

DATA PROTECTION AND INFORMATION DISCLOSURE POLICY

Purpose

This policy explains how Richmond Estates Management Ltd collects, stores, uses, shares and protects personal information relating to applicants, occupants, guarantors, contractors and other individuals.

The organisation is committed to complying with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and all other applicable data protection legislation.

Organisation Memberships and Accreditations

Richmond Estates Management Ltd may hold memberships, accreditations or registrations with relevant professional, regulatory or industry bodies. Details of current memberships and accreditations can be recorded below:

- Membership/Accreditation Body: Information Commissioners Office
- Membership Number/Reference: ZA483561
- Expiry/Renewal Date: 15th May 2027

Data Controller

Richmond Estates Management Ltd is the Data Controller for the personal information it processes in connection with the management of its accommodation.

The organisation maintains registration with the Information Commissioner's Office (ICO) where required.

Personal Information Collected

The organisation may collect and process information including:

- Name, address, telephone number and email address;
- Date of birth;
- Proof of identity and right to rent documentation;
- Educational institution details;
- Financial and referencing information;
- Guarantor information;
- Tenancy and occupancy records;
- Correspondence and communication records;
- Emergency contact details;
- Maintenance and complaint records.

Lawful Basis for Processing

Personal information is processed only where a lawful basis exists, including:

- Performance of a contract;
- Compliance with a legal obligation;
- Legitimate interests;
- Protection of vital interests;
- Consent, where required.

The organisation will only process personal information that is necessary for the purpose for which it was collected.

Special Category and Sensitive Information

Special category data and other sensitive personal information will only be collected and processed where:

- there is a lawful basis to do so;
- it is necessary for the provision of services, safeguarding, health and safety or legal compliance;
- appropriate safeguards are in place.

Access to sensitive information is restricted to those who require it for legitimate business purposes.

Information Sharing and Disclosure

Personal information may be shared where necessary with:

- Educational institutions;
- Deposit protection schemes;
- Referencing providers;
- Maintenance contractors;
- Utility providers;
- Local authorities;
- Emergency services;
- Regulatory bodies;
- Legal advisers;
- Other organisations where disclosure is required by law.

Information will not be disclosed to third parties unless there is a lawful basis for doing so.

Where practicable and appropriate, occupants will be informed when sensitive personal information is disclosed.

Data Security

The organisation takes reasonable technical and organisational measures to protect personal information against:

- Unauthorised access;
- Loss;
- Misuse;

- Alteration;
- Disclosure;
- Destruction.

Personal information is stored securely and access is limited to authorised personnel.

Data Retention

Personal information will be retained only for as long as necessary to fulfil the purpose for which it was collected, comply with legal obligations, resolve disputes or enforce agreements.

Retention periods will be reviewed periodically.

Data Subject Rights

Individuals have rights under UK GDPR, including:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure where applicable;
- The right to restrict processing;
- The right to data portability where applicable;
- The right to object to processing;
- Rights relating to automated decision making.

Subject Access Requests

Individuals may request access to the personal information held about them.

Requests should be made in writing and will be responded to within the timescales required by applicable legislation.

Data Breaches

Any actual or suspected data breach will be investigated promptly.

Where required by law, breaches will be reported to the Information Commissioner's Office and affected individuals within the required timescales.

Staff Responsibilities

All staff and contractors handling personal information are expected to comply with this policy and any related procedures.

Failure to comply may result in disciplinary action and, where appropriate, legal action.

Review

This policy will be reviewed annually or sooner where required by changes in legislation, guidance or business operations.