Aspect Housing Ltd

Data Protection Policy

(Reviewed and Updated September 2026)

Aspect Housing Ltd
171 Alcester Road
Moseley, Birmingham, B13 8JR
Tel: 0121 792 5342
Company Number: 07787308

Approved: September 2025
Last reviewed and updated: September 2026

Aspect Housing

Table of Contents

1. Policy Statement 4
2. Aims and Objectives 4
3. Scope 4
4. Responsibilities 4
5. Lawful Bases for Processing 4
6. Data Subject Rights 5
7. Data Security 5
8. Data Breaches 5
9. Training and Awareness 5
10. Confidentiality 5
11. Body-Worn Cameras 9
12. Legislative and Regulatory Framework 9
13. Monitoring and Review 9

Summary

This policy sets out Aspect Housing Ltd's approach to data protection, ensuring that personal data relating to staff, residents, contractors, and visitors is handled lawfully, fairly, and transparently, including recordings made using body-worn cameras.

The policy covers: lawful bases for processing; data subject rights; security measures; body-worn camera use; breach reporting; staff training; confidentiality agreements; and record keeping.

It complies with the Data Protection Act 2018, the UK GDPR, the Human Rights Act 1998, the Freedom of Information Act 2000 (where applicable), the Equality Act 2010, the Building Safety Act 2022, the Worker Protection (Amendment of Equality Act 2010) Act 2023, the Renters' Rights Bill 2025, and Birmingham City Council Exempt Accommodation Standards (2023–25).

1. Policy Statement

Aspect Housing Ltd is committed to protecting personal data and ensuring compliance with the Data Protection Act 2018 and UK GDPR. We will handle all data lawfully, fairly, and transparently.

2. Aims and Objectives

- Protect the privacy of staff, residents, contractors, and visitors.

- Ensure lawful processing of data under UK GDPR.

- Safeguard sensitive and special category data.

- Provide staff training on data protection responsibilities.

3. Scope

This policy applies to all personal data processed by Aspect Housing Ltd, including resident records, staff files, contractor information, safeguarding data, CCTV and body-worn camera video and audio. It applies to all employees, agency workers, volunteers and contractors who use or handle such data.

4. Responsibilities

- Organisation: Appoint a Data Protection Officer (DPO) or responsible person, ensure policies and systems are in place.

- Managers: Monitor compliance, authorise and oversee body-worn camera arrangements, manage data rights requests, and ensure secure data handling.

- Staff: Follow this policy and the body-worn camera procedure, complete required training, protect equipment and recordings, and report any loss, misuse or breach immediately.

- Residents/Contractors: Informed about how their data is collected, stored, and shared.

5. Lawful Bases for Processing

- Consent: where freely given, informed, and explicit.

- Contract: processing necessary for contracts with residents or staff.

- Legal Obligation: compliance with laws and regulations.

- Vital Interests: protection of life.

- Legitimate Interests: where processing is necessary for the organisation's activities.

6. Data Subject Rights

- Right to access, rectification, and erasure.

- Right to restrict or object to processing.

- Right to data portability.

- Right to withdraw consent at any time.

7. Data Security

- Personal data will be stored securely with access restricted to authorised personnel.

- Electronic data, including body-worn camera footage, will be encrypted where appropriate and protected by access controls and strong passwords.

- Paper records will be stored securely in locked cabinets.

8. Data Breaches

- All breaches must be reported immediately.

- Serious breaches will be reported to the ICO within 72 hours as required by law.

- Incidents will be investigated and corrective action taken.

9. Training and Awareness

- All staff will receive regular training on data protection responsibilities.

- Confidentiality agreements will be signed by staff and volunteers.

10. Confidentiality

Personal and sensitive data will be kept confidential and shared only where there is a valid lawful basis, including where legally required. Body-worn camera recordings must never be copied, viewed or shared for personal or unauthorised purposes.

11. Body-Worn Cameras

11.1 Purpose and application

Aspect Housing Ltd may issue body-worn cameras to authorised night-team staff for use during all property and community rounds. Their purpose is to support staff and resident safety, deter or document aggression and antisocial behaviour, provide an accurate record of significant incidents, and assist with safeguarding, complaints, investigations and the establishment, exercise or defence of legal claims. Cameras are a safety and evidential tool; they must not be used for routine continuous monitoring, staff performance monitoring, covert surveillance or recording for personal purposes.

11.2 Lawful, fair and proportionate use

Body-worn camera processing will be undertaken only where necessary and proportionate. Depending on the circumstances, Aspect Housing Ltd will rely on legitimate interests, legal obligation, vital interests and/or substantial public interest conditions under data protection law. Consent will not ordinarily be relied upon because it may not be freely given in housing, employment, safeguarding or emergency situations. A Data Protection Impact Assessment (DPIA) must be completed and reviewed before deployment and whenever the purpose, technology, operating practice or risk materially changes.

11.3 Activation during night rounds

Cameras may be worn throughout all rounds but must remain on standby unless recording is justified. Staff should activate recording where they reasonably anticipate or encounter aggression, violence, harassment, antisocial behaviour, criminal activity, a safeguarding concern, a serious dispute, a threat to life or property, or another incident for which an accurate evidential record is necessary. Recording should begin as early as reasonably practicable and end when the incident or relevant risk has passed. Staff must not record entire routine rounds merely because a camera is being worn.

Where safe and practicable, staff must announce that recording has started and explain the reason. The camera's visible indicator should remain enabled. If prior notice cannot safely be given, the reason must be documented in the incident record. Staff must not deliberately record inside bedrooms, bathrooms, toilets, changing areas or other places where there is a heightened expectation of privacy unless an immediate and serious safety, safeguarding or evidential need makes recording necessary and proportionate. Particular care must be taken where children, visitors, people receiving care, or individuals in distress are present.

Audio recording may be used only when it is necessary to capture the context of an activated incident. Continuous audio recording while the camera is on standby is prohibited.

11.4 Transparency

Residents, staff, visitors and contractors will be informed of body-worn camera use through appropriate privacy information, the resident or tenant handbook, signage where appropriate, staff communications and verbal notification at the point of recording where safe and practicable. Privacy information will explain the purposes of recording, lawful bases, retention, potential recipients, individual rights and how to contact Aspect Housing Ltd.

11.5 Handling and security of recordings

Only Aspect Housing-approved cameras, accounts and storage systems may be used. Personal phones or personal cloud accounts must never be used to capture, download, transmit or store footage. Recordings must be uploaded to the approved secure system as soon as practicable after the shift or incident and deleted from the device through the approved process once upload is confirmed. Staff must not edit, rename, duplicate, screenshot, post online or informally share recordings. Devices must be securely stored, charged and issued or returned in accordance with local equipment controls. Any loss, damage, unauthorised access or suspected misuse must be reported immediately as a data security incident.

Access will be restricted to specifically authorised personnel on a need-to-know basis. Access, export, viewing, disclosure and deletion should be logged and capable of audit. Where footage is retained as evidence, its integrity and chain of custody must be protected.

11.6 Retention and deletion

Recordings that do not relate to an incident, safeguarding concern, complaint, investigation or legal matter should be deleted automatically within 31 days. Relevant footage may be retained for longer only for a documented purpose and for no longer than necessary, in line with the retention schedule and any legal hold. At the end of the retention period, recordings and authorised copies must be securely deleted. The responsible manager will review any extended retention at appropriate intervals.

11.7 Access, disclosure and data subject rights

Recordings may be disclosed only where lawful and necessary, including to the police, local authority, safeguarding partners, legal advisers, insurers, regulators or courts. Each request must be verified, documented and approved by the responsible manager or Data Protection Officer. Where appropriate, third-party images or voices must be redacted before disclosure. Staff must not provide footage directly from a device to another person unless an emergency legal requirement applies and the disclosure is subsequently documented.

Individuals may request access to footage containing their personal data and may exercise other applicable UK GDPR rights. Requests must be passed promptly to the responsible manager or Data Protection Officer and handled within the statutory timescale. Rights may be limited where an exemption applies, including to protect other people, safeguarding activity, crime prevention or an ongoing investigation. Footage relevant to a request must be preserved while the request is being considered.

11.8 Training, supervision and misuse

Only trained and authorised staff may use body-worn cameras. Training will cover activation decisions, privacy, respectful communication, safeguarding, de-escalation, equipment security, incident reporting, evidence handling, disclosure and data subject rights. Compliance will be monitored through proportionate audits. Deliberate misuse, unauthorised disclosure or tampering may result in disciplinary action and, where appropriate, referral to the police or Information Commissioner's Office.

12. Legislative and Regulatory Framework

- Data Protection Act 2018 and UK GDPR

- Human Rights Act 1998

- Freedom of Information Act 2000 (where applicable)

- Equality Act 2010

- Building Safety Act 2022

- Worker Protection (Amendment of Equality Act 2010) Act 2023

- Renters' Rights Bill 2025

- Birmingham City Council Exempt Accommodation Standards (2023–25)

13. Monitoring and Review

This policy will be reviewed annually, or sooner following data breaches, legislative changes, inspection findings, complaints, audit results or any material change to body-worn camera technology or practice. The body-worn camera DPIA, retention arrangements and access logs will form part of the review. Lessons learned will be incorporated into revised procedures, privacy information and staff training.