DRAFT 1: 31 OCTOBER 2026

BATTERSEA REACH
RTM
COMPANY LIMITED

DATA PROTECTION & PRIVACY POLICY

Approved by:
Date adopted:
Next review date:
Policy owner:

DRAFT 1: 31 OCTOBER 2026

1. Purpose

Battersea Reach RTM Company Limited (the **Company**) is committed to protecting the privacy, confidentiality and security of personal information entrusted to it.

As a residential Right to Manage company, the Company may collect, hold and process personal information relating to leaseholders, residents, tenants, landlords, Directors, contractors and other individuals in connection with the management of Battersea Reach.

This Policy establishes the principles and procedures governing the collection, use, storage, disclosure and disposal of personal data.

The Company shall comply with applicable data protection legislation, including:

- the UK General Data Protection Regulation (UK GDPR);
- the Data Protection Act 2018, as amended;
- the Privacy and Electronic Communications Regulations 2003, where applicable; and
- other relevant statutory and regulatory requirements.

The Company recognises that responsible handling of personal information is essential to maintaining the trust and confidence of leaseholders and residents.

2. Scope

This Policy applies to all personal data processed by or on behalf of the Company, whether held electronically, in paper records or through third-party systems.

It applies to:

- all Directors and officers of the Company;
- employees and administrative personnel;
- managing agents acting on behalf of the Company;
- contractors and professional advisers with access to personal information; and
- other persons authorised to process personal data for Company purposes.

The Policy covers information relating to leaseholders, shared owners, residents, tenants, property owners, Directors, suppliers and other identifiable individuals.

3. Data Protection Principles

The Company shall observe the following fundamental principles.

3.1 Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and transparently. Individuals must be provided with appropriate information about how their data is used.

3.2 Purpose limitation

Personal information must be collected for specified, explicit and legitimate purposes and not subsequently used in an incompatible manner.

3.3 Data minimisation

Only personal information reasonably necessary for legitimate Company purposes shall be collected and processed.

3.4 Accuracy

Reasonable steps must be taken to ensure personal information is accurate and kept up to date.

3.5 Storage limitation

Personal data must not be retained for longer than necessary for the purposes for which it was collected, subject to legal and legitimate retention requirements.

3.6 Integrity and confidentiality

Personal information must be protected against unauthorised access, disclosure, alteration, loss or destruction through appropriate technical and organisational safeguards.

3.7 Accountability

The Company must be able to demonstrate compliance with its data protection obligations.

4. Categories of personal information

The Company may process the following categories of personal data where necessary and lawful:

Category	Examples
Identification	Names, titles and property ownership details
Contact details	Postal addresses, telephone numbers and email addresses
Property information	Apartment numbers, ownership and occupancy records
Financial information	Service charge accounts, payment records and arrears
Correspondence	Complaints, enquiries and communications
Governance information	Directors' details, membership records and declared interests
Building management	Access permissions, maintenance requests and incident records
Security information	CCTV footage and access-control records, where applicable
Legal information	Information relating to disputes, proceedings or enforcement matters

Special category personal data, such as health or disability information, shall be processed only where an additional lawful condition applies and appropriate safeguards are in place.

5. Purposes of Processing

The Company may process personal information for legitimate property management and corporate governance purposes, including:

- maintaining leaseholder, shared owner, resident and membership records;
- administering service charges and related financial matters;
- managing maintenance, repairs and building services;
- communicating with leaseholders, residents and property owners;
- managing contractors, suppliers and professional advisers;
- addressing complaints, disputes and enquiries;
- ensuring compliance with legal and regulatory obligations;
- managing building safety, security and emergency arrangements;
- conducting Board meetings, general meetings and Company administration; and
- establishing, exercising or defending legal claims.

Personal data must not be used for unrelated personal, commercial or political purposes.

6. Lawful basis for processing

The Company shall identify and document an appropriate lawful basis for each category of processing. Depending on the circumstances, these may include:

- legal obligation: processing necessary to comply with statutory requirements;
- legitimate interests: processing necessary for the Company's legitimate management and administrative interests, provided these are not overridden by individuals' rights and freedoms;
- contract: processing necessary for the performance of a contract with the relevant individual or to take steps at their request before entering into a contract;
- consent: processing based on freely given, specific, informed and unambiguous consent, where appropriate; and
- vital interests: processing necessary to protect someone's life.

The Company shall not assume that consent is required for all processing, nor that its statutory Right to Manage responsibilities automatically establish a legal obligation basis for every activity.

7. Responsibilities of Directors

Directors have collective responsibility for ensuring that the Company maintains appropriate data protection arrangements.

Each Director must:

- handle personal information responsibly and confidentially;
- access personal data only where necessary for legitimate Company purposes;

- avoid downloading, copying or circulating personal information unnecessarily;
- use secure methods of communication and document storage;
- ensure personal data is not disclosed to unauthorised persons;
- report suspected data breaches promptly; and
- comply with this Policy and applicable legal requirements.

Directors must not use personal information obtained through their position for private disputes, personal advantage or purposes unrelated to Company business.

8. Managing agents and third party processors

The Company may appoint managing agents and other service providers to process personal data on its behalf.

Where a service provider acts as a data processor, the Company shall ensure that an appropriate written agreement is in place meeting the requirements of Article 28 UK GDPR.

Such agreements should address:

- the nature and purpose of processing;
- confidentiality obligations;
- appropriate security measures;
- restrictions on subcontracting;
- assistance with data subject requests and breaches;
- retention and deletion of information; and
- audit and compliance arrangements.

The Company shall establish whether each third party acts as a processor, an independent controller or a joint controller, as appropriate.

The Board shall exercise reasonable oversight of data protection arrangements operated by its managing agents.

9. Confidentiality and information sharing

Personal information shall be disclosed only where there is a legitimate purpose and an appropriate lawful basis. The Company may share relevant information with:

- its appointed managing agents;
- contractors undertaking authorised works;
- accountants, auditors and legal advisers;
- insurers and insurance brokers;
- emergency services and public authorities; and
- landlords and other parties where disclosure is legally required or otherwise lawful.

Only the minimum information reasonably necessary should be disclosed.

The Company shall not routinely disclose leaseholders' private contact details to other residents or third parties without an appropriate lawful basis.

Statutory rights to inspect certain Company records or obtain information must be respected.

10. Email communications and distribution lists

The Company shall take particular care when communicating with groups of leaseholders or residents.

Directors and persons acting on behalf of the Company must:

- use approved mailing lists and communication systems;
- use blind carbon copy (BCC) or an appropriate secure mailing platform where recipients' email addresses should not be visible to one another;
- avoid unnecessarily including personal information in group communications;
- verify recipients before sending confidential documents;
- ensure mailing lists are maintained accurately; and
- respect applicable rules concerning electronic marketing and consent.

Personal email accounts should not be used for Company business unless appropriate security and governance safeguards have been approved.

11. Information security

The Company shall implement proportionate technical and organisational security measures. These should include:

- strong passwords and multifactor authentication where available;
- restricted access to confidential documents;
- secure electronic storage and appropriate backup arrangements;
- encryption where appropriate;
- secure disposal of obsolete records;
- appropriate safeguards for portable devices; and
- prompt removal of access when Directors or authorised personnel leave their roles.

Directors must not share passwords or permit unauthorised access to Company systems.

12. Retention and disposal of personal data

The Company shall retain personal information only for as long as necessary for legitimate business purposes or to meet applicable legal requirements.

A documented retention schedule should identify the relevant record categories, retention periods and reasons for retention.

Records may include financial documents, correspondence, contracts, membership information, service charge accounts and complaints.

Where information is no longer required, it shall be securely deleted, destroyed or anonymised.

The Company shall take reasonable steps to ensure that managing agents and other processors follow applicable retention and disposal requirements.

13. Individual rights

Individuals have rights under applicable data protection legislation, subject to relevant conditions and exemptions. These include:

- the right to be informed about processing;
- the right of access to their personal data;
- the right to rectification of inaccurate data;
- the right to erasure in certain circumstances;
- the right to restriction of processing;
- the right to data portability, where applicable;
- the right to object to certain processing; and
- rights relating to solely automated decisions with legal or similarly significant effects, where applicable.

Requests must be handled promptly and in accordance with statutory requirements.

14. Subject access requests

Individuals may submit a subject access request seeking access to personal information held about them. The Company shall:

- identify and record the request;
- verify identity where reasonably necessary;
- establish the scope of the request;
- identify relevant information held by the Company and its processors;
- consider applicable exemptions and the rights of third parties; and
- respond within the statutory deadline.

Requests must ordinarily be answered without undue delay and within one month, subject to permitted extensions or adjustments.

The Company shall not impose a routine fee for subject access requests.

15. Personal data breaches

A personal data breach may include accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Examples include:

- Sending confidential information to an incorrect recipient.
- Loss of a device containing personal information.
- Unauthorised access to leaseholder records.
- Cybersecurity incidents.
- Accidental disclosure of financial or personal details.

Any suspected breach must be reported promptly to the person designated by the Board to oversee data protection matters.

The Company shall assess the breach, take appropriate containment and remedial action, and document the incident.

Where a breach is likely to result in a risk to individuals' rights and freedoms, the Company must notify the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of it.

Where a breach is likely to result in a high risk to individuals' rights and freedoms, affected individuals must also be informed without undue delay, subject to applicable exceptions.

16. CCTV and building access systems

Where the Company determines the purposes and means of processing personal data through CCTV, entry systems or other security technologies, it shall ensure that:

- processing has an appropriate lawful basis;
- residents and visitors receive suitable privacy information;
- surveillance is necessary and proportionate;
- access to recordings and logs is restricted;
- retention periods are documented and justified; and
- requests for footage or access records are handled lawfully.

The Company shall establish whether responsibility for such systems rests with the Company, the landlord, a managing agent or another party.

17. International data transfers

Personal information shall not be transferred outside the United Kingdom unless applicable data protection requirements are satisfied.

Where necessary, the Company shall ensure that appropriate transfer mechanisms and safeguards are in place, including when using cloud-based systems or overseas service providers.

18. Privacy notices

The Company shall make an appropriate privacy notice available to individuals whose personal information it processes. The notice should explain:

- the Company's identity and contact details;
- the categories of personal information collected;
- the purposes and lawful bases of processing;
- recipients or categories of recipients;
- relevant international transfers;
- applicable retention periods or criteria;
- individuals' data protection rights;
- how to contact the Company about privacy concerns; and
- the right to complain to the Information Commissioner's Office.

The notice shall be reviewed whenever material changes occur in processing arrangements.

19. Complaints and concerns

Individuals who have concerns about the handling of their personal information should contact the Company through its designated data protection contact.

Complaints shall be considered fairly, promptly and confidentially.

Individuals also have the right to complain to the Information Commissioner's Office at www.ico.org.uk

20. Breaches of this policy

Failure to comply with this Policy may result in appropriate action, depending on the circumstances and the individual's relationship with the Company. Such action may include:

- additional guidance or training;
- restrictions on access to Company information;
- review or withdrawal of delegated responsibilities;
- contractual remedies against service providers; and
- referral to relevant regulatory or enforcement authorities.

Any action concerning a Director must comply with the Companies Act 2006, the Company's Articles of Association and other applicable legal requirements.

21. Review and amendment

The Board shall review this policy annually, or sooner where required by legislative changes, material changes in the Company's activities or identified governance concerns.

Amendments shall be approved by the Board and recorded in the minutes. Amendments so approved shall be posted to the Company's website within five business days and be put to the next general meeting for further approval. Where such general meeting does not approve such amendments, they shall be deemed to be abrogated from the date of such meeting.

22. Adoption

This policy was approved by resolution of the Board of Directors of the Company on [] 2027.

This policy was further approved by the general meeting of the Company on [] 2027