CCTV and Surveillance Equipment Policy

Policy ref:	
Policy author /holder	Data Protection Manager
Date approved:	15 December 2021
Approved by:	Information Security & Governance Team
Effective date:	15 December 2021
Review date:	1 December 2024

1 Purpose and anticipated outcomes

1.1 The purpose of this policy is to ensure that LiveWest's use of closed-circuit television (CCTV) and dashcam complies with:

- The General Data Protection Regulation as implemented in the UK (UK GDPR)
- The Data Protection Act 2018
- The Surveillance Camera Commissioners Code of Practice

1.2 This policy addresses resident's use of domestic CCTV (including 'Ring' doorbells and similar devices)

1.3 This policy should be used alongside the CCTV installation procedure which clarifies departmental responsibilities.

2 Scope and definitions

2.1 CCTV operated by LiveWest

LiveWest uses CCTV within its business and premises (including vehicles) for the purposes of:

- Crime prevention and detection, and the apprehension and prosecution of offenders
- Ensuring customer, staff, and public safety

- The detection and management of anti-social behaviour and other criminal acts
- Establishing, exercising, and defending legal rights
- A source of evidence for compliance with LiveWest policies and procedures.

We do not typically permit the use of CCTV for any other purpose. A data protection impact assessment (DPIA) must be completed and approved by the Data Protection Manager for any changes of use or new use of CCTV or surveillance equipment.

2.2 This Policy applies to any employee (or other member of staff including contractors and temporary staff) who has access to, responsibility for, or may otherwise use the CCTV systems in operation.

2.3 Customer installed CCTV

When LiveWest are aware that customers have installed CCTV, including Ring doorbells or similar devices at their own properties, we will advise them to ensure that they are aware of the legal implications, and that they do not invade the privacy of others. These systems are not within LiveWest's control.

Our approach to customer installed CCTV is detailed below.

2.4 Dummy CCTV

We do not install or use dummy CCTV cameras.

2.5 Dashcams

This policy also addresses the use of dashcams in LiveWest company vans.

3 Policy statement

3.1 CCTV technology

LiveWest use cloud-based surveillance technology. All new installations will be cloud-based, and as other contracts end, installations will be moved onto the cloud-based system.

3.1.1 Having a single standard technology enables us to meet several legal and business requirements.

Data protection (UK GDPR) compliance:

- Controlling retention periods for recordings
- Controlling access to live images and recordings
- Maintaining privacy of individuals when using cameras
- Ability to respond to official requests from Law Enforcement Agencies

Business requirements:

- One system for maintenance and support
- A clear overview of our CCTV coverage
- Access to live images and recordings when mobile working
- Access to the system can be managed and amended easily if required (e.g., in case of staff illness)

3.1.2 CCTV and surveillance equipment installations

- The CCTV overt surveillance procedure details the process to be followed for installation of overt CCTV cameras at LiveWest sites.
- The CCTV covert surveillance procedure details the process to be followed for the installation of covert CCTV cameras. This is for use by the Enforcement Team only.
- The use of body-worn cameras may be approved if they are assessed as being proportionate and necessary. A data protection impact assessment (DPIA) will be required for each usage, to define when cameras will be switched on (it is unlikely that there would be justification for continuous recording). Careful consideration must be given to the use of video only or video with audio recording, and whether the selected technology enables a choice to be made. Anyone using a body-worn camera will need to have signage on their person. Any staff or contractors using body-worn cameras will need to be trained on the appropriate use of the equipment and the recorded footage.

- The installation or use of any other surveillance equipment which could be

used across LiveWest's housing stock, such as drones and smart technology would require a DPIA (Category 2) which sits outside of this policy and will require prior approval by the Data Protection Manager or Data Protection Officer

3.1.3 Data protection impact assessments (DPIA)

A DPIA is required and will form part of the decision to install any type of surveillance system at LiveWest sites. A CCTV installation form which forms part of the Overt /Covert surveillance Procedures must be completed prior to installations for every site. This will ensure:

- There is a clear purpose and benefit for the installation
- The number of cameras installed is not excessive for the purpose
- The siting of the cameras is relevant to the purpose
- Care is taken to avoid unnecessary infringements on privacy

If privacy concerns are identified the Data Protection Team and Area Housing Manager will carry out a risk/benefit analysis on order to mitigate the risks.

3.1.4 Approval of installations

Approval for the installation is made by the Data Protection Manager, Senior Departmental Manager, or relevant Head of Service.

3.1.5 Access to CCTV live feeds and recordings

This is limited to the staff listed on the installation form. The Data Protection Team may also be given access in order to respond to subject access requests (SAR's). CCTV images must not be viewed by customers or any staff that are not listed on the CCTV installation form. CCTV footage should only be viewed when necessary to meet the purposes outlined above (2.1).

3.1.6 Monitoring CCTV

The level of monitoring of CCTV required for each site forms part of the CCTV installation form. Cloud-based systems enable monitoring from any location using a laptop or other mobile device. CCTV should only be monitored using a LiveWest device. There should be no "public" monitoring or any recording on mobile devices attached to the cloud-based CCTV installation.

Scheduled real-time monitoring will be authorised in some cases, but the default is that we do not carry out real-time monitoring, unless there is an emergency. Real-time monitoring should be authorised by the Data Protection Team. If you are responding to an emergency and authorisation cannot be gained at the time, the Data Protection Team should be informed of the situation without delay.

3.1.7 Retention of recorded CCTV images

CCTV footage will be retained for 3 months. Any footage required for complaint handling, a police investigation or court case can be retained for longer within the cloud-based system, if identified before deletion. Once the footage is no longer needed it should be deleted without delay.

3.1.8 Signage

We are legally required to notify individuals (whether members of staff, customers, or the public) if they are in an area where CCTV surveillance is being carried out.

The main way to achieve this is through prominent signs in the area which is being monitored. LiveWest have standard signage which can be ordered via the communications team and installed by property services.

The signs must:

- Alert individuals that they are entering a CCTV monitored zone
- Be legible and visible

We will also reference that CCTV may be used on our sites in our online privacy notice.

There may be rare occasions where giving notice of the presence of CCTV would no be appropriate, for instance if it would undermine investigations into illegal subletting or would increase the risk of physical violence against staff or customers. The process for installing these covert surveillance systems is contained within the covert surveillance procedure.

3.2 Dashcams

LiveWest make use of dashcams in company vans. The footage is collected by front-facing, non-audio cameras and the dashcam records whilst the engine is running on a 20-hour loop.

The main purposes for installing dashcams are:

- To protect our IMS Operatives against allegations of dangerous driving by other road users or members of the public
- To protect LiveWest from false insurance claims by providing evidence regarding liability
- To support IMS Operatives and LiveWest managers in resolving issues of driver performance in line with the driver's handbook, performance management and disciplinary procedures.

3.2.1 Access to the footage

The footage will be stored on a web-based system, and footage will only be accessible for download by the Fleet Manager or Procurement Manager in the Fleet Manager's absence. It may be viewed by the IMS Operative's line manager and the IMS Operative who was driving the vehicle, as necessary. It may also be necessary for representatives of the People Services Team, Legal Advisors, Senior Managers (including the relevant Executive Leader) and our insurance company to view footage in cases involving performance management/ disciplinary issues or insurance claims. Anonymised versions of the recordings may also be used for training purposes.

3.2.2 Retention periods

The dashcam footage will be stored for three months. Any footage required for dealing with a complaint, a police investigation or court case could be retained for longer within the cloud-based system, if identified before deletion. Once the footage is no longer needed it should be deleted without delay.

3.2.3 Signage

LiveWest company vans will be fitted with standard signage to provide notification that a dashcam is installed.

3.3 Subject Access Requests

Individuals have the right to access personal data which we process about them, which includes (in most cases) CCTV images of them from cameras sited where they live and the immediate surroundings, and at a place of work including dashcam footage taken whilst driving. If you receive a request from an individual asking to see CCTV or dashcam footage involving them or otherwise mentioning access to personal data, please refer to the Data Protection Team for advice data.protection@livewest.co.uk

3.4 Non-cloud-based installations

On sites where we have older CCTV technology which has not been upgraded to a cloud-based system the site owner, as listed on the overt installation form needs to:

- Check monthly that equipment is functioning
- Ensure that access to monitors and footage is limited to those listed on the CCTV installation form
- Ensure that access to the live feed and recordings is limited to only the appropriate staff
- Update the CCTV register of monthly site checks to confirm that these checks have been done

3.5 Customer installed domestic CCTV filming within their property boundary

If a customer installs CCTV which only records footage within their own boundary LiveWest consent is not required.

3.6 Customer installed domestic CCTV filming outside of their property boundary

This section of the policy relates to customers use of domestic CCTV, which refers to any video surveillance equipment mounted or fixed on a customer's home or positioned within the home so that it films external areas outside of the boundaries of the property, or areas to which members of the public have access. It can include cameras fitted to doorbells, including Ring doorbells.

LiveWest is aware that residents may wish to install domestic CCTV, and of the benefits this brings in terms of increased security and convenience. However, these benefits need to be balanced against the privacy rights of other individuals and members of the public, particularly where CCTV may be filming communal areas.

LiveWest does not prohibit the use of domestic CCTV, but residents are expected to use domestic CCTV in a reasonable manner which respects other people's privacy, and in accordance with the law, and their tenancy agreement or other contract with us. Cameras should only be installed on/in the property which has been let to the customer and any alterations that are needed in order to make the installation would need to be undertaken in compliance with the terms of the tenancy agreement.

3.6.1 Operation of customer installed domestic CCTV

LiveWest does not involve itself in complaints and disputes between neighbours regarding the use of domestic CCTV. Such complaints should be directed to the Information Commissioners Office and/ or the customer involved (who may be the data controller for the purposes of the Data Protection Act 2018 and UK GDPR). However, LiveWest reserves the right to require customers to remove domestic CCTV

if they are found to be using it in a breach of the law or their tenancy agreement, or the use of CCTV has become a substantial source of ASB complaints.

Residents who wish to install domestic CCTV should be aware that if their CCTV system captures images beyond the boundary of their property, of people not within their household, and the footage is used for any purpose which is not connected to their household, they will have to comply with the Data Protection Act 2018 and the UK General Data Protection Regulations (GDPR).

Where LiveWest become aware of a domestic CCTV installation we will provide guidance to customer on how to comply with their legal obligations, using the information set out in the Customer CCTV Guidance Note. If the customer fails to comply with their legal obligations, they may be subject to enforcement action by the ICO. This could include a fine, becoming subject to legal action by the individuals affected and court claims for compensation.

Customers who install domestic CCTV do so at their own risk, and LiveWest does not accept responsibility for any loss incurred, including fines and penalties suffered as a result of customers use of CCTV.

4 CCTV Registers and disclosures to third parties

4.1 Data protection team

The data protection team will maintain a register of CCTV installation forms. The team will ensure that installations are reviewed within the agreed timescales detailed on the installation form, with each installation being reviewed at least every three years.

The disclosure of CCTV footage to any third party, such as the police should be authorised by the Data Protection Team prior to disclosure as per the Law Enforcement and Third-Party Disclosure Guidance Sheet. Disclosures will be recorded by the data protection team and held in the disclosure register.

Other registers:

- Maintenance records (Property services)
- Register of monthly site checks (Scheme staff)

4.1.1 This policy will be reviewed annually by the data protection team to ensure compliance with data protection regulations. The policy will be reviewed every three years by the Information Security and Governance Team.

5 Legal considerations

- UK implementation of the General Data Protection Regulations (UK GDPR)
- Data Protection Act 2018
- Home Office CCTV guidance
- Surveillance Camera Commissioner guidance
- Domestic CCTV systems- guidance for people using CCTV (ICO)

6 Linked / associated policies and other references

- Data Protection Compliance Policy
- Neighbourhood Management Policy
- CCTV and Surveillance Equipment Installation Procedure
- Customer installed CCTV Guidance Note
- CCTV and Surveillance Equipment Briefing Note for Staff
- Law Enforcement Guidance Note
- CCTV Overt Installation Form
- CCTV Covert Installation Form
- Information Risk Management Policy