



Sentinel Lettings

Privacy and Digital Media Policy

Agency Details

Tu Nguyen Management Limited,
trading as Sentinel Lettings
c/o Benison Solvers Limited
1000 Great West Road
Brentford
Middlesex
United Kingdom
TW8 9DW

DOCUMENT AUTHOR:	Quoc Thanh Vo
DOCUMENT OWNER:	Dinh Tu Nguyen
STATUS:	Final
DATE CREATED:	10/01/2025
VERSION:	2
LAST UPDATED:	14/09/2026
SECURITY CLASSIFICATION:	Low



SENTINEL

LETTINGS

Revision History

VERSION	REVISION DATE	SECTION REVISED	REASON FOR REVISION	DESCRIPTION OF REVISION
1	10/01/25	N/A	Original version	N/A
2	14/09/26	SAR	Updated SAR	ID verification explanation



Who we are and our role

Tu Nguyen Management Limited, c/o Benison Solvers Limited, 1000 Great West Road, Brentford, Middlesex, TW8 9DW.

Tu Nguyen Management Limited acts as a data controller for personal data it processes for its own business purposes, including website operation, marketing, enquiries, supplier management, tenancy administration, compliance, complaints handling, and records held in TNM systems.

In some cases, we process personal data on behalf of a landlord or client and in accordance with their instructions. In those cases, TNM may act as a processor. In some arrangements, TNM and the landlord/client may act as joint controllers where we jointly determine how and why personal data is used.

Our role depends on the specific processing activity. If you would like more information about our role in relation to a particular service or data set, please contact us.

Summary of how we use your data

We use your personal data:

- to deliver services to you, to send you information about properties and property related services you may request of us or that we think will be of interest to you;
- to conduct searches about your identity, your current and past residency addresses, and your right to live in the UK and credit history to meet applicable laws including money laundering regulations;
- to provide a recommendation to landlord clients, on your suitability as a tenant;
- to carry out our obligations arising from any contracts (written or verbal) entered into by you, us or which it is contemplated may be entered into;
- to notify you of changes to our services;
- to process a job application;
- for administrative and business purposes;
- for advertising and analytical purposes;
- in connection with our legal rights and obligations and to pursue our legitimate interests;
- for certain additional purposes but only with your consent.
- We may share information about you with others as described in this policy who have undertaken to hold your personal data in compliance with applicable laws;
- Where we rely on your consent for direct marketing purposes, you can withdraw this consent at any time.



What information do we collect?

We collect and process personal data about you when you interact with us on messaging applications such as SMS, WhatsApp, Social Media messaging or other communication platforms and our websites and when you register with us to receive our services.

Use of WhatsApp and other messaging applications

We use messaging applications such as WhatsApp to communicate with you in a convenient and secure way. We do not create separate archives or databases of WhatsApp message content outside of the WhatsApp application itself.

We use WhatsApp messages only for day-to-day operational purposes (for example arranging viewings, inspections, repairs or discussing tenancy matters). We do not rely on WhatsApp message content as our primary record of a transaction; key decisions and records are stored in our internal systems (for example, our email, property management or client relationship management systems).

As a matter of policy, we do not intentionally store or retain WhatsApp messages beyond what is necessary to manage our relationship with you. This follows the data-protection principle of storage limitation and reduces the risk of sensitive information being retained unnecessarily. Chats are routinely deleted from our devices as part of our data security protocol. In any event, we will delete WhatsApp chats relating to you when our business relationship with you ceases, except where we reasonably need to retain specific messages as evidence for legal, regulatory, complaint-handling or anti-money laundering purposes. In those limited cases, relevant messages may be copied into our internal records and retained in line with our general retention periods set out below.

Other than the personal data which you give us (which will usually include, name, address, telephone number, email address, date of birth, credit history, previous addresses, identification) in response to requests from us or other parties to a transaction which you are participating in, information that we may directly or indirectly collect from you includes:

- technical information, including the Internet protocol (IP) address used to connect your computer to the Internet, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform; and
- information about your website visit, including the full Uniform Resource Locators (URL) clickstream to, through and from our site (including date and time); pages you viewed or searched for; page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page.



SENTINEL LETTINGS

- photographs and video recordings taken at or around properties we manage by our staff, landlords, contractors or cleaners, where required to record maintenance issues, confirmation of works completed, fire safety concerns, other health and safety matters or breaches of tenancy / property rules.

CCTV Recording

The Company or some of the properties it manages on behalf of landlords may operate CCTV systems in or around the properties to protect tenants, premises, assets, staff, visitors and trades from crime.

We do this on the basis of our legitimate interests in a way which might reasonably be expected as part of running our business and which does not materially impact your rights, freedom or interests.

If we discover any criminal activity or alleged criminal activity through our use of CCTV, we will process this data for the purposes of preventing or detecting unlawful acts. Our aim is to protect and/or deter the individuals we interact with from criminal activities and particularly serious offences under Schedule 1, as amended by Section 47 of the SCA 2015 and Schedule 5, of the Modern Slavery Act 2015 (Section 7).

The company CCTV systems do not use facial recognition nor do they collect biometrics; they are also not connected to other systems containing personal data.

Where footage contains your personal data, you may have the right to request access to that footage. We will consider such requests on a case-by-case basis in accordance with data protection law. In some cases and where possible, we may need to redact or obscure images, audio or other information relating to third parties, or withhold limited information where an exemption applies. If there is a criminal offence or likelihood of future criminal proceedings, we reserve the right to withhold the data for the Police or relevant authorities to avoid hindering any future investigations.

If a surveillance system is owned or controlled by a landlord rather than TNM, the landlord may be the relevant controller for that system. In those circumstances we may direct you to the landlord or provide contact details where appropriate.

We will comply with our legal obligations to share data with law enforcement on their request.



Photographs and Video Captured by Contractors, Cleaners and Other Third Parties

From time to time, we and our contractors, cleaners and other third parties acting on our behalf may take photographs and short video clips at or around properties that we manage. This may include images of:

- maintenance issues (for example, leaks, damage, disrepair or defective fixtures);
- fire safety concerns (for example, blocked escape routes, tampered fire doors, missing or damaged fire safety equipment);
- other health and safety issues or breaches of property rules (for example, significant cleanliness concerns in common areas, evidence of smoking indoors, or unsafe storage).

These photographs and videos are taken solely for the purpose of documenting and resolving maintenance and safety issues, monitoring compliance with legal and regulatory obligations (including HMO and fire safety requirements), and evidencing our management actions. Our legal basis for this processing is our legitimate interests in managing and protecting the properties, tenants, visitors and neighbours, and compliance with our legal and regulatory obligations.

Images will usually focus on the relevant part of the property (for example, a wall, appliance, fire door or communal area). However, on occasion individuals may be captured incidentally in the background. We seek to minimise this wherever possible.

These photographs and videos may be shared with:

- the landlord or their representatives;
- contractors and professionals engaged to diagnose or address the issue;
- insurers, loss adjusters and warranty providers;
- local authorities, emergency services or regulators where required for licensing, investigation, enforcement or other legal purposes; and
- our professional advisers where necessary (for example, in connection with a complaint or legal claim).

All contractors and cleaners who capture such images or videos on our behalf are contractually required to handle them securely, only for the purposes we specify, and in accordance with data protection law and this policy. We retain these images and videos in line with our retention periods for maintenance, compliance and legal records.

Telephone Call Recording

We may operate call recording:



It is in our legitimate interests to record calls unless those interests are overridden by you by asking for your call not to be recorded. In that case, we may ask you to contact us by email or in writing.

- You will be informed if call recording is in operation
- Personal data revealed during a telephone call will be digitally recorded, for example name and contact details, to deliver services to you or for your benefit.

Call recordings may be used to:

- respond to any questions, complaints or claims made by you or on your behalf;
- show that we treated you fairly
- keep records required by law
- protect the interests of you, our staff or both

All call recordings are held securely.

What information do we receive from third parties?

Sometimes, we receive information about you from third parties. In particular:

- Social Media Companies including Facebook, Twitter, Google+ when you interact with our brand through these platforms;
- Live chat suppliers who may be partnered with us through Live Chat applications hosted on our website;
- Previous or current landlords for the purpose of referencing;
- Contractors or other professionals who may interact with you as part of our business with you;
- Enquiries through property portals when you request further information on a property or request information or contact from one of us;
- Financial advisors, mortgage brokers, lenders and solicitors/conveyancing agents through transactions relating to the service we are providing; and
- Other agents/companies as and when required for purposes which will be disclosed to you at the time.

The purposes for using your personal information

We process your personal data for the following purposes:

- To fulfil a contract, or in preparation of a contract by, for example providing our services, including processing information in connection with a property's letting, sourcing, development or management;



SENTINEL LETTINGS

- we may use your information to provide services to you before we have a contract with you (for instance sending potential buyers and tenants property details), and to respond to any comments or complaints you may send us
- As required by us to conduct our business and pursue our respective legitimate interests, for example:
 - to monitor use of our websites and online services, and to help us monitor, improve and protect our products, content, services and websites, both online and offline, including as set out in our Cookie policy below;
 - the Company uses information you provide to personalise our website, products or services for you, including as set out in our Cookie policy below;
- Where you give us consent we will send you direct marketing in relation to products and services, provided by us, members of our group of companies and selected third parties
- On other occasions when we ask you for consent, we will use the data for the purpose which we explain at that time.
- For purposes which are required by law, for example:
 - to verify your identity; and
 - in response to requests by government or law enforcement authorities conducting an investigation.

Withdrawing consent or otherwise objecting to direct marketing

Wherever we rely on your consent, you will always be able to withdraw that consent, although there may be other legal grounds for processing your data for other purposes, such as those set out above. In some cases, we are able to send you direct marketing without your consent, where we rely on our respective legitimate interests or for delivery related services which are required for us to deliver the services we have contracted or preparing to contract with you.

You have an absolute right to opt-out of direct marketing or profiling we carry out for direct marketing, at any time. You can do this by following unsubscribe instructions contained in the communication, or by contacting us using the details set out below.

Who will we share this data with, where and when?

We will share your personal data with companies in the same group of companies as us and third parties detailed in the section below for the purpose of providing a service to you, under our legitimate interests and understanding your use of our products and services. We will not sell or provide your information to third parties other than to parties with whom we have entered into contracts which require them to comply in all respects with the requirements of this Privacy Policy and all legal requirements relating to information privacy.



We may share your data with or on:

- Any other named party to a signed contract entered into by you in accordance with your instructions, such as your landlord or tenant;
- Third parties who provide services to the property for maintenance, required checks for the property and repairs including but not limited to plumbers, electricians, builders, carpenters. Information will also be shared to contractors where they wish to pursue any unpaid invoices.
- Utilities companies where we are required to do so to adhere to a tenancy agreement or for utility switching purposes;
- Referencing companies to obtain references for letting a property;
- Deposit protection schemes for registration of a deposit;
- Block managers where a let property is a leasehold property;
- Inventory companies who conduct check ins and check outs;
- Insurance and warranty companies for both introduction to products and for information requested to process any claims;
- Alternative deposit scheme companies;
- Photographers for photography;
- If you provide a credit or debit card as payment, we may use third parties to process the payment and to check the validity of the sort code, account number and card number you submit in order to prevent fraud;
- Third parties who we contract to provide administration services and sales of related products and services required for the purposes of delivering the services and products to you;
- In connection with legal claims, compliance, regulatory and investigative purposes as necessary (including disclosure of such information in connection with legal process or litigation);
- Third parties such as The Property Ombudsman to investigate any complaints received from you or from others, about our services or the properties which we deal with;
- Third parties for the purposes of confirming your identity and complying with AML and “right to rent” requirements;
- Software platforms to facilitate email marketing ;
- Audit purposes;
- Debt collection companies;
- E-signature companies for online signatures;
- Property CRMs in order to manage your data;
- Other software solutions to help provide the services to you for example, property maintenance online reporting, Identity check platforms, sales progression software, material information and other compliance requirements e.g property licensing;
- Website hosting companies for website hosting;
- Property specialist advisors for specialist advice;
- Property auction companies for auctioneering services;



SENTINEL LETTINGS

- Telephone answering service and online chat providers in order for us to process your data to fulfil our requirements;
- Internal client CRMs for client management services;
- Lead Management providers to help us to process enquiries;
- Accountancy software in order to fulfil our services;
- Third parties who provide services to the property for maintenance, required checks for the property and repairs including but not limited to plumbers, electricians, builders, carpenters, some of whom may capture photographs or short video clips on our behalf to document maintenance, fire safety or other safety issues.
- Photographers for photography and other visual media (including video) relating to the marketing, management or inspection of a property;
- approved artificial intelligence, automation and technology service providers where reasonably necessary to assist us with administration, document handling, correspondence, property management, compliance or other purposes described in this policy;

Personal data may be shared with government authorities and/or law enforcement officials, if required for the purposes above including any required information sharing or platforms for publication of legally required information, if mandated by law or if required for the legal protection of our legitimate interests in compliance with applicable laws.

In the event that we sell or integrate our business with another business, your details will be disclosed to our advisers and any prospective purchaser's adviser and will be passed to the new owners of the business.

Artificial Intelligence and Automated Tools

We may use approved artificial intelligence ("AI"), machine-learning and automated software tools to assist our staff or agents in carrying out administrative and property-management activities.

This may include using AI to assist with:

- organising, categorising and summarising correspondence;
- identifying relevant issues within enquiries or complaints;
- preparing draft correspondence for staff review;
- locating, organising or reviewing records and documents;
- assisting with maintenance, compliance and property-management workflows;
- administrative, analytical and record-management activities; and
- assisting staff or agents when responding to data protection or information requests.



Where personal data is processed using an AI or automated system, we will process that information in accordance with applicable data protection law. Depending on the circumstances, our lawful basis may include performance of a contract, compliance with a legal obligation, or our legitimate interests in efficiently administering our business, managing properties, maintaining accurate records and providing services.

We will seek to use only the personal information reasonably necessary for the relevant purpose. Where an external AI or technology provider processes personal information on our behalf, we will take appropriate steps to assess the provider and put suitable contractual, confidentiality and security arrangements in place.

AI-generated information may be inaccurate or incomplete. Agents must therefore exercise appropriate human oversight and must not assume that an AI-generated statement, summary, legal reference or recommendation is correct.

We do not rely upon generative AI as the final decision-maker when determining a formal complaint, deciding whether an individual may exercise a statutory data protection right, taking tenancy enforcement action, or making another significant decision about an individual.

We do not currently make decisions producing legal or similarly significant effects about individuals solely by automated means without meaningful human involvement. If this changes, we will update this policy and provide the information and safeguards required by applicable data protection law.

How long will you retain my data?

We retain personal data only for as long as necessary for the purpose for which it was collected, taking into account legal, regulatory, tax, anti-money laundering, complaint-handling, insurance and limitation-period requirements.

For some types of information, we keep data for shorter periods than 5 years. In particular, transient communications such as WhatsApp messages, SMS and other instant messages are kept only for as long as they are needed to manage your enquiry, application, tenancy or other relationship with us. We aim to delete these chats on a rolling basis and, in any event, at the point our business relationship with you ceases, unless we reasonably need to retain specific messages as evidence in connection with a complaint, legal claim, regulatory investigation or to comply with our anti-money laundering or other legal obligations. In those cases, we will retain only the relevant extracts in our internal systems and apply the normal retention periods to those records.



Where we use personal data for marketing purposes or with your consent, we process the data until you ask us to stop and for a short period after this (to allow us to implement your requests). We also keep a record of the fact that you have asked us not to send you direct marketing or to process your data indefinitely so that we can respect your request in future.

Type of data

- tenancy and deposit records: 5 years after the tenancy ends;
- landlord and client records: 5 years after the business relationship ends;
- complaints and legal claims files: 5 years after conclusion of the matter;
- CCTV / video surveillance footage: the agency is currently not a data controller.
- WhatsApp, SMS and other transient communications: kept only for as long as needed operationally, unless specific messages are extracted and retained as evidence for a complaint, legal claim, investigation, compliance purpose or other legal obligation.

Cookies and other tracking technologies

What are they?

Cookies are small pieces of information sent by a web server to a web browser which allows the server to uniquely identify the browser on each page. Other tracking technologies are also used which are similar to cookies. This can include pixel tags and tracking URLs.

All these technologies are together referred to in this Policy as “Cookies”.

How do we use Cookies?

Cookies and similar technologies

We use strictly necessary cookies without consent where they are required for the operation, security and core functionality of our website.

We only set non-essential cookies or similar technologies, including analytics, advertising, targeting and social media cookies, after you have actively consented. Closing a banner, continuing to browse, or clicking elsewhere on the website does not amount to consent.



Our cookie controls allow you to accept or reject non-essential cookies by purpose, and to withdraw consent as easily as you gave it.

Our cookie banner and settings panel identify the categories of cookies we use, the purposes for which they are used, and the third parties involved.

If you do not want to allow Cookies at all, or only want to allow use of certain Cookies, please refer to your browser settings. You can also use your browser settings to withdraw your consent to our use of Cookies at any time and delete Cookies that have already been set. Please note that by deleting our cookies or disabling future Cookies you may not be able to access certain areas or features of our site.

To find out more about Cookies please visit: www.allaboutcookies.org or see www.youronlinechoices.eu.

Handling Mail Not Addressed to the Tenant

In situations where a tenant reports receiving letters or mail at a property that is not addressed to them, the agency must treat this as a potential data protection matter.

The agency or contractor should:

- Advise the tenant not to open, discard, or interfere with the contents of the letter.
- Request a photo of the envelope showing the name and address (if appropriate), without opening the letter.
- Arrange collection by the landlord; or
- Provide secure instructions for the tenant to set the letter aside until it can be returned; or
- Passed on to the appropriate party; or
- Return to sender

Do not advise tenants to destroy the letter. Where personal data of a previous tenant or third party is involved, this must be treated as a potential data handling risk under UK GDPR.

If the landlord wishes the tenant to open the letter, this request must be made in writing and the agency accepts no liability should the information contained within the letter be misused.

Handling Mail Addressed to Former Tenants (Post-Tenancy)

Once a tenancy has ended and vacant possession has been given, all responsibility for managing a former tenant's mail rests with the tenant. The agency and landlord are not responsible for receiving, storing, or forwarding post after the end of the tenancy.



Tenant responsibilities

Tenants are responsible for:

- Setting up a Royal Mail Redirection service before the end of the tenancy.
- Updating their address directly with banks, employers, government bodies, and any other relevant organisations.
- Removing all personal post and parcels from the property at check-out.

Tenants will be reminded of this responsibility:

- In pre-move-out communications; and
- At check-out, where practical.
-

Mail delivered after the tenant has moved out

Where mail continues to arrive at the property for a former tenant after the tenancy has ended:

The agency and/or landlord will not:

- Open, scan, photograph, or forward mail to the former tenant; or
- Use personal contact details to notify former tenants each time post is delivered.

The default action will be:

- Mark the envelope "Return to sender – addressee no longer at this address" and place it back into the postal system; or
- Where appropriate and secure disposal facilities are available, securely dispose of the mail without opening it.

Any handling of post will be carried out in a way that minimises data protection risk and complies with UK GDPR. Former tenants should not rely on the agency or landlord to manage or forward personal or sensitive correspondence.

Post left behind at check-out

Any letters or mail left behind in the property by the tenant at the end of the tenancy will be treated as abandoned.

Such items may be:



SENTINEL LETTINGS

- Marked "Return to sender – addressee no longer at this address" and returned via the postal system; or
- Securely disposed of without opening, in line with data protection principles.

Secure collection in limited circumstances

In exceptional cases, and only where operationally feasible, the agency may agree to hold post for short-term, one-off collection by a former tenant.

This will be:

- By prior appointment only;
- Subject to identity verification of the person collecting; and
- Subject to a reasonable administrative fee for agency time, in line with the agency's published fee schedule at the time of the request.

The agency reserves the right to refuse collection where:

- Security or data protection concerns arise; or
- The volume of mail or time elapsed since the tenancy ended makes collection impractical.
- The agency does not have operational capacity to assist.

No ongoing mail-handling service

The agency and landlord do not offer an ongoing mail-handling or forwarding service for former tenants.

Former tenants must not:

- Use the rental property as a correspondence or registered address after their tenancy has ended; or
- Instruct third parties to continue sending mail to the property once vacant possession has been given.

This section should be read alongside the agency's data protection, tenancy management, and check-out procedures.



Changes to our Privacy Notice

Any changes we may make to this policy in the future will be posted on this page and, where appropriate, notified to you by e-mail. Please check back frequently to see any updates or changes to our policy.

What rights do I have?

You have the right to:

- access your personal information and to be informed about its use by us
- correct your personal information;
- have your personal information deleted;
- restrict the use of your personal information;
- object to the use of your personal information;
- complain to the Information Commissioner's Office;
- withdraw your consent to the use of your personal information;
- ask for the personal information to be transferred.

UNDER 18?

We are especially concerned with protecting the privacy of children/minors. If you are under the age of 18, you must obtain your parent/guardian's permission before providing any personal information. When providing personal information your parent/guardian should be with you to help you through this process.

Accessing your information

The accuracy of your information is important. If the personal information you have provided to us changes, if you change email address, or any of the other information we hold, please email the office who have been delivering the services and products to you.

When you exercise your right of access (a "subject access request"), we will search the systems and records under our control for personal data relating to you. This includes any WhatsApp or other messaging-app content that we still hold at the time of your request and that falls within the scope of your request.

Because we operate a policy of not retaining WhatsApp messages beyond the duration of the business relationship (except where specific messages are needed for legal or compliance purposes), some historical message content may already have been deleted by the time we receive your request. In those cases, we will explain this to you and will not be



able to recover or provide copies of messages that have been permanently deleted in line with our retention policy.

Security Measures

We will ensure that your personal information is held securely.

Some of your “non-sensitive” details (such as your email address) may be transmitted over the internet and this can never be guaranteed to be 100% secure.

Other websites

Our websites may contain links to other websites which we do not own

but this privacy policy only applies to our website and we cannot be responsible for the privacy policies and practices of other sites whether or not you access them using links from our websites.

How to contact us and make a data rights request

If you have any questions about this policy, would like to make a subject access request or exercise any other data protection right, or would like to opt out of direct marketing, please contact us at info@sentinellettings.co.uk.

To help us process requests quickly, we ask that data protection requests are sent to this address. However, you may make a request through any TNM contact channel and we will route it to the appropriate person or team.

Where reasonable and proportionate, we may ask for information to verify your identity before disclosing personal data.

Company Data Protection Registration Certificate issued by the Information Commissioner's Office.

Identity verification for Subject Access Requests

Before disclosing personal data in response to a Subject Access Request (“SAR”), we must take reasonable steps to satisfy ourselves that the person making the request is the individual to whom the personal data relates, or is otherwise properly authorised or legally entitled to receive that information.



Where we have reasonable doubts about the identity or authority of the person making the request, we may ask for additional information or identification that is reasonably necessary to verify their identity. This may include, where appropriate, photographic identification, proof of address, confirmation of information already held by us, or evidence that a person is authorised to act on behalf of the data subject.

We will only request information that is proportionate and necessary for the purpose of verification. Any identification information provided for this purpose will be handled securely and used only so far as necessary to verify the request and comply with our data protection obligations.

Where identity or authority verification is required, we will notify the requester and ask them to provide the required information. The applicable statutory response period will be dealt with in accordance with data protection law once the information reasonably required to verify identity has been received.

We will not disclose personal data where we cannot reasonably verify the identity or authority of the person requesting it.

If the requester does not provide the information reasonably required to verify their identity or authority within the period specified in our verification request, or if we are unable to verify their identity after considering the information provided, we may close the SAR as incomplete. We will notify the requester where practicable. A new request may be submitted at any time, subject to satisfactory identity verification.

Use of AI in Data Protection Requests

Individuals may use artificial intelligence or other digital tools to assist them in preparing a Subject Access Request or another data protection request. Use of AI does not, by itself, affect the validity of a statutory request.

However, the person making the request remains responsible for ensuring that their request accurately reflects the information or right they wish to exercise. AI systems may produce inaccurate statements, irrelevant material, incorrect legal references or unnecessarily broad requests.

Where the scope of a request is unclear, we may ask the requester for information reasonably necessary to clarify the information they are seeking.

We will independently determine the legal effect and scope of any request and are not required to accept an AI-generated statement about the law merely because it has been presented as a legal requirement.



Where a request is manifestly unfounded or manifestly excessive, including where appropriate because of its repetitive nature or substantial overlap with previous requests, we may apply the provisions available to us under data protection law. Any such decision will be made on the individual circumstances and will not be based simply upon whether AI has been used.

Data Protection Complaints

If you believe that we have not handled your personal information in accordance with data protection law, you may make a data protection complaint to us.

This may include a complaint about how we have collected, used, shared, retained or secured your personal information, or about how we have handled a Subject Access Request or another data protection right.

You do not need to use legal terminology or identify a particular provision of data protection legislation in order to make a complaint.

Data protection complaints may be sent to info@sentinellettings.co.uk. If a complaint is made through another Sentinel Lettings contact channel, we will take reasonable steps to identify it and route it to the appropriate person.

We will acknowledge a data protection complaint within 30 days of receipt. We will take appropriate steps to investigate the complaint without undue delay, make any enquiries that are reasonably necessary, keep the complainant appropriately informed and communicate the outcome without undue delay.

Where a complaint also concerns another matter, such as property management, repairs, tenancy administration or customer service, the relevant parts may also be considered under our [Complaints Procedure](#).

If you remain dissatisfied with our handling of your personal information or your data protection complaint, you have the right to raise the matter with the Information Commissioner's Office.