GRIDSTEAD

Data Protection Policy

How Gridstead handles personal data, as a business and as a processor for its clients

Owner	Thomas Hawtin, Gridstead
Version	1.0
Date	[date]
Review	Every 12 months, or sooner if the service changes

1. Purpose and scope

This policy sets out how Gridstead handles personal data. It covers two distinct roles. Gridstead is a controller for its own business data, such as enquiries, client contacts, billing records and marketing contacts. Gridstead is a processor for the tenant, contractor and staff data that clients enter into the appointment platform, where the client letting agency is the controller.

2. Principles we work to

- Lawfulness, fairness and transparency. We tell people what we do with their data and we do nothing surprising with it.
- Purpose limitation. Client data is used only to run the service for that client.
- Data minimisation. The platform collects a name, a phone number, an address and access notes, because that is what a visit needs. Nothing more is asked for.
- Accuracy. Clients can correct or delete any record from within the service at any time.
- Storage limitation. Data is kept only while a client uses the service, then deleted or returned on request.
- Integrity and confidentiality. Encryption, individual logins and company isolation, as set out in section 4.
- Accountability. Decisions and measures are documented here and in the data processing agreement issued to each client.

3. Lawful bases

For its own business data, Gridstead relies on legitimate interests to correspond with prospective and current clients, and on contract to provide and bill for the service. For data processed on a client’s behalf, the lawful basis is the client’s to determine as controller, and is typically contract, legal obligation and legitimate interests.

4. Security measures

- Data at rest is encrypted with AES 256 GCM. Data in transit is encrypted with HTTPS.
- Passwords are stored only as salted scrypt hashes. Nobody at Gridstead, and nobody at the client, can read a user’s password.
- Every member of client staff has an individual login, so every action in the record is attributable to a named person. Repeated failed logins are locked out.
- Each client company is isolated. Every request is checked against the requesting company, so one client cannot reach another client’s records.
- Tenant and contractor access uses long, unguessable, revocable links rather than accounts, so no vulnerable person has to manage a password.
- Hosting is in the European Union on Render. Text messages are delivered by Twilio.
- Platform level administration is restricted to the Gridstead owner and protected by a separate credential that is not shared with any client.

- No client data is used to train artificial intelligence or machine learning models, and no client data is sold or shared for advertising.

5. Sub-processors

Gridstead uses Render for hosting in the EU, Twilio for text message delivery, and an email delivery provider for account and invitation emails where enabled. Each is bound by its own terms, and clients are notified in advance of any change so that they may object.

6. Personal data breaches

Any suspected breach is investigated immediately. Where a client's data is affected, that client is notified without undue delay and within 48 hours of Gridstead becoming aware, with the detail they need to meet their own 72 hour duty to the Information Commissioner's Office. Where Gridstead's own controller data is affected, Gridstead reports to the ICO within 72 hours where the breach is likely to result in a risk to individuals. A record is kept of every breach, including those not reported, with the reasoning.

7. Individuals' rights

Requests about data held in the platform are referred to the relevant client, who is the controller, and Gridstead assists them in responding within the statutory month. Requests about Gridstead's own business data are handled by Gridstead directly. There is no charge for a first request unless it is manifestly unfounded or excessive.

8. Retention

- Client account and billing records: kept for the life of the relationship and then six years, for tax and contractual purposes.
- Data inside the platform: retained at the client's direction, deleted or returned within 30 days of a written request at the end of the relationship.
- Enquiries that do not become clients: deleted within 12 months.

9. ICO registration

Gridstead is registered with the Information Commissioner's Office as a controller of its own business data and pays the annual data protection fee. Each client letting agency remains separately registered as the controller of its own tenant and contractor data. Registration number: [insert once registered].

10. Responsibilities

Thomas Hawtin, as owner, is accountable for data protection at Gridstead. There is no requirement for a statutory Data Protection Officer at this scale, since Gridstead does not carry out large scale systematic monitoring or large scale processing of special category data. This position is reviewed if the business grows or the service changes.

This policy is a working document for Gridstead and is provided to clients on request. It is not legal advice.