PROPERTY MANAGEMENT
YOUR PROPERTY, OUR PROFESSION

General Data Protection Regulation Policy and Guidance

Introduction

We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes. This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated so that relevant compliance steps are addressed.

As a company we have a commitment to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all legal obligations.

JCF Property Management Ltd is registered with the information Commissioner Office (ICO) (registration reference Z3533803)

Definitions

Business Purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. Business purposes include the following: - • Compliance with our legal, regulatory and corporate governance obligations and good practice; • Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests; • Ensuring business policies are adhered to (such as policies covering email and internet use); • Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking; • Investigating complaints; • Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments; • Monitoring staff conduct, disciplinary matters; • Marketing our business - Improving services

Personal data	'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data we gather may include: individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV
Special categories of personal data	Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information — any use of special categories of personal data should be strictly controlled in accordance with this policy.
Data controller	'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.
Data processor	'Data Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data Processing	'Data Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
Supervisory authority	This is the national body responsible for data protection. The supervisory authority for JCF Property Management Ltd is the Information Commissioners Office.

.

Scope

This policy applies to all employees, contractors and third party service providers working on behalf of JCF who must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use and the staff handbook. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for data protection ?

The Data Protection Officer (DPO)

The DPO has overall responsibility for the day-to-day implementation of this policy. You should contact the DPO for further information about this policy if necessary.

Stewart White *MRICS*
JCF Property Management Ltd
322 Upper Richmond Road
London SW15 6TL
Tel: 020 8785 9700
E-Mail: stewart.white@jcfpropertymanagement.com

Employees, Contractors and other Third Party Service Providers

All employees, contractors and third party service providers are required to understand this policy and comply with it at all times.

The Principles

JCF Property Management Ltd will comply with the principles of data protection regulations ("The Principles") set out in the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR). We will make every effort possible in everything we do to comply with the principles which are:-

1. Data is processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Data is obtained for specified, explicit and legitimate purposes.
3. Data collected will be adequate, relevant and limited to what is necessary.
4. The data held will be accurate and up to date.
5. The data will not be kept any longer than necessary for the purposes for which the data is being processed.
6. The data will be stored securely.

Lawful Bases for Processing Data

We process personal data based on one or more of the following lawful grounds:-

- Performance of a contract (i.e. the lease / TP1 and the management agreement)
- Compliance with legal obligations
- Legitimate interests of the company or stakeholders
- Consent

The Data we Process

We process the following categories of personal data:

- Full names, contact details (email, phone, address)
- Property ownership or tenancy information
- Payment and service charge information
- Correspondence records (emails, letters, calls)
- CCTV footage (where installed)
- Employee and contractor details (where applicable)

Rights of Individuals

Individuals (known as data subjects) have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

1. **Right to be informed**
   - We provide a privacy notice which is concise, transparent, intelligible and easily accessible, free of charge, explaining the data we collect and how we use this data.
   - We keep records of how we use personal data to demonstrate compliance with the need for accountability and transparency.
2. **Right of access**
   - We will enable data subjects to access their personal data and any supplementary information held about them.
   - We ensure data subjects are aware of the lawfulness of the processing activities which is in the performance of a contract.
3. **Right to rectification**
   - We will rectify or amend the personal data of the data subject if requested because it is inaccurate or incomplete. This must be done without delay, and no later than one month following receipt of the request. (This can be extended to two months with permission from the DPO).
4. **Right to erasure**
   - We must delete or remove a data subject's data if requested and there is no compelling reason for its continued processing.
5. **Right to restrict processing**
   - We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
   - We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.
6. **Right to data portability**
   - We must provide data subjects with their data so that they can reuse it for their own purposes or across different services.
   - We must provide it in a commonly used, machine-readable format, and send it directly to another data controller if requested.
7. **Right to object**
   - We must respect the right of a data subjects to object to data processing based on legitimate interest or the performance of a public interest task.
   - We must respect the right of a data subjects to object to direct marketing, including profiling.
   - We must respect the right of data subjects to object to processing their data for scientific and historical research and statistics.
8. **Rights in relation to automated decision making and profiling**
   - We must respect the rights of data subjects in relation to automated decision making and profiling.
   - Data subjects retain their right to object to such automated processing, have the rationale explained to them, and request human intervention

Data Sharing

Personal data may be shared with the following parties in line with our privacy notice

- Resident Management Company Directors and Freeholders
- Contractors and service providers
- Insurance brokers and underwriters
- Solicitors and debt recovery firms
- Government authorities or regulators (including the Police, HMRC and local authorities)
- Managing Agents during handover with the written instruction of the client and confirmation of their ICO registration.

Personal data may be shared with other property owners, leaseholders and residents **only** with the express permission of the data subject which should be obtained in writing where possible.

Data Security

We implement technical and organisational measures to ensure data security
Examples:

- Checking the identity of data subject before disclosing any personal data
- Use of encrypted storage and secure cloud platforms
- Password protection and access control for digital files
- Secure physical storage for paper records
- Staff training on data protection and IT security

Data Retention

We keep personal data only as long as necessary for the purposes for which it was collected.
Examples:

- Financial records: 6 years (statutory)
- Service charge records: 6–12 years (based on lease terms)
- Tenancy and ownership records: up to 12 years
- CCTV footage: typically 30–90 days (subject to policy)

Any data that is not necessary for the purposes for which it is collected should be routinely deleted.

Data Breaches

All suspected data breaches must be reported immediately to the DPO.

Where a breach poses a risk to data subjects' **rights and freedoms**, it will be reported to the ICO within 72 hours. Examples of this type of breach include:

Risk Category	Example Scenario	Risk to Data Subject
Identity Theft	Bank and NI data leaked during cyberattack	Financial loss, credit damage, legal complications
Personal Safety	Address of vulnerable resident (e.g., abuse survivor) disclosed	Risk of physical harm or stalking, right to security compromised

Risk Category	Example Scenario	Risk to Data Subject
Harassment / Scams	Contact details leaked to third parties	Phishing attacks, psychological distress, potential financial loss
Reputational Harm	Service charge arrears or dispute records published online	Stigmatization among neighbours, damage to reputation and relationships
Discrimination	Equality data (e.g., ethnicity, religion, disability) exposed	Unlawful discriminatory treatment, infringement of equality rights
Suppression of Legal Rights	Involvement in legal complaints or RTM activities revealed	Retaliation or pressure, reduced willingness to assert legal rights
Intrusion into Family Life	Household/family member data leaked	Breach of privacy, unwanted contact, exposure of minors

Where the data breach is not likely to result in a risk to data subjects' rights and freedoms there is no requirement to notify the ICO or the data subjects concerned.

In the event of a data breach the DPO will determine the action to be taken and who should carry out such action. This may include informing the client of the breach, advising data subjects of the breach, making a full apology to the data subjects affected and/or requesting that the recipients of the data delete the information.

Following a breach the DPO will document in the data breach incident log and discuss with any employees involved what caused the breach and what to be aware of to avoid a repetition. Any proposed changes to procedure will be implemented as soon as possible.

Subject Access Requests (SAR)

A data subject has the right to receive a copy of any information we hold about them free of charge. This mut be sent to them without delay and within one month of receipt of the request. The DPO must be informed of any SAR immediately.

In order to minimise the work in providing information following a SAR it is recommended that only essential emails are saved in the tenant folder on the shared drive and reports or correspondence can be run from MRI Qube or accessed by the data subject by logging into the Engage portal. All data that is no longer required should be deleted.

Training and Awareness

All staff will receive training about data protection procedures as part of their induction when joining JCF Property Management Ltd and receive regular training or reminders of procedure as necessary.

Monitoring and Review

This policy was last reviewed in June 2025 and will be reviewed every 2 years or sooner if required due to changes in legislation, guidance or business practices.