# Data Protection & Records Management Policy

## Contents

## Policy Version

- Policy Prepared by the JVL Estate Manager & Company Secretary
- Approved by JVL Management Committee 25th May 2018
- Policy became operational on 25th May 2018
- Next Review Date TBA
- Draft Version 1.0

# Introduction

Jordans Village Limited ("The Society") needs to gather and use certain information about individuals ("Data Subjects").

These Data Subjects include residents, tenants, committee members, shareholders, suppliers, business contacts, employees and other people the Society has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled, and stored to meet The Society's data protection standards – and to comply with the law.

## Glossary

| | |
|---|---|
| Chairman | The Chairman of Jordans Village Limited Management Committee |
| Committee Members | Members of the Jordans Village Limited Management Committee |
| Data Subjects | Individual persons |
| JVL | Jordans Village Limited |
| Members | Shareholders of Jordans Village Limited |
| Partners | Companies, Suppliers, and Contractors providing goods or services to JVL |
| Residents | All those living on Jordans Village land and the wider community of Jordans |
| Staff | The Estate Manager and JVL Management Committee Members |
| Tenants | Tenants of properties owned by JVL |
| The Society | Jordans Village Limited (JVL) |
| Treasurer | The appointed Treasurer of Jordans Village Limited |
| Vice-Chairman | The Vice-Chairman of Jordans Village Limited Management Committee |

## Why this policy exists

This data protection policy ensures that The Society:

- Complies with data protection law and follows good practice
- Protects the rights of staff, residents, and partners,
- Is open about how it stores and processes individuals' data
- Protects itself from the risk of a data breach

## Data Protection Law

The Data Protection Act 1988 describes how organisations – including The Society – must collect, handle, and store personal information.

These rules apply regardless of whether the data is stored electronically or physically (on paper or on other materials).

To comply with the law, personal information must be collected and used fairly, stored safely, and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant, and not excessive
4. Be accurate and kept up to date
5. Not be held for longer than necessary
6. Be processed in accordance with the rights of Data Subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA) unless that country or territory also ensures an adequate level of protection

# People, Risks, & Responsibilities

## Policy Scope

This policy applies to

- The Jordans Village Estate Office;
- All staff, committee members, and volunteers of Jordans Village Limited;
- All contractors, suppliers, and other people working for or on behalf of Jordans Village Limited.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1988. This can include:

- Names of individuals;
- Postal addresses;
- Email addresses;
- Telephone numbers;
- Historic correspondence;

- …and any other information relating to individuals.

## Data Protection Risks

This policy helps to protect Jordans Village Limited from some very real data security risks, including:

- Breaches of Confidentiality
    - For instance, information being given out inappropriately
- Failing to offer choice
    - For instance, all individuals should be free to choose how the company uses data relating to them
- Reputational Damage
    - For instance, the company could suffer if hackers successfully gained access to sensitive data

## Responsibilities

Everyone who works for The Society has some responsibility for ensuring that data is collected, stored, and handled appropriately.

Each Committee, Sub-Committee, group, contractor, volunteer, or team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

**The Management Committee is ultimately responsible for ensuring that The Society meets its legal obligations.** They are also responsible for:

- Approving any data protection statements attached to communications such as emails and letters;
- Addressing any data protection queries from journalists or media outlets such as newspapers;

**The Estate Manager & Company Secretary is also designated as the Data Protection Officer for The Society. He is responsible for:**

- Keeping the Management Committee updated about data protection responsibilities, risks, and issues;
- Reviewing all data protection procedures and policies, in line with an agreed schedule;
- Arranging data protection training and advice for the people covered by this policy;
- Handling data protection queries from anyone else covered by this policy;
- Dealing with requests from individuals to see the data which The Society holds about them (Also called “Subject Access Requests”);
- Checking and approving any contracts or agreements with third parties that may handle The Society’s sensitive data;
- Ensuring that all systems, services, and equipment used for storing data meet acceptable security standards;

- Performing regular checks and scans to ensure security hardware and software is functioning properly;
- Evaluating third party services The Society is considering using to store or process data, for instance cloud computing services;
- Where necessary, working with committee members, volunteers, or other partners to ensure that marketing & communication initiatives abide by data protection principles.

## General Staff Guidelines

- The only people able to access data covered by this policy must be those who **need it for their work.**
- **Data should not be shared informally**. When access to confidential information is required, committee members can request it from the Chairman or via the Estate Manager.
- The Society **will provide guidance and/or training** to all Committee Members to help them understand their responsibilities when handling data.
- Committee Members and the Estate Manager must keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Committee Members **should request help** from the Estate Manager if they are unsure about any aspect of data protection.

## Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Estate Manager.

These guidelines also apply to data that is stored electronically but has been printed out for some reason.

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Paper records should be kept in a secure place where unauthorised people cannot see it, i.e. **not left on a printer or in a publicly accessible area**.
- **Data printouts should be shredded** and securely disposed of when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between Committee Members.
- If data is **stored on removable media** (like a memory stick, CD, DVD, or hard drive), these should be kept locked away securely.

- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing service or services**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly to personal laptops** or other mobile devices such as tablets or mobile phones, with the exception of the Estate Office laptop.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

## Data Use

Personal data is of no value to Jordans Village Limited unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption, or theft.

- When working with personal data, the Estate Manager and Committee Members should ensure that the **screens of their computers are locked when left unattended**.
- Personal data should not be shared informally.
- Data should be **encrypted before being transferred electronically**.
- Personal Data should **not be transferred outside of the European Economic Area**.
- Staff **should not save copies of personal data to their own computers**.

## Data Accuracy

The law requires The Society to take reasonable steps to ensure that data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort that The Society should put into ensuring its accuracy.

It is the responsibility of the Estate Manager and all Committee Members who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be **held in as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure that data is updated**. For instance, by confirming a resident's details when they call.
- The Society will make it **easy for Data Subjects to update the information** that The Society holds about them. For instance, by contacting the Estate Office.
- Data should be **updated as inaccuracies are discovered**. For instance, if a resident can no longer be reached on a stored telephone number, it should be removed from the database.

## Subject Access Requests

Under the GDPR, all individuals who are subject of personal data held by The Society are entitled to:

- Ask what information The Society holds about them and why;

- Ask how to gain access to it;
- The right to rectify inaccurate data;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling;
- Be informed how The Society is meeting its data protection obligations.

And, in some circumstances:

- the right to erase;
- the right to restrict processing

## Subject Access Request Process

If an individual contacts The Society requesting information about themselves, this is called a Subject Access Request. Subject Access Requests from individuals should be made by email, addressed to the Estate manager at estateoffice@jordansvillage.co.uk .

Upon receipt of a formal request for data, JVL would

i. Validate the identity of the person making the request.
ii. Verify that it is obliged to provide the data requested
iii. Note the deadline for responding, usually on the corresponding date of the following month, so between 28-31 days.
    a. The Estate Manager will aim to provide the relevant data within 14 days, but in any case, will usually be within 40 days from the date of the request.
iv. If the enquiry is particularly complex, the deadline may be longer; this must be communicated to the applicant.
v. Confirm that data is processed if the first two tests are passed.
vi. Request an email address from the data subject for receiving such information. Alternatively, information may be provided on a password-protected memory stick if the recipient pays a small fee (currently £10) for the cost of providing such hardware.
vii. If our personal data requires rectification following an enquiry, this will be made without undue delay.
viii. If a data subject objects to JVL holding their personal data, they should put their complaint in writing. The objection will be investigated and reviewed by the Committee before JVL responds.

## In what format would we provide data?

Data would be provided in the same format & software as which they are created.

## How would we delete data?

JVL retains all correspondence relating to each property, its shareholders, and waiting lists so as to create an historic archive of the community. This is an exemption provided for within GDPR.

## Disclosing Data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the Data Subject.

Under these circumstances, The Society will disclose requested data. However, the Estate Manager will ensure that the request is legitimate, seeking assistance from the Management Committee and the Society's legal advisors where necessary.

## Providing Information

The Society aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How their data is being used
- How to exercise their rights

To these ends, The Society has a Privacy Statement setting out how the data relating to individuals is being used by The Society.

Our Privacy Policy is available on request, or via the downloads page of our website www.jordansvillage.co.uk

## Lawful basis for processing personal data

The lawful basis for processing activity within JVL is "Legitimate interests".

The lawful basis for processing Shareholder data within JVL is "Legal obligation".

## Records Management - Personal Data

### What personal data does JVL hold?

a. **Shareholders**: Names, Addresses, Home & Mobile Telephone Numbers, Email Addresses, Historic Correspondence (Physical & Electronic)
b. **Loan Stock Holders**: Names, Addresses, Home & Mobile Telephone Numbers, Email Addresses, Bank Details, Historic Correspondence (Physical & Electronic)
c. **Tenants**: Names, Addresses, Dates of Birth, Names of Children, Home & Mobile Telephone Numbers, Email Addresses, Historic Correspondence (Physical & Electronic)
d. **Waiting List Applicants**: Names, Addresses, Dates of Birth, Names of Children, Children's Dates of Birth, Home & Mobile Telephone Numbers, Email Addresses, Historic Correspondence (Physical & Electronic)
e. **Other Residents**: Names, Addresses, Home & Mobile Telephone Numbers, Email Addresses, Historic Correspondence (Physical & Electronic)
f. **Contractors & Suppliers**: Names, Addresses, Work & Mobile Telephone Numbers, Email Addresses, Company Number, Accreditations, Company Insurance details, Historic Correspondence (Physical & Electronic)
g. **Committee Members**: Name, Spouse Name, Address, Date of Birth, Length of time living in property, Work & Mobile Telephone Numbers, Email Addresses, details of a Business

Interests or Directorship of any Company, details of Spouse Business Interests or Directorship of any Company, Historic Correspondence (Physical & Electronic)

## What types of data does JVL hold?

a. **Physical Data**: JVL holds physical data in the form of paper records in the Estate Office & some records will also be held by our Solicitors.
b. **Electronic Data**: Held in our computer systems, in hard drive back-ups, and in the iDrive cloud back up. This data can be accessed by the Estate Manager, the Chairman, and the FS-C Chairman.
c. **Telephone Data**: Telephone calls are not recorded. Voicemails are recorded, and deleted periodically.
d. **Special Category Data:** includes (but is not limited to) information about an individual's race, ethnic origin politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation. Data held by JVL would typically be (but not limited to) information about the data subject's health or financial position, or criminal record. This data is held in electronic and physical form, in a separate file to other types of data.

## Where did it come from?

a. **Shareholders**: From data subjects themselves.
b. **Loan Stock Holders**: From data subjects themselves.
c. **Tenants**: As supplied by tenant through administration of their contract.
d. **Waiting List Applicants**: From data subjects themselves.
e. **Other Residents**: From surveys of residents, with their consent.
f. **Contractors & Suppliers**: From the contractors themselves.
g. **Committee Members**: from the Member themselves.
h. **Special Category Data**: may be held where the data subject or their legally appointed representative has given explicit consent to the processing of such personal data for one or more specified purposes, and where processing is necessary to protect the vital interests of the data subject, or for the legitimate purpose relating to the administration of our business. We require that those providing data voluntarily sign & complete a Special Category Data Consent Form at the time it is provided.

## Who do we share it with?

a. **Shareholder Data** is not shared with anyone other than JVL Committee Chairman & Finance Sub-Committee Chairman.
b. **Loan Stock Holders Data** is not shared with anyone other than JVL Committee Chairman & Finance Sub-Committee Chairman.
c. **Tenants Data** is not shared with anyone other than Committee Members. Limited Data may be published in the Village Directory and shared with our Contractors & Suppliers (Name, Address, Telephone Number).
d. **Waiting List Applicants Data** is not shared with anyone other than Committee Members.

e. **Other Residents**: Data is not shared with anyone other than The Chairman & Finance Sub-Committee Chairman. Limited Data may be shared in the Village Directory, and with our Contractors & Suppliers (Name, Address, Telephone Number).
f. **Contractors Data** is not shared with anyone other than Committee Members. Limited Data may be shared with Residents and Tenants (Name, Address, Telephone Number, Email Addresses).
g. **Committee Members data** is shared with our Auditor, and the Financial Conduct Authority.
h. **Special Category Data** is shared with the JVL Company Secretary, Chairman, Vice-Chairman, & Treasurer; JVL's Legal Representatives; and any other persons so nominated by the person providing the data via the Special Category Data Consent Form.
i. **Personal data** may be shared with our Solicitor, with our Book Keeper, and with our Auditor as is required for the normal course of running our business.

## Children

JVL only holds minimal data on Children (Name & Data of Birth) where parental consent has been given to hold such data.

## How do we seek, record, and manage consent?

When people apply to become a **shareholder**, or to join a **waiting list**, they consent to giving the data required so that we can administer our business by signature on the appropriate application form.

**Private Residents** moving in to their own property within the Village give their personal information to JVL either via their solicitor, or voluntarily.

Those giving **Special Category Data** voluntarily are also asked to sign a consent form specifying what kind of information they are providing and who may have access to it.

# Data breaches

The GDPR introduces a duty on all organisations to report certain types of personal data breaches to the ICO and, in some cases, to the individuals affected.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

## What is our process for detecting, reporting, & investigating personal data breaches?

i. Once a year the Chairman, Treasurer, or Vice Chairman may ask to check records held by JVL so that compliance with policy can be demonstrated.
ii. If a breach is found, then The Chairman will appoint a member of the Management Committee who is un-conflicted with the person or persons concerned by the data breach (if applicable). That Appointed Person will investigate the breach together with The Secretary.
iii. If the Chairman is conflicted, then the Vice-Chairman will take on the process of Appointment.

iv. The Secretary and Appointed Person will report back as to the cause & nature of the breach, and the steps taken to rectify the breach and avoid any re-occurrence.
v. The Chairman will then decide on the course of action to take.
vi. The ICO will be notified if it is appropriate or necessary to do so.
    a. The ICO only needs to be notified of a breach where it is likely to result in a risk to the rights and freedoms of individuals.
    b. A notifiable breach has to be reported to the ICO within 72 hours of the business becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide additional information in phases. You should make sure that your staff understand what constitutes a personal data breach, and that this is more than a loss of personal data.
vii. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly and without undue delay.
viii. In all cases you must maintain records of personal data breaches, whether or not they were notifiable to the ICO.