Streetfield Mews
GDPR Data Protection and Data Breach Policy

Date of Committee Approval:	1 February 2021
Date of Issue:	2 February 2021
Date of Next Review:	1 February 2023

1. Introduction

1.1 Streetfield Residents Society Limited (the **Company**) is required to keep and process certain information about its shareholders and the residents (each being **Data Subjects**) of Streetfield Mews, London SE3 0ER (**Streetfield Mews**).

1.2 This policy is in place to ensure that Directors of the Company are aware of their responsibilities and outlines how the Company complies with the core principles of the General Data Protection Regulation (**GDPR**).

2. Applicable Data

2.1 The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier. A wide range of personal identifiers constitute personal data, including name, identification number, location data or online identifier.

2.2 The GDPR refers to sensitive personal data as "special categories of personal data". The following categories of data are included in this definition: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

3. Principles

The GDPR sets out the following data protection principles:

(a) data will be processed lawfully, fairly and in a transparent manner;
(b) data is collected for specified, explicit and legitimate purposes and not processed further in a manner incompatible with those purposes;
(c) data is adequate, relevant and limited to what is necessary for the purpose collected;
(d) data is accurate and kept up to date and that inaccurate data is erased without delay;
(e) data is kept in a form which permits identification of Data Subjects for no longer than is necessary for the purpose for which the data is processed;
(f) data is processed in a manner which ensures appropriate security of the data, including protection against unauthorised/unlawful processing and against accidental loss, destruction or damage.

4. Accountability & Governance

The Company will maintain a register of data processing activities which will be reviewed on an annual basis. The register will include the following:

(a) categories of personal data held;
(b) purpose of data processing;
(c) legal basis for data collection;
(d) security measures in respect of the data;
(e) details of data transfers to third parties/countries;
(f) retention period.

5. Data Protection Officer (DPO)

The Company has appointed a Data Protection Officer (**DPO**) to monitor compliance with the GDPR and other laws.

6. Lawful Processing

6.1 The legal basis for processing data must be identified and documented prior to data being processed. In line with the requirements of Article 6 of the GDPR data processing will be lawful when the consent of the Data Subject has been obtained and when processing is necessary for one or more of the following reasons:

(a) compliance with a legal obligation;
(b) the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(c) for the performance of a contract with the Data Subject or to take steps to enter into a contract;
(d) protecting the vital interests of a Data Subject or another person;

(e) for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the Data Subject.

7. Consent

7.1 Consent can be withdrawn by a Data Subject at any time.

7.2 Where a child is aged under 16 the consent of parents will be sought prior to the processing of their data.

8. Rights of the Individual

The GDPR provides individuals with a number of rights in respect of how their personal data is processed:

The right to be informed:

Privacy notices provided in respect of data processing will be in clear plain language and accessible and will detail the identity and contact details of the controller and the DPO.

Privacy notices will set out the legal basis for processing the data and the legitimate interests of the controller. The rights of the Data Subject will also be detailed. The legal basis for holding the data and retention requirements will also be included.

The right of access

Data Subjects will have the right to submit a subject access request (**SAR**) to gain access to their personal data. In the first instance information will be supplied without charge, however, the Company will reserve the right to impose a 'reasonable fee' for further requests for the same information.

All requests for data will be responded to within one month of receipt of the request, unless the request is complex in which case an extension of one month may be applied. The Company reserves the right to refuse unfounded or excessive requests.

The right to rectification

Data Subjects will be entitled to have any inaccurate or incomplete data rectified. Where the personal data has been disclosed to a third party the Company will inform them of the rectification if possible. Requests for rectification will be responded to within one month or two months where a request is deemed to be complex.

The right to erasure

Data Subjects will have the right to request the deletion of their data where there is no compelling reason for its continued processing. The right to request erasure will also apply where a Data Subject withdraws their consent or when personal data has been unlawfully processed. The Company has the right to refuse a request for erasure for the following reasons:

(a) to exercise the right of freedom of expression and information;
(b) to comply with a legal obligation for the performance of a public interest task or exercise of official authority;
(c) for public health purposes in the public interest;
(d) for archiving purposes in the public interest; or
(e) the exercise or defence of legal claims.

Where personal data has been made public within an online environment, the Company will inform other organisations who process the data to erase links to and copies of the data.

The right to restrict processing

Data Subjects have the right stop or restrict the processing of their personal data. In the event that processing is restricted the Company will store the personal data but not further process it.

The Company will restrict the processing of personal data in the following circumstances where:

(a) a Data Subject contests the accuracy of the personal data, processing will be restricted until the Company has verified the accuracy of the data;

(b) a Data Subject has objected to the processing and the Company is considering whether their legitimate grounds override those of the individual;
(c) processing is unlawful and the individual opposes erasure and requests restriction instead;
(d) the Company no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

If the personal data has been disclosed to a third party the Company will inform them about the restriction on the processing of the personal data.

The right to data portability
Data Subjects have the right to obtain and reuse their personal data across different services. Personal data may be moved, copied or transferred from one IT environment to another in a secure manner, in a structured, commonly used and machine readable format.

Data Portability
The right to data portability will apply in the following cases:
(a) to personal data that a Data Subject has provided to a controller;
(b) where the processing is based on the Data Subject's consent or for the performance of a contract;
(c) when processing is carried out by automated means.

The Company is not required to adopt or maintain processing systems which are technically compatible with other organisations. The Company will respond to requests for portability within one month. In the event that the request is complex the timescale may be extended by two months.

The Right to Object
The Company will inform Data Subjects of their right to object. This information will be included in privacy notices.

Data Subjects have the right to object to the following:
(a) processing based on legitimate interests or the performance of a task in the public interest;
(b) direct marketing;
(c) processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:
(a) a Data Subject's grounds for objecting must relate to his or her particular situation;
(b) the Company will stop processing the Data Subject's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Company can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Automated decision making and profiling
Data Subjects have the right not to be subject to a decision when it is based on automated processing.

9. Data Security

9.1 Confidential paper records will be kept in a locked filing cabinet, drawer or safe with restricted access. Paper records will not be left unattended anywhere with general access.

9.2 Digital data will be coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off site.

9.3 Where data is saved on removable storage or a portable device the device will be kept in a locked filing cabinet, drawer or safe when not in use.

9.4 Emails containing sensitive or confidential information are password protected if there are unsecure servers between the sender and the recipient.

9.5 Circular emails to shareholders will be sent blind carbon copy (bcc) so that email addresses are not disclosed to other recipients.

9.6 Where personal data that could be considered private or confidential is taken off premises, either in electronic or paper format, the Company Directors will take extra care to follow procedures for security. The person taking the information accepts full responsibility for the security of the data.

9.7 Before sharing data the Company Directors will ensure:
(a) they are allowed to share it;
(b) that adequate security is in place to protect it; and
(c) the recipient of the data is detailed in the privacy notice.

10. Data Breaches

10.1 A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. This includes breaches that are the result of either accidental or deliberate causes.

10.2 Where a breach is likely to result in a 'risk' to the rights and freedoms of individuals the relevant supervisory authority will be informed within 72 hours of the Company becoming aware of the breach.

10.3 In the event that a breach is likely to result in a 'high risk' to the rights and freedoms of a Data Subject, the Company will notify the subject(s) of the data breach without undue delay.

10.4 Within a breach notification, the following information will be outlined:
(a) the nature of the personal data breach, including the categories and approximate number of individuals and records concerned;
(b) the name and contact details of the DPO;
(c) an explanation of the likely consequences of the personal data breach;
(d) a description of the proposed measures to be taken to deal with the personal data breach;
(e) where appropriate, a description of the measures taken to mitigate any possible adverse effects.

10.5 The Company will ensure that Directors are aware of and understand what constitutes a data breach and the action they should take in the event that they become aware of a breach.

10.6 Following a breach a meeting will be convened by the DPO and the Company Directors to review the breach, the process followed and agree measures to mitigate future breaches.

10.7 The data breach procedure is attached at Appendix 1 of this document.

11. Recorded Images and Photography

11.1 The Company acknowledges that recording images of identifiable individuals constitutes processing personal data. Processing of this type of data will be managed in line with the principles of the GDPR.

11.2 The Company will notify shareholders of the purpose for collecting images via its website, announcements and email.

11.3 Images captured by individuals for recreational/personal purposes are exempt from the GDPR.

12. Data Retention & Disposal

12.1 Data will not be kept for longer than is necessary and timescales for the retention of documents is set out in the Streetfield Mews Information And Documentation Retention Schedule (see website).

12.2 Paper documents will be disposed of securely and electronic data deleted, once the data should no longer be retained.

13. Privacy Notice

The form of Privacy Notice for the Company is contained in Appendix 2.

Appendix 1
Personal Data Breach Procedure

On being notified of, or finding or causing a breach, or potential breach, the Directors or data processor must immediately notify the Company's Data Protection Officer (**DPO**).

The DPO will investigate the report, and determine whether a breach has occurred.

The DPO will consider whether personal data has been accidentally or unlawfully:
(a) lost;
(b) stolen;
(c) destroyed;
(d) altered;
(e) disclosed or made available where it should not have been; or
(f) made available to unauthorised people.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by the Directors of the Company.

The DPO will determine if the breach must be reported to the Information Commissioners Office (**ICO**). This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
(a) loss of control over their data;
(b) discrimination;
(c) identify theft or fraud;
(d) financial loss;
(e) unauthorised reversal of pseudonymisation (for example, key-coding);
(f) damage to reputation;
(g) loss of confidentiality; or
(h) any other significant economic or social disadvantage to the individual(s) concerned.

If it's likely that there will be a risk to people's rights and freedoms, the DPO will notify the ICO within 72 hours of the breach.

The DPO will document the decision, in case of challenge at a later date by the ICO or an individual affected by the breach. The DPO will maintain a register of all data breaches and reports to the Individual, subject to the breach and the ICO.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
(a) a description of the nature of the personal data breach including, where possible;
    (i) the categories and approximate number of individuals concerned;
    (ii) the categories and approximate number of personal data records concerned;
(b) the name and contact details of the DPO;
(c) a description of the likely consequences of the personal data breach; and
(d) a description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
(a) the name and contact details of the DPO;
(b) a description of the likely consequences of the personal data breach; and
(c) a description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

The DPO will notify any relevant third parties who can help mitigate the loss to individuals.

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

(a) facts and cause;
(b) effects; and
(c) action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

Following a data breach and as soon as is practicable a meeting will be convened by the DPO and relevant staff to review the reason for the breach, and agree measures to mitigate future breaches.

Appendix 2
Form of Privacy Notice

STREETFIELD RESIDENTS SOCIETY LIMITED
PRIVACY NOTICE

Introduction
Streetfield Residents Society Limited (the **Company**) is a company registered in England and Wales with company number 1746097 and whose registered office is 18 Streetfield Mews, Blackheath SE3 0ER. The Company owns and operates the website www.steetfieldmews.weebly.com

In this Privacy Notice, references to **you** or **your** are to any person who submits data to the Company about themselves or on behalf of someone else.

Notice Assurance
This Privacy Notice (together with any other the Company contractual terms and conditions, and any other documents referred to in them) sets out the basis on which any personal data the Company collects from you, or that you provide to the Company, will be processed by the Company. Please read this Privacy Notice carefully to understand the Company's views and practices regarding your personal data and how the Company will treat it.

The Company only use your personal data in the manner set out in this Privacy Notice. The Company will only use your personal data where it is necessary for the Company to do so and where it is relevant to its dealings with you. The Company will only keep your personal data for as long as it is relevant to the purpose for which it was collected or for as long as the Company are required to keep it by law. A copy of its Information and Documentation Retention Schedule is contained on the Company's website.

Personal Data
The Company will only use personal data for the following purposes:
(a) to inform you of news, events, activities, meetings and services connected with Streetfield Mews;
(b) to manage events, meetings, rotas and volunteers for the benefit of shareholders and residents of Streetfield Mews;
(c) to administer the shareholder and resident records;
(d) to provide a contact directory for shareholders and residents which enables them to communicate with each other easily;
(e) to fundraise and promote the Company interests, those of any collaborative partners and associated organisations;
(f) to maintain the Company accounts and records;
(g) to comply with its obligations to maintain records and registers, including but not limited to Companies House; and
(h) to manage relationships with outside users and suppliers.

Legal Basis:
In processing personal data the Company rely on the following legal bases:
(a) processing as necessary for contractual obligations;
(b) explicit consent is provided by the data subject.

The Company shall not sell or disclose your personal data to third parties without obtaining your prior consent, unless it is necessary for the purposes set out in this Privacy Notice or unless the Company are required to do so by law.

You should only submit information to the Company which is accurate and not misleading. You should keep that information up to date and let the Company know as soon as possible of any changes to that information in writing to streetfieldmews@gmail.com

By submitting your or anyone else's data to the Company, you must ensure that you have full authority and consent to supply that data on their behalf. You warrant to the Company that you have such authority.

The Company advise that you have the right to access your data, have your data amended to remove errors, to withdraw your consent for some or all processing which is based upon consent, and to have such records deleted. For these purposes you may contact the Company data controller by writing to the Company's registered office or by email to streetfieldmews@gmail.com.

You further have the right to lodge any complaint regarding the handling of your data subject access request with the supervisory authority, the Information Commissioner's Office. See www.ico.org.uk

Any correspondence with the Company will be recorded.

Any changes to this Privacy Notice in the future will be posted on the Company website, in the Company contractual terms and, where appropriate, notified to you by email.

This Privacy Notice was last updated on [DATE].