# HomeOrbit Legal Pack

Prepared for Joshua Roberts trading as HomeOrbit

*Version 1.0 | Last updated: 15 April 2026*

This pack contains the core legal and operational documents drafted for the current HomeOrbit website and platform setup, based on the project files, schema, and information provided in this conversation. It is written for a UK sole-trader-operated B2B SaaS / pilot model serving care-sector organisations.

## Contents


1. Website Terms of Use
2. Platform Terms of Service
3. Acceptable Use Policy
4. Privacy Notice
5. Cookie Policy
6. Data Processing Agreement
7. Subprocessor Schedule
8. Retention and Deletion Schedule
9. Security and Support Policy
10. Accessibility Statement
11. Enquiry Privacy Summary

# HomeOrbit Website Terms of Use

**Version:** 1.0

**Last updated:** 15 April 2026

These Website Terms of Use apply to the public HomeOrbit website, including marketing pages, contact and enquiry forms, and any non-authenticated content made available at or through the HomeOrbit website.

## 1. Who we are

HomeOrbit is operated by **Joshua Roberts trading as HomeOrbit**, a UK sole trader based at **Apartment 414, 35 Greenland Street, Liverpool, L1 0AD, United Kingdom**.

**Contact email:** support@homeorbit.co.uk

References in these terms to **"HomeOrbit"**, **"we"**, **"us"** or **"our"** mean Joshua Roberts trading as HomeOrbit.

## 2. About these terms

These Website Terms govern your access to and use of the public website only. If you are given access to the HomeOrbit software platform, your use of the platform is also governed by the applicable platform terms, pilot agreement, order form, or other written commercial agreement.

By using the public website, you agree to these Website Terms. If you do not agree, do not use the website.

## 3. Who the website is for

HomeOrbit is intended for businesses and organisations operating in the care sector and related professional users. The website is not directed to children and must not be used by anyone under the age of 18.

## 4. Permitted use

You may use the website only for lawful purposes and only in a way that does not infringe the rights of others or restrict or inhibit anyone else's use of the website.

You may:

- view pages from the website for your own legitimate business use;
- make enquiries about HomeOrbit and its services;
- print or download limited extracts for internal evaluation purposes; and
- share links to public website pages.

## 5. Prohibited use

You must not:

- use the website in breach of any law or regulation;
- attempt to gain unauthorised access to any account, system, server, data, or network;
- upload, submit, or transmit malicious code, harmful files, or any material designed to disrupt the website;
- probe, scan, scrape, harvest, benchmark, mirror, data-mine, or systematically extract website content except where we have given prior written permission;
- interfere with website security, performance, or availability;
- impersonate another person or misrepresent your affiliation;
- use the website to send spam or other unsolicited communications; or
- use the website in any way that could damage the reputation of HomeOrbit.

## 6. Enquiries and communications

If you contact us through the website, you must ensure that the information you provide is accurate and not misleading. You must not include confidential patient information, special

category data, criminal offence data, or other unnecessary sensitive personal data in public website enquiries unless we have expressly asked for it through a secure process.

Submitting an enquiry does not create any obligation on us to provide services, and does not create a customer relationship by itself.

## 7. Intellectual property

Unless otherwise stated, we own or license all intellectual property rights in the website and its content, including text, branding, graphics, page layouts, software, visual assets, design elements, and underlying code.

You may not reproduce, modify, republish, distribute, reverse engineer, frame, or commercially exploit any part of the website or its content except as allowed by law or with our prior written permission.

**HomeOrbit** and related branding are proprietary rights of Joshua Roberts trading as HomeOrbit. Nothing in these terms grants any licence to use our name, logo, marks, or branding except to identify us accurately.

## 8. Availability and changes

We may update, suspend, withdraw, restrict, or change any part of the website at any time. We do not guarantee that the website, or any content on it, will always be available, uninterrupted, secure, or error-free.

## 9. Information on the website

The website is provided for general information about HomeOrbit and its services. We aim to keep content accurate and up to date, but we do not guarantee that all information is complete, current, or free from error.

Nothing on the website constitutes legal advice, regulatory advice, employment advice, medical advice, care advice, financial advice, or a binding offer to contract.

## 10. Links to third-party websites

The website may contain links to third-party websites or services. Those links are provided for convenience only. We do not control and are not responsible for third-party websites, their content, availability, security, or privacy practices.

## 11. Security

You must not misuse the website by knowingly introducing viruses, trojans, worms, logic bombs, or other harmful material. You must not attempt to gain unauthorised access to the website, the server on which it is stored, or any server, computer, or database connected to it.

We may suspend access, block IP addresses, preserve evidence, and report activity to law enforcement or regulators where appropriate.

## 12. Liability

To the fullest extent permitted by law:

- the website is provided on an "as is" and "as available" basis;
- we exclude all implied warranties, representations, conditions, and other terms that may apply to the website or any content on it; and
- we will not be liable for any indirect, incidental, consequential, special, or punitive loss, or for any loss of profit, revenue, business, contracts, opportunity, goodwill, anticipated savings, data, or business interruption arising out of or in connection with the use of, or inability to use, the website.

Nothing in these terms excludes or limits liability for fraud, fraudulent misrepresentation, death or personal injury caused by negligence, or any other liability that cannot lawfully be excluded or limited.

## 13. Privacy and cookies

Use of the website is also subject to our Privacy Notice and Cookie Policy, which explain how we handle personal data and cookies in connection with the website.

## 14. Breach of these terms

If you breach these Website Terms, we may take any action we reasonably consider appropriate, including suspending or blocking access, issuing warnings, removing content, refusing enquiries, or taking legal action.

## 15. Governing law and jurisdiction

These Website Terms are governed by the law of **England and Wales**.

The courts of **England and Wales** will have exclusive jurisdiction over any dispute or claim arising from or connected with these Website Terms or the use of the website, except where mandatory law provides otherwise.

## 16. Changes to these terms

We may update these Website Terms from time to time. The latest version published on the website will apply from the date shown at the top of the document.

# HomeOrbit Platform Terms of Service

**Version:** 1.0

**Last updated:** 15 April 2026

These Platform Terms of Service govern access to and use of the HomeOrbit software platform and related services.

## 1. Parties

These Platform Terms are between:

**Service Provider: Joshua Roberts trading as HomeOrbit**, a UK sole trader of Apartment 414, 35 Greenland Street, Liverpool, L1 0AD, United Kingdom, contactable at support@homeorbit.co.uk; and

**Customer:** the organisation, business, or other entity that is given access to HomeOrbit under a pilot, trial, order form, proposal, or other written agreement.

## 2. Definitions

In these terms:

- **Account** means a user account used to access the platform.
- **Authorised User** means an individual whom the Customer allows to use the platform under the Customer's authority.
- **Customer Data** means data, content, records, files, documents, attachments, text, images, and other material submitted to or stored in the platform on the Customer's behalf.
- **Documentation** means any usage guidance or operating instructions we make available for the platform.
- **Pilot Period** means any period during which the Customer is permitted to use the platform on a trial, evaluation, implementation, testing, or pilot basis.

- **Services** means the HomeOrbit platform and related support, implementation, maintenance, and ancillary services that we agree to provide.
- **Special Category Data** has the meaning given in the UK GDPR.
- **Subprocessor** means a third party engaged by us to process personal data on behalf of the Customer in connection with the Services.

## 3. Nature of the service

HomeOrbit is a role-based operational and administration platform intended for care-sector organisations. Depending on the modules enabled, it may support operational workflows, rota management, training records, forms, policies, budgets, personnel records, payslips, young person records, medication-related information, internal documents, and similar business functions.

The platform is an administrative and operational support tool. It does **not** replace professional judgment, safeguarding judgment, medical judgment, employment law advice, payroll advice, legal advice, or regulatory decision-making. The Customer remains responsible for its own decisions, care delivery, staffing decisions, compliance obligations, and record-keeping duties.

## 4. Basis of access

The Services may be provided:

- under a free pilot or trial;
- under a written proposal or implementation arrangement;
- under a paid order form or later commercial agreement; or
- under another written arrangement between the parties.

Unless the parties expressly agree otherwise in writing, any initial access granted before a paid agreement is treated as a **revocable pilot** and may be subject to additional onboarding, security, or usage conditions.

## 5. Grant of licence

Subject to these terms and any agreed usage limits, we grant the Customer a limited, non-exclusive, non-transferable, non-sublicensable right during the applicable term to permit its Authorised Users to access and use the Services for the Customer's own internal business purposes.

No rights are granted except those expressly stated.

## 6. Customer responsibilities

The Customer must:

- ensure only authorised adults use the platform;
- keep its account credentials secure and ensure users do the same;
- ensure its use of the platform complies with applicable law, regulation, safeguarding requirements, employment requirements, data protection law, and internal policy;
- ensure that Customer Data uploaded to the platform is accurate enough for the Customer's intended use;
- ensure it has a lawful basis and all required notices, permissions, and internal approvals for the personal data it uploads;
- configure and use the platform responsibly, including permissions, workflows, and records;
- promptly notify us of any suspected security issue, credential compromise, or unauthorised access;
- be responsible for its users, internal instructions, and all activity carried out through its accounts; and
- maintain its own offline or independent records where prudent for business continuity, legal, safeguarding, or regulatory purposes.

## 7. Restrictions

The Customer must not, and must not permit any third party to:

- copy, modify, adapt, create derivative works from, decompile, disassemble, reverse engineer, or attempt to extract source code from the platform except where such restriction is prohibited by law;
- resell, lease, sublicense, timeshare, distribute, or otherwise commercially exploit the platform for third parties;
- access the platform in order to build a competing product or service;

- use the platform unlawfully, abusively, or in a way that could damage the platform, other users, or our reputation;
- upload malicious code or attempt unauthorised access, testing, or scanning;
- use the platform to store or process data that the Customer is not legally entitled to process; or
- misrepresent the platform's outputs or use them as the sole basis for emergency, disciplinary, safeguarding, clinical, payroll, or regulatory action without appropriate review.

## 8. User management and permissions

The Customer is responsible for deciding who should have access to its tenant, homes, modules, records, and workflows, except where we manage certain initial configuration settings during setup.

We may rely on account instructions and administrator instructions given through the platform or through an agreed implementation contact unless we have reason to believe they are unauthorised.

## 9. Customer Data

As between the parties, the Customer retains ownership of Customer Data. The Customer grants us the limited rights necessary to host, process, transmit, back up, secure, troubleshoot, maintain, and improve the Services in line with these terms and the applicable data processing terms.

We do not acquire ownership of the Customer's operational records or uploaded content merely because they are stored in the platform.

## 10. Personal data roles

For most Customer Data processed through the platform, the Customer acts as the **controller** and HomeOrbit acts as the **processor**. The parties agree that the HomeOrbit Data Processing Agreement forms part of these Platform Terms and applies automatically where required.

For data relating to public website visitors, prospective customers, customer contacts, billing contacts, platform administration, service communications, platform security, and our own business records, HomeOrbit may act as an independent controller.

## 11. Special category and sensitive data

The platform may be used by Customers to process sensitive operational data, including special category data and criminal offence data, where the Customer chooses to do so. The Customer is solely responsible for ensuring that it has identified an appropriate lawful basis and, where required, an additional condition for processing under applicable law.

The Customer must not use the platform for biometric identification, covert monitoring, or high-risk processing that materially changes the nature of the agreed services without first notifying us and, where appropriate, completing an appropriate risk review.

## 12. Security

We will apply reasonable and appropriate technical and organisational measures designed to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access, taking into account the nature of the Services and the information available to us.

No system can be guaranteed to be completely secure or available at all times. The Customer accepts that the Services may be affected by outages, maintenance, internet failures, supplier incidents, force majeure events, malicious activity, or other matters outside our reasonable control.

## 13. Support, maintenance, and changes

During any pilot or early access period, support is provided on a **reasonable endeavours** basis during normal UK business hours, together with any additional support separately agreed through implementation arrangements or the user's dual-role engagement.

We may:

- release patches, fixes, updates, and improvements;
- modify features, workflows, or interfaces where reasonably necessary;
- perform scheduled or emergency maintenance; and
- change infrastructure providers or subprocessors, subject to the data processing terms.

We will use reasonable efforts to avoid material degradation of the core Services, but we do not guarantee that every feature will remain unchanged.

## 14. Beta and pilot status

Where the platform or particular modules are provided as part of a pilot, testing phase, implementation phase, or pre-commercial rollout:

- the Services may include evolving, incomplete, experimental, or changing functionality;
- features may be added, removed, limited, or altered;
- documentation may be lighter than for a mature service;
- support may be more hands-on but not governed by formal service credits; and
- the Customer uses the pilot with that understanding.

## 15. Fees and payment

Unless the parties agree fees in writing, access granted during a pilot period is provided **without separate software charges**.

If fees are introduced later, they must be set out in a written proposal, order form, contract variation, or other written agreement. No public website pricing page forms part of these terms unless expressly incorporated in writing.

## 16. Suspension

We may suspend access to all or part of the Services immediately if:

- we reasonably believe continued access would create a security risk or legal risk;

- the Customer materially breaches these terms;
- the Customer's use is unlawful or abusive;
- credentials are compromised;
- a third-party provider failure requires urgent restriction; or
- suspension is necessary to protect the platform, other customers, or data.

Where reasonably practicable, we will notify the Customer and work toward restoration.

## 17. Term and termination

These Platform Terms start when access to the Services is first granted and continue until terminated.

Either party may terminate a pilot or ongoing access on written notice. Unless a different period is agreed in writing, either party may terminate for convenience on **30 days' written notice**.

Either party may terminate immediately if the other commits a material breach that is incapable of remedy or is not remedied within 14 days of written notice requiring remedy.

## 18. Effect of termination

On termination or expiry:

- the Customer's right to access and use the Services ends;
- we may disable accounts and customer environments;
- the Customer may request export of its Customer Data during an **export window of 30 days** following the effective date of termination, provided the Customer has complied with applicable law and any outstanding agreed administrative steps; and
- after the export window, we may delete or render inaccessible Customer Data unless retention is required by law or reasonably necessary for security, backup integrity, dispute resolution, or compliance.

We may retain limited records needed for legal, tax, anti-fraud, security, or evidential purposes.

## 19. Confidentiality

Each party must keep the other's confidential information confidential and use it only for the purposes of the relationship, except where disclosure is required by law, regulation, court order, professional advisers under a duty of confidence, or competent authorities.

Customer Data is treated as the Customer's confidential information.

## 20. Intellectual property rights

We and our licensors retain all right, title, and interest in and to the Services, software, database structure, user interfaces, documentation, branding, workflows, know-how, and all improvements or derivative works created by or for us, excluding Customer Data.

Except for the limited licence expressly granted, the Customer receives no intellectual property rights in the Services.

## 21. Feedback

If the Customer or its users provide feedback, ideas, suggestions, or enhancement requests, we may use them freely without restriction or payment, provided we do not identify the Customer as the source without permission unless the idea is already public or obvious from the context.

## 22. Warranties and disclaimers

We warrant that we have the right to provide the Services.

Except as expressly stated in these terms, the Services are provided on an "as is" and "as available" basis. To the fullest extent permitted by law, we disclaim all implied warranties, conditions, and

representations, including implied warranties of merchantability, fitness for a particular purpose, satisfactory quality, non-infringement, or uninterrupted availability.

The Customer acknowledges that:

- the platform supports operational administration but is not a substitute for the Customer's own controls;
- internet-based services are not free from bugs, outages, or cyber risk;
- the Customer remains responsible for reviewing outputs and records; and
- availability, storage, and functionality may depend partly on third-party providers.

## 23. Liability

Nothing in these terms excludes or limits liability for fraud, fraudulent misrepresentation, death or personal injury caused by negligence, or any liability that cannot lawfully be excluded or limited.

Subject to the paragraph above, to the fullest extent permitted by law:

- neither party will be liable for any indirect, incidental, special, punitive, or consequential loss, or for loss of profit, revenue, business, contracts, opportunity, goodwill, anticipated savings, or reputation;
- neither party will be liable for loss or corruption of data except to the extent caused by its failure to apply obligations expressly accepted under these terms; and
- our aggregate liability arising out of or in connection with the Services during any 12-month period will not exceed the greater of (a) the total fees actually paid by the Customer for the Services in that period and (b) **£1,000**, except where a higher amount is required by law or separately agreed in writing.

The liability cap above is intended to remain workable during unpaid pilot use.

## 24. Publicity

Neither party may issue a public announcement or use the other party's name, logo, or marks in publicity without prior written consent, except that we may identify the Customer privately to suppliers, advisers, insurers, or regulators where reasonably necessary.

## 25. Assignment and subcontracting

The Customer may not assign or transfer its rights or obligations under these terms without our prior written consent.

We may use employees, contractors, and subprocessors to deliver the Services, provided we remain responsible for our obligations under these terms.

## 26. Entire agreement

These terms, together with any order form, pilot agreement, written variation, privacy notice, acceptable use policy, and data processing agreement incorporated into them, set out the entire agreement between the parties in relation to the Services and supersede prior discussions on the same subject matter.

## 27. Variation

Any commercial change to these terms should be agreed in writing. We may update ancillary policies from time to time where reasonably necessary for legal, regulatory, security, or operational reasons. Updated policies will apply from the date published or notified, unless a longer notice period is required by law or expressly agreed.

## 28. Governing law and jurisdiction

These Platform Terms and any dispute or claim arising out of them are governed by the laws of **England and Wales**.

The courts of **England and Wales** have exclusive jurisdiction, unless mandatory law requires otherwise.

# HomeOrbit Acceptable Use Policy

**Version:** 1.0

**Last updated:** 15 April 2026

This Acceptable Use Policy applies to all use of the HomeOrbit website and platform.

## 1. Purpose

This policy is designed to protect HomeOrbit, Customers, users, data subjects, and connected systems from unlawful, unsafe, abusive, or irresponsible use.

## 2. Lawful and professional use only

You must use HomeOrbit only for lawful, authorised, and legitimate business purposes. You must not use the service:

- in breach of data protection law, employment law, safeguarding obligations, confidentiality duties, or any sector-specific rule that applies to your organisation;
- to process data you do not have authority to process;
- to harass, discriminate against, victimise, defame, or retaliate against any person;
- to facilitate fraud, deception, or unauthorised surveillance; or
- in any way that risks harm to children, young people, staff, service users, or other individuals.

## 3. No under-18 use

HomeOrbit must not be used by anyone under the age of 18.

## 4. Credentials and access

You must:

- keep passwords and access methods confidential;
- use only accounts assigned to you or properly authorised for your organisation;
- not share credentials or attempt to access another person's account without permission; and
- notify your organisation and HomeOrbit promptly if you suspect credentials have been compromised.

## 5. Security restrictions

You must not:

- introduce malware, ransomware, spyware, trojans, worms, logic bombs, or any other harmful code;
- attempt to probe, scan, penetrate, test, exploit, or bypass security controls without prior written permission from HomeOrbit;
- interfere with service performance, availability, logging, monitoring, or other users;
- perform automated scraping, mass extraction, or systematic harvesting of platform data except through approved workflows; or
- attempt to access data outside your own authorised scope.

## 6. Sensitive data handling

Because HomeOrbit may be used to hold sensitive data, users must act carefully and proportionately. You must not:

- upload sensitive data where it is unnecessary for the relevant workflow;
- misuse special category data, criminal offence data, safeguarding records, medication information, payroll details, DBS records, right-to-work records, or personnel information;
- download, print, export, or share data outside the platform except where authorised and necessary; or
- leave exported files or printed records unsecured.

## 7. Professional judgment

HomeOrbit supports operations and record keeping. It must not be used as the sole basis for:

- urgent safeguarding decisions;
- medical decisions;

- disciplinary findings;
- payroll calculations without review;
- medication decisions;
- legal conclusions; or
- any other high-risk decision where independent review is required.

Users must apply appropriate professional judgment and organisational oversight.

## 8. Content standards

Any information uploaded, written, or shared through HomeOrbit must, so far as reasonably possible:

- be accurate and not deliberately misleading;
- be relevant to the relevant operational purpose;
- be respectful and professional;
- not contain unlawful, threatening, obscene, discriminatory, or abusive content; and
- not infringe intellectual property, confidentiality, or privacy rights.

## 9. Audit and enforcement

HomeOrbit may monitor platform activity, logs, security events, and access patterns for lawful security, support, compliance, and service-management purposes.

A breach of this policy may result in:

- warning or required remediation;
- temporary suspension;
- restriction of access;
- termination of access;
- reporting to the Customer organisation;
- reporting to regulators or law enforcement where appropriate; and
- legal action.

## 10. Customer responsibility

Customer organisations are responsible for ensuring their own staff, managers, administrators, and contractors are trained and authorised to use HomeOrbit appropriately. Internal misuse by a Customer's users is the Customer's responsibility unless caused by HomeOrbit's own breach.

## 11. Changes to this policy

We may update this policy where needed to reflect legal, security, operational, or service changes. The latest published version will apply from the stated update date.

# HomeOrbit Privacy Notice

**Version:** 1.0

**Last updated:** 15 April 2026

This Privacy Notice explains how **Joshua Roberts trading as HomeOrbit** collects, uses, stores, and protects personal data in connection with the HomeOrbit website, enquiries, customer relationships, platform administration, and operation of the HomeOrbit service.

## 1. Identity and contact details

**Controller for this notice:** Joshua Roberts trading as HomeOrbit

**Address:** Apartment 414, 35 Greenland Street, Liverpool, L1 0AD, United Kingdom

**Email:** support@homeorbit.co.uk

Where this notice refers to **"HomeOrbit"**, **"we"**, **"us"**, or **"our"**, it means Joshua Roberts trading as HomeOrbit.

## 2. Scope of this notice

This notice covers personal data we process:

- as controller for website visitors, people who make enquiries, customer contacts, administrators, billing contacts, support contacts, and business relationship contacts;
- for account administration, platform security, audit, support, and service communications; and
- where we process limited operational metadata in our own right for service improvement, fraud prevention, legal compliance, and platform security.

For most personal data that a customer organisation uploads into the HomeOrbit platform for its own operational purposes, **the customer organisation is the controller and HomeOrbit acts as the processor**. That customer organisation is responsible for its own workforce privacy information and notices to its staff, workers, young people, service users, and other data subjects.

## 3. Categories of personal data we process as controller

Depending on how you interact with HomeOrbit, we may process:

### 3.1 Website and enquiry data

- name;
- work email address;
- employer or organisation name;
- phone number if you provide it;
- enquiry message content;
- records of communications with us.

### 3.2 Customer account and service relationship data

- names and business contact details of customer contacts;
- job title or role;
- account identifiers;
- login-related information;
- correspondence and support history;
- implementation notes and customer relationship history.

### 3.3 Security and technical data

- IP address;
- approximate geolocation derived from IP where available;
- browser and device information;
- operating system;
- timestamps and access logs;
- diagnostic and error information;
- audit and security events.

### 3.4 Platform administration and profile data

- user profile data;
- organisational assignment information such as company, home, role, and permissions;
- theme preference or other user preference information;
- profile images where uploaded.

### 3.5 Data processed within customer environments

When HomeOrbit acts as processor for a customer, the categories of data may include operational and workforce records that the customer chooses to use in the platform, including:

- employee and worker records;
- rota and attendance records;
- training records and certificates;
- payslip and payroll-related records;
- right to work and DBS-related records;
- personnel and HR records;
- policies and internal documents;
- signatures;
- forms and workflow records;
- young person records;
- medication-related information;
- budgets, receipts, and financial supporting documents; and
- other customer-controlled records uploaded to the platform.

Where this data is processed, we usually act only on the customer's instructions.

## 4. How we collect personal data

We collect personal data:

- directly from you when you contact us, make an enquiry, or use the website;
- from customer organisations that create or administer user accounts;
- from your use of the platform and website;
- from cookies and similar technologies where applicable;
- from infrastructure, security, and monitoring providers; and
- occasionally from public sources or referrals where relevant to legitimate B2B business contact.

## 5. Purposes and lawful bases

We process personal data for the following purposes and lawful bases:

### 5.1 Website enquiries and pre-contract communications

We use personal data to respond to enquiries, discuss the service, arrange demonstrations, and assess interest in HomeOrbit.

**Lawful basis:** legitimate interests, and where appropriate, steps at your request before entering into a contract.

### 5.2 Customer onboarding, administration, and service delivery

We use personal data to create accounts, manage customer relationships, configure the service, provide support, and communicate about the platform.

**Lawful basis:** contract, and legitimate interests in running and administering our service.

### 5.3 Platform security, authentication, fraud prevention, and incident management

We use personal data to secure accounts, detect suspicious activity, investigate incidents, preserve logs, and protect the service.

**Lawful basis:** legitimate interests, legal obligation where applicable, and contract where security is necessary to provide the service.

### 5.4 Product support, maintenance, troubleshooting, and service communications

We use personal data to diagnose issues, answer support requests, notify users of service matters, and maintain the platform.

**Lawful basis:** contract and legitimate interests.

### 5.5 Legal compliance, dispute management, and record keeping

We may retain or use personal data where needed to comply with law, respond to lawful requests, enforce rights, maintain business records, or defend legal claims.

**Lawful basis:** legal obligation and legitimate interests.

### 5.6 Limited service improvement and operational analytics

We may use technical and usage information to understand faults, improve reliability, refine workflows, and improve the service. We do not use customer operational records for advertising profiling.

**Lawful basis:** legitimate interests.

### 5.7 Cookies and similar technologies

Where non-essential cookies are introduced in future, we will rely on consent where required. Strictly necessary cookies are used on the basis that they are necessary to provide the service you request.

## 6. Special category and criminal offence data

As controller, we generally try to minimise the special category or criminal offence data we collect directly. Please do not send unnecessary sensitive data through public website enquiries.

As processor, HomeOrbit may host or otherwise process special category data and criminal offence data uploaded by customer organisations, including young person information, medication-related information, employment records, DBS-related records, and other sensitive care-sector data. In those cases, the customer organisation is responsible for identifying the relevant lawful basis and condition under applicable law.

## 7. Recipients and categories of recipient

We may share personal data, where necessary, with:

- hosting and infrastructure providers;
- database and storage providers;
- error monitoring and security providers;
- email and communications providers;
- professional advisers such as lawyers, insurers, accountants, or auditors under duties of confidentiality;

- regulators, courts, law enforcement, or competent authorities where required; and
- other service providers acting on our instructions.

A current subprocessor schedule is provided in the HomeOrbit legal pack and may be updated from time to time.

## 8. International transfers

HomeOrbit aims to use UK and EEA-friendly hosting arrangements where practical. However, some suppliers, service routes, support systems, or infrastructure components may involve processing outside the UK.

Where personal data is transferred internationally, we will use an appropriate transfer mechanism and appropriate safeguards as required by applicable law, such as:

- adequacy regulations;
- the UK International Data Transfer Agreement or Addendum;
- European Commission standard contractual clauses where relevant; or
- another lawful transfer mechanism.

## 9. Data retention

We keep controller-side personal data only for as long as reasonably necessary for the purposes described in this notice, including legal, security, support, contractual, and record-keeping needs.

Typical retention periods are described in the HomeOrbit Retention and Deletion Schedule. Customer-controlled data held in the platform is generally retained for the duration of the customer relationship and then handled under the relevant contract and data processing terms.

## 10. Security

We use reasonable technical and organisational measures designed to protect personal data. These measures may include access controls, role-based permissions, logging, supplier security controls, encryption in transit, managed hosting, secret management, and issue monitoring.

No internet-based system can be guaranteed to be completely secure. You should also keep your credentials secure and use appropriate internal controls.

## 11. Your rights

Where HomeOrbit acts as controller, and subject to legal limits and exemptions, you may have the right to:

- request access to your personal data;
- request correction of inaccurate data;
- request erasure;
- request restriction of processing;
- object to certain processing based on legitimate interests;
- request portability in certain cases; and
- complain to the Information Commissioner's Office.

If your personal data is primarily held by HomeOrbit on behalf of a customer organisation, you should normally direct your request to that organisation first, because it is usually the controller for that data. We will assist the relevant customer where required.

## 12. Complaints

You can raise privacy queries by contacting **support@homeorbit.co.uk**.

You also have the right to complain to the **Information Commissioner's Office (ICO)** if you believe your personal data has been handled unlawfully or unfairly.

## 13. Automated decision-making

HomeOrbit does not use personal data for solely automated decisions that produce legal effects or similarly significant effects on individuals as part of the general operation of the service, so far as we are aware at the date of this notice.

## 14. ICO registration

As at the date of this notice, HomeOrbit does not publish an ICO registration number. This may change as the service deployment and operational model evolve.

## 15. Changes to this notice

We may update this Privacy Notice from time to time to reflect legal, technical, operational, or service changes. The latest version published by us will apply from the date shown at the top of the notice.

# HomeOrbit Cookie Policy

**Version:** 1.0

**Last updated:** 15 April 2026

This Cookie Policy explains how HomeOrbit uses cookies and similar technologies on its website and platform.

## 1. What are cookies?

Cookies are small text files placed on your device when you visit a website. They can help a website operate securely, remember your preferences, maintain a logged-in session, and improve usability.

## 2. How HomeOrbit currently uses cookies

HomeOrbit currently uses cookies and similar technologies primarily for **strictly necessary** purposes, including:

- maintaining authenticated sessions;
- keeping users securely logged in;
- supporting platform security and request integrity;
- remembering theme or interface preferences, such as dark or light display mode; and
- ensuring core website and platform features work correctly.

At the date of this policy, HomeOrbit does **not** state that it uses advertising cookies or behavioural marketing cookies.

## 3. Types of cookies and similar technologies we may use

### 3.1 Strictly necessary cookies

These cookies are essential to provide the website or platform you have requested. Without them, core functions such as secure login, account session management, and requested preferences cannot operate properly.

Examples may include:

- session and authentication cookies;
- security and anti-abuse cookies;
- load-balancing or service integrity cookies where used by infrastructure providers; and
- preference cookies necessary to deliver your chosen interface mode.

### 3.2 Preference technologies

HomeOrbit may store certain preferences, such as theme mode or recently used account identifiers, using browser storage or cookies in order to improve usability.

### 3.3 Future optional technologies

If HomeOrbit later introduces optional analytics, performance measurement, or other non-essential technologies, the website and this policy will be updated and a consent mechanism will be implemented where required by law.

## 4. Lawful basis and consent

Where cookies or similar technologies are **strictly necessary** to provide the service you request, HomeOrbit relies on the applicable legal exemption for those technologies.

If HomeOrbit introduces **non-essential** cookies or similar technologies in future, it will seek consent where required before placing or reading them.

## 5. Managing cookies

You can usually manage cookies through your browser settings, including blocking or deleting cookies. Please note that blocking strictly necessary cookies may prevent parts of the website or platform from working properly.

## 6. Third-party services

Some third-party providers that support HomeOrbit may also use necessary cookies or similar technologies as part of providing infrastructure, authentication, security, or embedded functionality. Where relevant, those providers' own privacy and cookie information may also apply.

## 7. Contact

If you have questions about this Cookie Policy, contact **support@homeorbit.co.uk**.

## 8. Changes to this policy

We may update this policy from time to time to reflect changes in law, technology, or website operation. The latest version will apply from the date shown above.

# HomeOrbit Data Processing Agreement

**Version:** 1.0

**Last updated:** 15 April 2026

This Data Processing Agreement (**DPA**) forms part of the agreement between the Customer and **Joshua Roberts trading as HomeOrbit** for the provision of the HomeOrbit services.

## 1. Parties

### 1.1 Processor

**Joshua Roberts trading as HomeOrbit**

Apartment 414, 35 Greenland Street, Liverpool, L1 0AD, United Kingdom

support@homeorbit.co.uk

### 1.2 Controller

The Customer organisation using the HomeOrbit platform and determining the purposes and means of the processing of Customer Personal Data.

## 2. Interpretation

In this DPA:

- **Controller**, **Processor**, **Data Subject**, **Personal Data**, **Personal Data Breach**, **Processing**, **Special Category Data**, and **Supervisory Authority** have the meanings given in applicable Data Protection Law.
- **Customer Personal Data** means Personal Data processed by HomeOrbit on behalf of the Customer in connection with the Services.
- **Data Protection Law** means all laws applicable to the processing of Personal Data under this DPA, including the UK GDPR, the Data Protection Act 2018, PECR where relevant, and any legislation replacing or amending them.

## 3. Roles of the parties

The parties acknowledge and agree that:

- the Customer is the **Controller** of Customer Personal Data; and
- HomeOrbit is the **Processor** of Customer Personal Data,

except to the extent that HomeOrbit acts as an independent controller for its own business administration, security, legal compliance, billing, support records, or website/enquiry data.

## 4. Customer instructions

HomeOrbit will process Customer Personal Data:

- only on the Customer's documented instructions;
- as necessary to provide the Services under the agreement;
- as necessary to comply with applicable law; or
- as otherwise agreed in writing.

The agreement, platform configuration, authorised user actions, and this DPA together form the Customer's documented instructions unless and until varied in writing.

If HomeOrbit believes an instruction infringes Data Protection Law, HomeOrbit may inform the Customer and may suspend the affected processing until the issue is resolved.

## 5. Confidentiality

HomeOrbit will ensure that persons authorised to process Customer Personal Data are subject to an appropriate duty of confidentiality.

## 6. Security of processing

Taking into account the state of the art, the costs of implementation, the nature, scope, context, and purposes of processing, and the risk to individuals, HomeOrbit will implement appropriate technical and organisational measures to protect Customer Personal Data.

Those measures are described at a high level in the Security Schedule to this legal pack and may be updated from time to time provided that the overall level of protection is not materially reduced.

## 7. Subprocessors

The Customer grants HomeOrbit general authorisation to engage subprocessors in connection with the Services.

HomeOrbit will:

- maintain information about its current material subprocessors;
- impose data protection obligations on subprocessors that are substantially similar to those imposed on HomeOrbit under this DPA, to the extent applicable to the services they perform; and
- remain responsible for the performance of its subprocessors' data protection obligations to the extent required by law.

A current subprocessor schedule is included in this legal pack.

## 8. International transfers

HomeOrbit will not transfer Customer Personal Data internationally except as permitted by Data Protection Law and only where an appropriate safeguard or lawful transfer mechanism is in place where required.

## 9. Assistance to the Customer

Taking into account the nature of the processing and the information available to HomeOrbit, HomeOrbit will provide reasonable assistance to the Customer with:

- data subject rights requests;
- security obligations;
- personal data breach notifications;
- data protection impact assessments; and
- consultations with supervisory authorities,

to the extent required by Data Protection Law and reasonably within HomeOrbit's control.

Where the request results from the Customer's own configuration, conduct, or legal obligations, HomeOrbit may charge reasonable costs if the agreement allows this or if agreed in writing in advance.

## 10. Personal data breaches

If HomeOrbit becomes aware of a confirmed Personal Data Breach affecting Customer Personal Data, HomeOrbit will notify the Customer **without undue delay** after becoming aware of it.

That notification will, where reasonably possible, include:

- the nature of the breach;
- the categories of data concerned;
- the likely consequences;
- measures taken or proposed; and
- a contact point for further information.

HomeOrbit may provide information in phases if full details are not available immediately.

## 11. Return or deletion of data

On termination or expiry of the Services, HomeOrbit will, at the Customer's choice and subject to the agreement, either return or delete Customer Personal Data after the applicable export period, unless applicable law requires storage.

The Customer acknowledges that deletion from backups and disaster recovery systems may not be instantaneous and residual copies may remain until overwritten in the ordinary backup cycle, provided they remain protected and inaccessible in the ordinary course.

## 12. Information and audits

HomeOrbit will make available to the Customer information reasonably necessary to demonstrate compliance with this DPA.

Where reasonably required and proportionate, the Customer may request an audit or inspection relating to HomeOrbit's processing of Customer Personal Data, subject to:

- reasonable prior written notice;
- confidentiality obligations;
- reasonable scope and frequency limits;
- protection of other customers' information and platform security;
- avoidance of disruption; and
- use of independent auditors where requested by HomeOrbit.

HomeOrbit may satisfy audit requests through documentation, certifications, summaries, completed questionnaires, or virtual review before any on-site or intrusive audit is considered.

## 13. Customer obligations

The Customer warrants and undertakes that it:

- has complied and will comply with Data Protection Law in relation to Customer Personal Data and its use of the Services;
- has all necessary lawful bases, notices, permissions, policies, and internal authority for the processing it instructs HomeOrbit to carry out;
- will not instruct HomeOrbit to process Personal Data unlawfully;

- is responsible for the accuracy, quality, and lawfulness of Customer Personal Data and the means by which it acquired it; and
- will respond to data subject requests and regulatory correspondence as controller unless otherwise agreed.

### 14. Liability

Liability under this DPA is subject to the liability provisions in the main agreement unless Data Protection Law requires otherwise.

### 15. Order of precedence

If there is a conflict between this DPA and the main agreement in relation to data protection matters, this DPA will prevail to the extent of the conflict.

### 16. Governing law

This DPA is governed by the laws of England and Wales. The courts of England and Wales have exclusive jurisdiction, unless mandatory law requires otherwise.

---

## Schedule 1 - Subject matter, duration, nature and purpose

### A. Subject matter

The processing of Customer Personal Data through the HomeOrbit platform and related support, maintenance, hosting, storage, security, and communications services.

### B. Duration

For the duration of the Customer's use of the Services, plus any limited post-termination period required for export, deletion, legal compliance, security, dispute resolution, or backup integrity.

### C. Nature of processing

Collection, recording, organisation, structuring, storage, hosting, viewing, retrieval, consultation, use, disclosure by transmission where instructed, restriction, erasure, and destruction.

### D. Purpose

To provide, secure, host, maintain, support, and improve the Services for the Customer, and to process Customer Personal Data strictly on the Customer's behalf in connection with the Customer's use of the platform.

## Schedule 2 - Categories of data subjects

Depending on the Customer's use of the Services, data subjects may include:

- employees and workers;
- agency, bank, or relief staff;
- contractors and consultants;
- managers and administrators;
- applicants where records are uploaded;
- young people or service users;
- family contacts or related individuals where the Customer uploads such information;
- payroll contacts;
- training providers or external professionals named in records; and
- other individuals whose data the Customer chooses to upload lawfully.

## Schedule 3 - Categories of personal data

Depending on the modules and workflows used, Customer Personal Data may include:

- name, role, job title, identifiers, and contact details;
- rota, attendance, working time, and shift records;

- training records, qualifications, certificates, and reminders;
- policies, acknowledgements, forms, notes, and workflow entries;
- payroll-related and payslip information;
- HR and personnel records;
- right to work information;
- DBS-related records and other criminal offence data uploaded by the Customer;
- signatures;
- young person records;
- medication-related information;
- receipts, budgets, and supporting documents;
- uploaded files, images, PDFs, and attachments;
- account assignment and permission data; and
- audit trail information.

## Schedule 4 - Special category and criminal offence data

The Customer may choose to upload special category data and criminal offence data, including health-related information, medication-related information, safeguarding information, and DBS-related records. The Customer is responsible for ensuring an appropriate lawful basis and condition applies to such processing.

## Schedule 5 - Technical and organisational measures summary

HomeOrbit applies measures designed to include, where relevant and appropriate:

- role-based access control and scoped permissions;
- authenticated access controls;
- encryption in transit;
- managed cloud hosting and managed database/storage services;
- activity logging and audit features in relevant parts of the platform;
- secret and credential management through managed deployment tooling;
- issue and error monitoring;
- patching and code updates through a controlled source management and deployment process;
- signed URLs or scoped file access for private stored content where implemented;
- reasonable restriction of administrative access; and
- incident investigation and remediation processes.

This schedule describes measures at a summary level and does not require disclosure of information that would weaken security.

# HomeOrbit Subprocessor Schedule

**Version:** 1.0

**Last updated:** 15 April 2026

This schedule lists the main third-party providers that may process personal data on behalf of HomeOrbit customers in connection with the service as operated at the date of this schedule.

## 1. Current subprocessors and service providers

### 1.1 Supabase

**Role:** Managed database, authentication, storage, and backend platform services.

**Relevant data:** Account data, authentication data, database records, uploaded files, and other customer content stored through the platform.

**Relevant region/configuration known to HomeOrbit:** Project configured in **eu-west-2 (London)**.

### 1.2 Vercel

**Role:** Application hosting, web delivery, and server-side runtime infrastructure.

**Relevant data:** Website requests, application traffic, logs, limited request metadata, and any personal data processed through application requests handled by the deployed service.

**Relevant note:** Depending on deployment configuration and provider routing, processing may involve infrastructure outside the UK.

### 1.3 Sentry

**Role:** Error monitoring, issue tracking, and diagnostic reporting.

**Relevant data:** Error and diagnostic data, which may include technical identifiers and, depending on configuration and events, user or request-related metadata necessary to investigate faults.

**Relevant note known to HomeOrbit:** Current configuration uses a **de.sentry.io** ingest endpoint associated with Sentry's EU region.

## 2. Additional providers

HomeOrbit may also use professional advisers, email or communications providers, domain providers, source control platforms, and other service providers in the ordinary operation of the business. Those providers will only act as subprocessors to the extent they process customer personal data on HomeOrbit's behalf in connection with the service.

## 3. Changes to this schedule

HomeOrbit may update this schedule from time to time to reflect operational, security, or infrastructure changes. Updated schedules may be published or otherwise notified to customers.

## 4. Questions

For subprocessor queries, contact **support@homeorbit.co.uk**.

# HomeOrbit Retention and Deletion Schedule

**Version:** 1.0

**Last updated:** 15 April 2026

This schedule sets out HomeOrbit's standard retention approach. It should be read alongside the Privacy Notice, Platform Terms, and Data Processing Agreement.

## 1. General approach

HomeOrbit keeps personal data only for as long as reasonably necessary for the purpose for which it was collected, together with any additional period required for security, legal compliance, dispute handling, backups, or evidential needs.

Customers remain responsible for setting and applying their own retention rules for records they control in the platform, including any sector-specific retention obligations.

## 2. Controller-side retention periods

### 2.1 Website enquiries and sales enquiries

**Standard retention:** up to **12 months** from the last meaningful contact, unless a longer period is needed to continue discussions or keep an accurate business record.

### 2.2 Customer contact records and implementation communications

**Standard retention:** for the duration of the customer relationship and up to **24 months** afterwards, unless longer retention is needed for legal, tax, contractual, security, or dispute reasons.

### 2.3 Support tickets and troubleshooting correspondence

**Standard retention:** up to **24 months** after closure of the relevant support issue, unless a longer period is reasonably required for recurring issues, security, or legal defence.

### 2.4 Security, authentication, and audit logs

**Standard retention:** retained for as long as reasonably necessary for security monitoring, incident investigation, platform integrity, and evidential needs. The exact period may vary depending on system design and provider defaults.

### 2.5 Billing and financial records

**Standard retention:** retained for the period required by applicable tax and accounting law.

## 3. Customer-controlled platform data

Customer-controlled data stored in the HomeOrbit platform is generally retained:

- throughout the active term of the customer relationship; and
- for a post-termination export period of **30 days**, unless a different arrangement is agreed in writing.

After the export period, HomeOrbit may delete or render inaccessible Customer Data unless retention is required by law or reasonably necessary for security, backup integrity, fraud prevention, or dispute resolution.

## 4. Backups and residual copies

Deletion from live systems may not result in instantaneous removal from backups or disaster recovery copies. Where residual copies remain, they are expected to remain protected and to be overwritten in the ordinary backup lifecycle.

## 5. Early deletion requests

Where HomeOrbit acts as controller, individuals may request deletion subject to legal rights and exemptions.

Where HomeOrbit acts as processor, deletion requests relating to customer-controlled data should normally be directed to the relevant customer controller. HomeOrbit will assist where required under the DPA.

## 6. Litigation, incidents, and legal holds

HomeOrbit may retain data for longer than the standard period where reasonably necessary to:

- investigate incidents or misuse;
- comply with legal obligations;
- establish, exercise, or defend legal claims;
- preserve evidence;
- respond to regulators or law enforcement; or
- protect the rights, property, or safety of HomeOrbit, customers, or others.

## 7. Review

Retention periods and practices may be reviewed and updated from time to time as HomeOrbit matures operationally and legally.

# HomeOrbit Security and Support Policy

**Version:** 1.0

**Last updated:** 15 April 2026

This document summarises HomeOrbit's current operational approach to security, support, maintenance, and incident handling.

## 1. Security principles

HomeOrbit is designed for use in a care-sector context where confidentiality, role-based visibility, and tenant separation are important. HomeOrbit aims to apply reasonable and proportionate security measures based on the nature of the service and the data processed.

## 2. Security measures summary

HomeOrbit's current approach includes measures designed to support:

- authenticated access to the platform;
- role-based permissions and scoped visibility;
- segregation between customer environments and data scopes;
- encryption in transit using modern HTTPS/TLS transport;
- managed infrastructure providers;
- controlled deployments through managed source control and hosting workflows;
- logging, diagnostics, and monitoring;
- secrets and environment-based credential handling;
- rate limiting or anti-abuse controls on sensitive routes where implemented; and
- restriction of access to files and stored assets through private storage and time-limited access mechanisms where implemented.

HomeOrbit does not represent that any system is invulnerable, and Customers must also maintain good internal security hygiene.

## 3. Customer-side security responsibilities

Customers should:

- assign access only to authorised adult users;
- promptly disable access for leavers or role changes;
- use strong passwords and secure devices;
- avoid sharing accounts;
- minimise unnecessary uploads of sensitive information;
- maintain their own internal policies and training;
- review permissions, data quality, and exports regularly; and
- report suspected incidents promptly.

## 4. Support model

At the date of this policy, HomeOrbit is in an early operational stage and may be delivered through a pilot and implementation model. Support is therefore provided on a **reasonable endeavours** basis, generally during UK business hours, with additional practical support where separately agreed through implementation arrangements.

No formal guaranteed response times, service credits, or 24/7 commitments are granted unless separately agreed in writing.

## 5. Maintenance and updates

HomeOrbit may deploy:

- bug fixes;
- security fixes;
- design and UX changes;
- workflow changes;
- feature enhancements; and
- infrastructure changes.

Some changes may be made without prior notice where urgently required for security, legal, or operational reasons. Where practicable, material planned changes affecting customers will be communicated in advance.

## 6. Incident reporting

Customers should report security incidents, suspected breaches, lost credentials, or suspicious activity to **support@homeorbit.co.uk** as soon as possible.

HomeOrbit will investigate reported issues and, where HomeOrbit is acting as processor and becomes aware of a confirmed breach affecting Customer Personal Data, HomeOrbit will notify the relevant customer controller without undue delay.

## 7. Availability

HomeOrbit aims to keep the service available and stable, but does not guarantee uninterrupted or error-free access. Availability may be affected by:

- planned maintenance;
- third-party infrastructure issues;
- internet or network failures;
- cyber incidents;
- force majeure events; or
- service development work.

## 8. Security reviews and improvement

HomeOrbit may continue to refine its legal, technical, and operational controls over time as the service develops, including changes to monitoring, policies, support processes, or hosting configuration.

# HomeOrbit Accessibility Statement

**Version:** 1.0

**Last updated:** 15 April 2026

HomeOrbit is committed to improving the accessibility and usability of its website and platform.

## 1. Our approach

We aim to make HomeOrbit as clear, usable, and accessible as reasonably possible for adult users across desktop and mobile devices. Accessibility is considered during design and development, including page structure, colour contrast, keyboard use, and responsive layouts.

## 2. Current status

HomeOrbit is an evolving product. Accessibility improvements are ongoing as part of the service's continued development. Some areas may not yet meet every accessibility expectation at all times, particularly where features are newly introduced or under active iteration.

## 3. Known approach areas

We aim, where reasonably practicable, to support:

- readable text and clear layouts;
- responsive design across common screen sizes;
- keyboard-friendly navigation in core areas;
- meaningful labels and prompts in user workflows; and
- consistent navigation and feedback states.

## 4. Feedback and requests

If you encounter an accessibility barrier on HomeOrbit, or need information in a different format, contact:

**support@homeorbit.co.uk**

Please include:

- the page or feature you were using;
- what problem you experienced; and
- what support or format you need.

## 5. Ongoing improvement

Accessibility will continue to be reviewed as HomeOrbit grows and moves from pilot use into broader deployment.

# HomeOrbit Enquiry Privacy Summary

**Version:** 1.0

**Last updated:** 15 April 2026

This short summary can be used alongside a website enquiry form or enquiry modal.

When you contact HomeOrbit, we use the information you provide to respond to your enquiry, manage pre-contract discussions, and keep a record of our communications.

**Controller:** Joshua Roberts trading as HomeOrbit

**Contact:** support@homeorbit.co.uk

We usually use your data because it is necessary for our legitimate interests in responding to business enquiries and, where relevant, to take steps at your request before entering into a contract.

We may share enquiry data with hosting, email, and support providers acting on our behalf. We keep enquiry records only for as long as reasonably necessary, typically up to 12 months from the last meaningful contact unless a longer period is justified.

You can ask about your privacy rights by contacting **support@homeorbit.co.uk**. Full details are set out in the HomeOrbit Privacy Notice.