliance with the requirements of this policy.

The additional considerations set out in Section 4.5, below, will apply in the case of any application for approval of covert CCTV monitoring.

The CE will consider all relevant factors to reach a balanced and proportionate decision.

4.5. Access to CCTV Recordings

Individuals wishing to access images from the system or formal subject access requests specifically relating to CCTV must write to the Business Support Manager. Such requests will be handled in accordance with our Access to Personal Information policy.

In addition, those making a request will be asked to provide:

- Two forms of proof of identification including photo ID and a recent utility bill.
- 2 recent photos, one straight on and one profile, to enable operators to identify the requester; and
- Times and dates of visits to the site where they may have appeared on CCTV. ATD cannot search through their entire archive of CCTV footage to facilitate each request.

Where ATD cannot comply with the request without disclosing the image of another identifiable individual it shall not make any disclosure unless:

- the other individual has consented to the disclosure of the information to the person making the request; or
- it is reasonable in all the circumstances to comply with the request without the consent of the other individual. For example, if ATD can blank or conceal the identity of the other individual without incurring excessive cost.

4.6. Viewing CCTV Images and Recordings

Viewing of live images on monitors should be restricted to authorised employees and will be done only where doing so meets the purpose of using CCTV.

Recorded images should be viewed in a restricted area, such as a private office and should be restricted to authorised employees who are viewing the images for the purposes stated above.

4.7. Storage and Destruction of Recorded Material

In most instances, CCTV used by ATD will automatically re-write after approximately 1 month, at which point older recorded material will be deleted and written over.

In any other instance, all material recorded by CCTV will be kept in a locked, secure cupboard which is only accessible by authorised employees. Material will not be kept for any longer than is necessary and will be destroyed after 3 months, unless it is required as part of on-going investigations under this Policy.

4.8. Breaches of This Policy

ATD will investigate any breaches of this policy using the procedures set out in the Disciplinary Policy and Procedure.

The purpose of this policy is safeguard and ensure the health and safety of staff, volunteers, residents and visitors, any intentional or reckless interference with any part of any monitoring equipment, including cameras/monitors/back-up media, may be regarded as potentially gross misconduct and a criminal offence.

4.9. Complaints

Complaints relating to the use of CCTV should be addressed to the Quality Manager (QM) and will be handled in accordance with our Complaints Policy.

4.10. Covert CCTV Operations

In exceptional circumstances, information may be presented whereby there is no alternative but to use covert CCTV operations.

Monitoring is covert if it is carried out without the knowledge or consent of individuals who may be viewed or recorded via a CCTV installation. In the case of covert CCTV monitoring the policy set out in this Section applies in addition to the policy set out in Section 4.4, above.

4.10.1. Approval to use Covert Monitoring

Any request to use Covert Monitoring must be made by the relevant unit Manager to the CE in accordance with Section 4.4 of this policy, above.

In addition to the considerations stated in Section 4.4 above, when deciding whether covert surveillance is necessary, the CE will consider:

- Whether it is lawful to undertake the proposed covert CCTV monitoring.
- What special measures are proposed to safeguard the interests of persons who may be viewed or recorded via the covert CCTV installation, and the effectiveness of those measures.

4.10.2. Using Covert Monitoring

Covert monitoring may only be used where:

- The monitoring relates to behaviour, not to contract performance.
- It is carried out to investigate a suspected criminal activity or malpractice; and/or
- Informing staff, volunteers or others filmed is likely to prejudice the above purpose.

The following may be considered instances where the use of covert recording may be used (this is not an exhaustive list and ATD reserves the right to use covert recording in other instances not listed):

- The theft of ATD monies or property.
- The theft of resident, staff, volunteers or visitor property.
- Suspected abuse in any form of a resident.
- The unauthorised use of the ATD equipment or facilities; and/or

- Any behaviour, act or omission which may be thought to amount to gross misconduct, or which puts others (most notably residents) at risk.

4.11. Intrusive Surveillance

In some circumstances, it may be an inevitable consequence of the surveillance that residents or staff are captured by the system in a manner that is intrusive. This type of surveillance could be particularly intrusive for residents and the CE will take this into account when considering requests for covert monitoring. Normally it will be approved only in exceptional circumstances.

ATD will take all steps possible to avoid intrusive surveillance including placing and positioning equipment to avoid or minimise such surveillance wherever possible. Reviews of potentially intrusive surveillance will be conducted at least every 14 days.

5. Finance, Value for Money & Social Value

The cost of monitoring and surveillance will be included in the decision-making process in installing CCTV.

Equipment will be sourced from and installed by reputable and approved companies, and advice will be sought where relevant.

6. Supported Appendices

APPENDIX 1: CCTV Surveillance Approval Form

7. Linked Policies

Disciplinary (S008P)

Data Protection (LG013P)

8. Legislation/Regulation

Data Protection Act 1998

Data Protection Code of Practice

Human Rights Act 1998

Regulation Investigatory Powers Acts 2000

Protection of Freedoms Act 2012

9. Review

Every 2 years, subject to regulatory and legislative changes.

10. Procedure/Guidance

N/A

Abbeyfield The Dales Ltd

CCTV Surveillance Monitoring Form



Applicant:

Full Name:

Job Title:

Date:

Location of Surveillance:

Full address to be monitored:

Precise location of camera:

Precise area monitored at the address:

Area type:

☐ Public

☐ Private

☐ Dwelling

☐ Intimate

Camera screen needed to block out other locations?

☐ Yes

☐ No

Surveillance Objects:

Person(s) under surveillance:

Other person(s) who may be directly affected:

Person(s) who may need to be informed or asked to consent:

Purpose of Surveillance:

Full details of the purpose(s):

Why is the surveillance necessary?

Duration of Surveillance:

Proposed start date:

Proposed duration/ end date, or ongoing?

If ongoing, in what circumstances will the surveillance stop?

Proposed intervals for review of whether surveillance is necessary and justified:

Abbeyfield The Dales Ltd. Registered Charity Number: 1160258, Company No: 9008680, Home England No: 5066

Method of Surveillance:

Explicit or covert?

☐ Explicit

☐ Covert

Technical requirements (e.g. camera size, resolution, weatherproofing, wired or wireless, optical zoom depth, sound or no sound recording, remote control or fixed field of view, constant recording or movement detection, recording hardware, recording file format):

Selection of Raw Footage for Storage/Use:

When will footage be checked?

Which CCTV-trained member(s) of staff will check the footage to identify footage that is relevant for the purpose(s)?

How will the interests of "accidental" surveillance subjects be safeguarded (e.g. regular check and deletion of unnecessary footage)?

Internal Use of Surveillance:

Who else internally will need access to footage that is identified as being relevant for the purpose(s)?

Method of sharing footage internally (note that good security measures are required, particularly for sensitive information)?

External Use of Surveillance:

Will any third party need access to live footage or raw (recorded) footage? If "yes", name each third party and their purpose for accessing footage:

Will any third party need access to selected relevant footage? If "yes", name each third party and their purpose for accessing footage:

Storage of Footage:

Proposed security measures (note that special measures will be required for sensitive information):

How long will unnecessary footage be kept?

How long will relevant footage be kept?

How will footage be destroyed:

Data Protection Officer ONLY:

Surveillance approved?

☐ Yes ☐ No

Reasons/ basis for approval:

Details of surveillance that is approved:

Prohibitions, restrictions, conditions:

Full Name:

Signature:

Date: