L&Q CCTV and Surveillance Policy

1 Purpose 2
2 Scope 2
3 Legislation and Regulation 2
4 Definitions 3
5 Systems Managed by Us 5
6 Residents Use of Surveillance and Recording Devices 7
7 Drones 9
8 Monitoring and Controls 9
9 Equality, Diversity and Inclusion 10
10 Communication 10
11 Policy controls sheet 11

1 Purpose

1.1 Use of CCTV and surveillance can play an important role in helping to protect residents, visitors, and colleagues, deter crime and anti-social behaviour, and support investigations where incidents occur. However, we recognise that CCTV and other forms of surveillance can also raise concerns about privacy and the appropriateness of monitoring.

1.2 We use CCTV and surveillance in some areas that we manage, to help keep residents, visitors, and colleagues safe. We are also aware that this is now an area of changing technology, and residents may have access to types of surveillance equipment. This policy includes where CCTV or surveillance may be in place or is being considered. It covers both systems we operate and those installed by residents, and how these are to be managed responsibly.

2 Scope

2.1 This policy applies to areas managed by us where CCTV or surveillance systems are, or could be, used. This includes, but is not limited to:

- Communal entrances, lobbies, landings, and hallways
- Car parks, bin stores, and cycle stores
- Estate perimeters and external communal areas
- Our operational buildings such as offices, hubs and community centres

2.2 It applies to all parts of the L&Q Group and all tenure types.

2.3 It sets out our approach to resident-managed systems, including domestic CCTV systems and video doorbells.

2.4 It also covers the use of other recording and surveillance devices such as mobile phones, drones, noise apps, and staff safety devices including body cameras.

2.5 This policy should be understood in the context of our Data Protection policy, as well as our Anti-Social Behaviour and Supporting Good Neighbourhoods Policies.

3 Legislation and Regulation

3.1 We always aim to meet our relevant legislative and regulatory obligations. Those relevant to this policy include, but are not limited to:

- **Data Protection Act 2018 and UK General Data Protection Regulation (GDPR)**

Under the Act, footage must only be collected for specific and legitimate purposes and individuals have rights to their data. Regulation ensures that personal data collected is processed lawfully, fairly and transparently.

- **The Human Rights Act 1998**

  The Act protects individuals from unjustified interference with their privacy. Any recording must respect this right, balancing security needs with privacy considerations.

- **Protection from Harassment Act 1997**

  This Act protects people from harassment. It does not specifically regulate CCTV or surveillance, but it may be relevant where surveillance or recording forms part of behaviour that amounts to harassment.

- **Surveillance Camera Code of Practice (under the Protection of Freedoms Act 2012)**

  This provides best practice guidance for using and managing surveillance systems in a way that is accountable, proportionate and transparent.

- **Information Commissioner's Office (ICO) – CCTV Code of Guidance**

  The ICO provides practical guidance on ensuring transparency and fairness, advising that individuals should be informed when they are being recorded, and that data is kept secure and used for specific, justified purposes.

- **Home Office - Surveillance Camera Code of Practice**

  Sets out principles for responsible use of surveillance cameras, stressing that systems should be proportionate, accountable, and respect individuals' privacy, ensuring regular review and clear governance.

- **Civil Aviation Authority (CAA) regulations and the Drone and Model Aircraft Code**

  These set out the legal and safety requirements for operating drones in the UK, including registration, flight restrictions, and responsibilities for safe and lawful use.

4 Definitions

4.1 These definitions explain how certain words and phrases are used throughout this policy.

4.2 **Closed- Circuit Television (CCTV)**- refers to fixed cameras that capture and record images of people and property to help keep areas safe.

4.3 **Surveillance**- monitoring a place, person, group, or ongoing activity in order to collect information.

4.4 **Overt surveillance-** the surveillance that people would reasonably expect or be aware of. This includes visible CCTV cameras with clear signs showing that CCTV is in use.

4.5 **Covert surveillance**- the surveillance where people would not reasonably be aware that monitoring is taking place. This can include the use of hidden safety devices.

4.6 **Communal area-** refers to areas of a house or a block of flats or an estate that residents have a right to use in common. Examples of communal areas include, but are not limited to, corridors and walkways, entranceways and exits, shared exterior spaces, communal lounges and kitchens.

4.7 **Data-** in relation to CCTV/surveillance equipment usually means recorded video images. It may also include audio recordings (where applicable) and still images, such as printed or saved screenshots.

4.8 **Audio recording**- the recording of sound or conversations, either on its own or alongside video recording.

4.9 **Personal data-** information that identifies a living person, either directly or when combined with other information. This can include images, names, addresses, or contact details.

4.10 **Lone working devices**- devices or applications used to support colleague safety when they are working alone or in higher-risk situations. These may include features such as location tracking, alarms, audio recording or incident reporting.

4.11 **Drone**- a small aircraft that can fly without a person on board. They are usually controlled remotely and may have cameras or other equipment attached.

4.12 **Data controller**- a person or organisation that decides why personal information is collected and how it is used.

In most cases, we are the data controller for our systems, as we decide how residents' personal information is collected, used, stored, and shared.

In some situations, individual residents can also be data controllers. This may happen when a resident chooses to collect, keep, or share personal information about other people and decides what that information will be used for (see section 6.3).

4.13 **Secured by Design (SBD)**- the official UK police crime-prevention programme. It provides guidance and standards to help reduce crime through the design of buildings, shared spaces, and security measures such as CCTV.

5 Systems Managed by Us

5.1 Our commitments

5.1.1 We are committed to the ethical and proportionate use of surveillance. CCTV systems will only be used where there is a clear and justifiable purpose.

5.1.2 We aim to balance the benefits of CCTV with individuals' rights to privacy. Systems will be designed and operated to minimise unnecessary intrusion into people's private lives, focusing only on relevant communal or operational areas.

5.1.3 We will be open and transparent about our use of CCTV. This includes providing clear signage about where systems are in place, why they are used, and how recorded information is handled.

5.1.4 We will manage our CCTV systems carefully and review them regularly to make sure they are working properly and being used in the right way. We will follow data protection law and our internal policies, and we have clear processes in place to deal with any concerns or complaints.

5.2 Purpose of CCTV and Surveillance

5.2.1 We use CCTV systems to:

- Support the security of our offices, properties, and the surrounding environment;
- Protect the health and safety of residents, colleagues, and visitors; and
- Prevent, deter, and assist in the investigation of anti-social behaviour and crime.

5.3 Locations and Types of CCTV

5.3.1 CCTV will not be installed inside individual homes.

5.3.2 Fixed cameras are typically the most appropriate form of installation for communal areas and external locations.

5.3.3 Clear and visible signage will be displayed to inform individuals that CCTV recording is taking place, except where covert monitoring is lawfully authorised and approved in line with legal requirements and internal procedures.

5.4 Temporary, Overt, Covert, and Audio Recording

5.4.1 We manage risk proactively and do not routinely rely on surveillance or recording. However, where necessary, surveillance may be used to support safety, service delivery, and evidence gathering. This may include the use of other recording and surveillance devices such as noise apps, lone working devices and body cameras.

5.4.2 Our default approach is to use overt surveillance. Examples include:

- General CCTV systems, which are installed for visible security and monitoring purposes
- Drones, where used for visible and legitimate purposes such as inspections or estate monitoring (further detail in section 7)

5.4.3 Covert surveillance will only be used in specific situations and will be subject to appropriate controls. This may include devices used to support colleagues' safety, or devices or applications provided to residents to help them capture evidence when they are experiencing anti-social behaviour.

5.4.4 In some circumstances, temporary CCTV systems may be used to monitor a specific location or gather evidence of particular activities. These systems may operate overtly or covertly, depending on the assessed need and subject to legal requirements and internal authorisation and checks.

5.4.5 Audio recording will only be used where it is lawful, necessary, and proportionate. For example, to protect colleagues in monitored reception areas or where required for specific investigations. Any use of audio recording must be fully justified, appropriately authorised, documented, and communicated through clear signage unless covert recording is approved.

5.5 Approval and Installation of New Systems

5.5.1 New CCTV systems may be installed where:

- A majority of residents on an estate request installation; or
- Installation is recommended as part of a Secured by Design (see definitions) review for new-build schemes.

5.5.2 We will consult with residents on significant changes to services or service charges where appropriate. Please see our Service Charges and Sinking Funds Policy for more detail on new systems or changes to existing systems.

5.6 Use, Access and Disclosure of CCTV Footage

5.6.1 We will ensure all CCTV systems and associated processing comply with UK data protection legislation, including the UK GDPR and Data Protection Act 2018. This includes ensuring systems are assessed, operated, and monitored in line with privacy principles

5.6.2 Access to recorded images is restricted to authorised officers only. All equipment and storage media will be kept secure and protected against unauthorised access.

5.6.3 CCTV footage will be retained only for as long as necessary, typically up to 31 days, after which it will be securely deleted.

5.6.4 CCTV images are considered personal data, so sharing them is only permitted where there is a lawful basis, such as crime prevention, detection, or legal obligations. Any

sharing must be proportionate and comply with our Data Protection Policy. We would not share CCTV footage with residents or third parties unless there is a legal obligation or it is required for safeguarding, legal proceedings or law enforcement.

5.6.5 Where footage is required for legal proceedings or investigations, it may be retained for longer in secure storage and will be subject to periodic review to ensure continued necessity.

6 Residents Use of Surveillance and Recording Devices

6.1 Permission

If you follow the requirements in this policy, you have our permission to use a domestic CCTV system or video doorbell. We have taken this as our default approach based on resident consultation. However, this permission is limited. We can require you to remove it if we have concerns about its use or receive a complaint about it.

6.2 Permitted Use

6.2.1 CCTV systems, video doorbells and similar devices must be used responsibly, proportionately and only for legitimate household purposes, such as:

- Home security
- Monitoring deliveries
- Supporting the safety and wellbeing of household members or visitors
- Managing access to their property

6.2.2 When installing CCTV or video doorbells, you must ensure your system is positioned and configured to minimise intrusion into other people's privacy. This includes:

- Positioning cameras to mainly capture your own property and avoid unjustified recording of neighbouring properties, communal areas, or other people's private activities
- Avoiding recording beyond the boundary "just in case"
- Adjusting camera angles and limiting the field of view to what is necessary
- Using privacy masking features where available
- Avoiding the use of audio recording unless strictly necessary, as this is more intrusive than video

6.2.3 You should not drill into doors, frames, or surrounding areas to install a video doorbell or CCTV equipment. This is especially important for fire doors, as any changes can affect their safety. Wherever possible, you should use non-invasive

installation methods, such as self-adhesive fittings, so that no damage is caused to the door or property.

6.2.4 Examples of inappropriate recording include (but are not limited to):

- A neighbour's front door, garden, or windows
- Shared internal spaces, such as communal lounges
- External communal areas, such as shared gardens
- Public pathways

Note- where those being filmed in communal areas have given permission this would not be deemed inappropriate.

6.2.5 The use of multiple devices, high-powered zoom, or excessive coverage beyond what is reasonably required for home security will be considered disproportionate.

6.3 Dealing with Data Protection

6.3.1 You are responsible for managing, monitoring, storing, accessing and deleting footage from your own system.

6.3.2 If your CCTV or video doorbell captures images beyond your property boundary (for example, neighbouring homes, shared areas, or the street), data protection law will apply. In these circumstances, you will be acting as a data controller (meaning you are responsible for how the footage is collected, used, and stored). As a data controller, you must:

- Use your system in a lawful, fair, and transparent way
- Only record what is necessary for your security purposes
- Keep footage secure and restrict who can access it
- Display a clear sign to let people know CCTV is in use
- Only keep footage for as long as you need it
- Respond to individuals' requests to access footage of themselves in line with data protection law
- Be able to explain why your camera records beyond your property boundary

For more information, you should refer to the Information Commissioner's Office (ICO) guidance on domestic CCTV.

6.4 Enforcement and Managing Concerns

6.4.1 If a complaint is made about your CCTV use, or we have concerns, we may:

- Request details about your system setup and field of view

- Ask you to adjust or reposition your camera
- Require you to remove your CCTV
- Provide guidance to help you comply, including signposting to the ICO
- Take legal action

6.4.2 If your use of CCTV is disproportionate, amounts to misuse, or if there are unresolved issues with neighbours where surveillance has been highlighted as a concern, your permission to use CCTV will be revoked at that time. Please also see our Supporting Good Neighbourhoods Policy.

6.4.3 You must not use CCTV or other recording devices to intimidate, harass, or monitor our colleagues or those working on our behalf. If this happens, we will take action under our Unreasonable Behaviour Policy, or Anti-Social Behaviour (ASB) Policy where it affects others.

7 Drones

7.1 We may use drones for specific operational purposes, such as roofing inspections, stock condition surveys, and other high-level property maintenance activities. Their use is intended to improve safety by reducing work at height and to support efficient management of homes.

7.2 We will carry out drone operations lawfully, proportionately, and transparently, considering residents' privacy and the surrounding environment. We will not use drones for resident surveillance or monitoring.

7.3 Where residents choose to use drones, they must do so responsibly and in full compliance with relevant legislation and regulatory requirements. This includes Civil Aviation Authority (CAA) rules, the Drone Code and data protection laws. Any use must not intrude on neighbouring properties, communal areas, or the privacy of others. Misuse may be addressed under tenancy or anti-social behaviour provisions.

8 Monitoring and Controls

8.1 Existing CCTV systems will be managed and maintained to ensure they remain effective, compliant, and fit for purpose. We will keep a record of Data Protection Impact Assessments, and these will be reviewed where there are significant changes.

8.2 Information will be stored in line with data protection principles.

8.3 Performance on subject access requests and data breaches will be monitored as part of our Data Protection Policy.

8.4 We will continue to monitor the use and impact of CCTV and surveillance, including through complaints. We will use this to review this policy where needed. For example, while our current default position is to give our permission for residents to install doorbell cameras, including for flatted buildings, we will keep this under review.

9 Equality, Diversity and Inclusion

9.1 We will apply this policy fairly and in accordance with the Equality Act 2010. An Equality Impact Assessment has been carried out as part of developing this policy.

9.2 We recognise that CCTV and surveillance may affect some residents differently. For example, older residents, those with a disability or impairment, those with limited English, as well as residents living in flats may face additional challenges. This can include understanding how surveillance is being or should be used, what their rights are, and raising concerns about privacy or misuse – particularly in shared areas.

9.3 We will take these circumstances into account and make reasonable adjustments where needed. This may include:

- providing information in accessible formats, interpretation or other communication support
- providing non-digital ways for residents to raise concerns or ask questions
- taking vulnerability and safeguarding concerns into account when responding to reports about CCTV or surveillance misuse

9.4 We also recognise that CCTV and other surveillance may be used inappropriately as part of harassment, intimidation, or controlling behaviour. We will handle these concerns sensitively and in line with relevant safeguarding, anti-social behaviour, and data protection processes.

9.5 We will monitor the impact of this policy and take action to address any unintended barriers or adverse effects on residents.

10 Communication

10.1 This policy will be published on the L&Q website.

10.2 We will publish this policy internally for colleagues to access, along with associated procedures, processes and guidance.

10.3 Residents have the right to question how their data (including CCTV images) is being used and can request information through a Subject Access Request.

10.4 Residents, representatives, members of the community, our partners, the police and other agencies, have concerns of anti-social behaviour they can report it to us either by phone, online, or in writing.

10.5 If a resident feels CCTV is being misused or installed without proper notice, they can raise a complaint. Complaints regarding the application of this policy will be managed in line with our Complaints Policy.

11 Policy controls sheet

Date of approval: 04/06/2026

Approved by: Customer Group

Effective date: 04/06/2026

Next Review date: 04/06/2029

Policy owned by: Director of Housing Management

Associated documents: ASB Policy, Supporting Good Neighbourhoods Policy, Unreasonable Behaviour Policy, Data Protection Policy

Main change	Key points
Introduction of a new CCTV and Surveillance Policy	• Introduces clear controls for L&Q and resident use of CCTV, surveillance and recording devices. • Sets requirements for lawful, proportionate use, privacy, data protection, complaints and safeguarding.
Reviewed by: The Policy Team	
Approved by: Customer Group	