LAKESIDE HANDY HIRE

# Privacy Policy

Version 1.3 | Effective 7 September 2026

This downloadable copy contains the same full policy available on the Lakeside Handy Hire website. The website presents the sections as expandable panels so customers can read the short version first and open the detail only when they want it.

| | |
|---|---|
| **Lakeside Handy Hire Ltd** | Data controller for the customer information described in this policy. |
| **Company number** | 17362091 |
| **Service base** | Barrow-in-Furness, Cumbria |
| **Contact** | Use the Lakeside Contact page for privacy requests or complaints. |

## Contents


**01 - Controller** - Who is responsible for your information?

**02 - Information collected** - What personal information do we use?

**03 - Purposes and lawful bases** - Why do we use it?

**04 - Didit identity verification and authentication** - How do identity and face checks work?

**05 - Payments** - How is payment information handled?

**06 - Hire, handover and support records** - What do we record when equipment changes hands?

**07 - Equipment security tracking** - Do hired items use location or security tracking?

**08 - Recipients and processors** - Who may receive personal information?

**09 - International processing** - Can information leave the UK?

**10 - Retention** - How long do we keep information?

**11 - Cookies and similar storage** - What does the website store on your device?

**12 - Your rights** - What can you ask us to do?

**13 - Security** - How do we protect information?

**14 - Children** - The hire service is for adults.

**15 - Contact, complaints and updates** - Questions or a privacy request?

01 - Controller

# Who is responsible for your information?

Lakeside Handy Hire Ltd , company number 17362091 , is the data controller for the customer information described in this policy. Lakeside is based in Barrow-in-Furness and trades as Lakeside Handy Hire.

We decide why personal information is needed for bookings, identity checks, payments, handovers, support, safety, fraud prevention and legal records. Using another company to perform a task does not remove our responsibility for choosing appropriate providers and handling your rights.

Contact us through the Lakeside Contact page . Choose Identity verification or General question and explain that your message concerns personal information.

02 - Information collected

# What personal information do we use?

## Contact and account details

Name, email, phone number, address, account credentials and communication preferences.

## Booking information

Equipment, dates, availability, delivery or collection details, pricing, consumables, locker or handover details and booking history.

## Agreement and checkout evidence

Agreement version, statements presented, acceptance timestamps, checkbox interaction records and whether the Hire Agreement link was opened, including first or last open time and open count where recorded.

## Identity information

Date of birth, identity-document information, proof of address where requested, verification status, session references and verification-validity dates.

## Images and biometric information

Identity documents, selfies, facial images, liveness captures, videos and biometric templates or comparison signals used for verification or optional returning-customer authentication.

## Payment information

Payment status, amount, transaction reference, limited card details such as brand and last digits, refunds and charge records.

## Equipment and handover evidence

Condition photographs or video, serial numbers, accessories, condition scores, signatures or confirmations, timestamps, return records and delivery information.

## Locker and console events

Where enabled, booking lookup, authentication result, locker or asset released, check-out and check-in actions, consumables collected and related timestamps.

## Equipment location and security data

For selected tracked equipment, data from one or more GPS, Bluetooth, network-based or other electronic security devices, including asset location, movement, time, device status, geofence or tamper information where the technology provides it.

### Support and incident information

Messages, calls where used, fault reports, photographs, complaints, cancellations, damage, loss, theft, recovery and insurance information.

### Technical and security data

IP address, browser, device, session, login, cookie, fraud-prevention and website-security logs.

We may receive information directly from you, from a person authorised to act for you, from our website and booking system, from equipment or security devices used during a hire, or from providers involved in verification, payments, delivery, security, asset recovery and fraud prevention.

**03 - Purposes and lawful bases**

# Why do we use it?

| Purpose | Typical information | Lawful basis |
|---|---|---|
| Create accounts, quote, book and supply equipment | Contact, account, booking, address, delivery, collection and handover details. | Contract or steps requested before entering a contract. |
| Record agreement presentation and acceptance | Agreement version, statements, checkbox and acceptance timestamps, order reference and agreement-link open telemetry where recorded. | Contract and legitimate interests in clear contracting, evidence and dispute prevention. |
| Take payment, issue refunds and keep financial records | Transaction, invoice, booking and limited payment information. | Contract and legal obligation. |
| Verify the named hirer and prevent fraud | ID, proof of address where required, selfie, liveness, biometric and risk signals. | Article 6: contract and/or legitimate interests. Where biometric recognition is used to uniquely identify a person, a separate Article 9 condition is also required; Lakeside expects to rely on explicit consent where appropriate. |
| Authenticate a returning customer or locate a booking by face where chosen | Live face, liveness result, reference portrait or biometric comparison signal and booking/account reference. | Article 6: legitimate interests and/or consent depending on the flow. Article 9: explicit consent where Lakeside relies on consent for special-category biometric recognition. |
| Record handover, condition, damage and return | Photos, video, serial numbers, condition scores, timestamps, signatures, locker events and incident records. | Contract and legitimate interests in protecting customers, equipment and legal claims. |
| Protect and recover selected tracked equipment | Asset location and security data from GPS, Bluetooth, network-based or other electronic tracking devices, including movement, time, device status, geofence or tamper information where available. | Legitimate interests in theft prevention, asset recovery, enforcing agreed location restrictions and investigating non-return, tracker interference or serious misuse. |
| Provide support and resolve complaints | Messages, booking records, evidence and account information. | Contract and legitimate interests in customer service and dispute resolution. |
| Secure the website and investigate misuse | Technical logs, IP, device, login and risk information. | Legitimate interests, recognised crime-prevention interests where applicable, and legal obligation. |
| Optional marketing | Contact details and preferences. | Consent or another lawful basis permitted for the specific communication. You can opt out. |

**Our legitimate interests**
These include operating a safe hire service, confirming the named hirer, preventing fraud and theft, protecting and recovering equipment, maintaining evidence, resolving disputes, securing the website and improving customer support. Before relying on legitimate interests for a new or intrusive use, Lakeside considers the purpose, necessity, proportionality, reasonable expectations and the customer's rights.

# How do identity and face checks work?

Lakeside uses Didit to power identity, liveness, facial-comparison and fraud checks. Lakeside decides why a check is needed, which checks are enabled and how the result is used. For the configured verification service, Didit normally acts as our data processor. Didit may act as an independent controller for limited purposes such as its own security, abuse prevention, audit, legal compliance and legal claims.

## Lakeside

Controller: requests the check, selects the workflow, decides whether equipment can be released, sets the normal verification cycle and handles customer rights.

## Didit

Verification and authentication provider: may process identity documents, extracted document data, proof of address, selfies, video, liveness and facial comparison data, reference portraits, device and IP information, fraud signals, results and audit records.

## Full verification and the 180-day cycle

A successful full identity verification is normally treated by Lakeside as current for up to 180 days from approval . We may require a fresh check sooner if important details change, the account or booking presents increased risk, there is a suspected identity problem or another lawful reason makes re-verification appropriate. After the 180-day period, the next relevant hire or handover may require a new full verification.

## Quick returning-customer authentication

During a current verification period, Lakeside may offer a quicker face and liveness check at collection, delivery, locker release or another handover point. This can compare a new live capture with a trusted portrait from an earlier approved verification. A successful quick authentication does not restart or extend the 180-day full-verification period.

## "Find my booking by face"

Where this optional feature is enabled on a collection or locker console, a customer may choose to ask the system to locate their booking from a live face scan. This may involve a one-to-many facial search against enrolled returning-customer faces in the relevant Lakeside application. It is not required just to browse the website. A customer can instead use a booking reference, QR code, account details or an appropriate manual identification route.

## Checks we may request

- Photo ID, such as a passport or driving licence.
- A selfie, short video or liveness check to confirm a real person is present.
- Facial comparison between the person and the identity document or a trusted reference portrait.
- Proof of address for a higher-value, unusual or risk-sensitive hire.
- A repeat or refreshed check when verification is old, details have changed or risk requires it.
- Technical and fraud checks involving IP, device, session and risk indicators.

## Choice, consent and manual alternatives

Biometric recognition used to uniquely identify a person is treated as special-category biometric data under UK data-protection law. Where Lakeside relies on explicit consent for that biometric use, the consent request must be specific, separate and clear. Optional convenience features such as face-based booking lookup will not be the only route: customers may use a non-biometric method such as booking details, QR code or a suitable manual photo-ID check. A customer may withdraw consent for future biometric processing, although Lakeside still needs to establish the identity of the named hirer before releasing equipment and may refuse release if identity cannot be established safely by an appropriate alternative.

## Access and automated checks

Depending on the workflow, Lakeside may receive a verification or authentication result, risk indicators, submitted details or supporting evidence. Access is restricted and should only be used where necessary for review, fraud prevention, a dispute, safety, a legal requirement or the release or recovery of equipment.

Didit uses automated checks for document integrity, liveness, face match and fraud signals. A failed or uncertain result may stop automatic progression, but the customer can contact Lakeside for an appropriate manual review or alternative route. Lakeside does not intend to make a final legally or similarly significant decision solely by automated means.

### Didit legal information

Didit publishes a verification-specific privacy notice as well as its general privacy policy. These provider notices sit alongside Lakeside's policy rather than replacing it.

Didit Verification Privacy Notice

Didit End User Terms for Identity Verification

Didit Privacy Policy

**05 - Payments**

## How is payment information handled?

Payments are handled by the payment option shown at checkout. Stripe may be used for card, Apple Pay or Google Pay transactions. TrueLayer may be used where a Pay by Bank or open-banking payment option is offered. Lakeside does not store the full card number or card security code in its own website database.

We may receive and retain the payment amount, status, date, transaction reference, payment method type, limited card information, refund information, fraud signals and evidence needed to reconcile or dispute a transaction.

A saved payment method or provider token is not unlimited permission to take money. Any additional post-hire charge must be supported by the hire agreement, reasonable evidence and the payment provider's process.

### Payment-provider privacy

Only the provider used for the payment method you choose receives the information needed for that service. Those providers may also process some information as independent controllers for security, fraud prevention, legal compliance or their regulated payment services.

Stripe Privacy Policy

Stripe Privacy Center

TrueLayer Privacy Notice

TrueLayer End User Terms

### Job Fuel and non-hire purchases

If you buy Job Fuel or another non-hire product without hiring equipment, Lakeside uses the contact, order and payment information reasonably needed to process the purchase, manage stock, provide collection or delivery where applicable, handle refunds or complaints and keep required financial records. Identity verification and the Hire Agreement are not required solely because a customer purchases Job Fuel where no hire equipment is included in the order.

**06 - Hire, handover and support records**

## What do we record when equipment changes hands?

Lakeside records the condition and supplied accessories at preparation, handover and return. This protects both sides by showing what was supplied, its visible condition, when custody changed and what came back. The same guided process may be used by staff on a phone or tablet, during delivery, or at a self-service collection or locker point where enabled.

- Equipment photographs focus on the asset, serial number, accessories and visible condition.

- Check-out and check-in may record a visible-condition score, checklist answers, fuel or battery state and completion timestamp.
- Delivery or collection records may include the named hirer, authentication result, confirmation, time and location details.
- Locker or self-service events may record which booking, locker, item and consumables were released or returned and when.
- Fault, damage or contamination reports may include customer-supplied photographs or video.
- Support messages are retained where needed to manage the booking, complaint or legal record.
- We do not use identity documents, selfies, biometric data or equipment-condition evidence for advertising.

**07 - Equipment security tracking**

# Do hired items use location or security tracking?

Selected equipment may contain one or more GPS, Bluetooth, network-based or other electronic security trackers. Customers are informed that tracking or security technology may be fitted to hired equipment. Because a tracker travels with the asset, location or movement information can sometimes reveal where the named hirer, delivery address or premises are while the equipment is on hire. Lakeside therefore treats asset-location data as personal information where it can be linked to an identifiable customer.

Tracking is used for proportionate asset-security purposes: preventing and investigating theft or loss, locating overdue or non-returned equipment, supporting lawful recovery, investigating tracker removal or tampering, and checking a serious breach of the agreed equipment-use location. The customer books the location where the equipment will be used, and Lakeside currently accepts hire use locations within its 25-mile straight-line service area . Any booking-specific movement or location restriction is shown in the Hire Agreement or booking information.

- Depending on the technology used, tracker data may include current or historic asset location, movement, time, device status, geofence or tamper information.
- Tracking devices may use GPS, Bluetooth, participating device networks, mobile networks or another asset-security technology.
- Access is limited to people or providers who need it for hire operations, security, recovery, a dispute or a legal requirement.
- Lakeside does not use equipment-location data for advertising, sell it as customer-location data or build unrelated customer movement profiles.
- Routine tracking is not intended to become a permanent history of a customer's movements. Where practical, review is limited to what is needed for asset management and security rather than continuous manual observation of a customer.
- Relevant location evidence may be preserved and shared with a tracker provider, insurer, lawful recovery provider, police, court or adviser where reasonably necessary and lawful.
- The Hire Agreement prohibits removing, disabling, shielding, damaging or deliberately interfering with fitted asset-security or tracking equipment.

> **Lawful basis for equipment tracking**
> Lakeside expects to rely on legitimate interests in protecting hired assets, preventing theft, recovering property and enforcing proportionate security restrictions. Before live customer-linked tracking is used, Lakeside should document a legitimate interests assessment and keep the necessity, proportionality, access controls and retention period under review.

**08 - Recipients and processors**

# Who may receive personal information?

We only share information where it is reasonably necessary for the stated purpose, permitted by law and subject to appropriate access controls or contracts.

- Didit for identity, liveness, biometric, document, returning-customer authentication, optional face-based booking lookup and fraud verification.
- Stripe, TrueLayer (where offered), banking and accounting providers for transactions, refunds, payment authentication, fraud controls and financial records.
- Website, hosting, WordPress, WooCommerce and security providers used to operate the booking service.
- Email and communications providers used to receive enquiries and send booking or support messages.
- Delivery, locker, equipment-security, tracker or recovery providers where necessary to complete a handover, operate a collection point, protect an asset or support lawful recovery.
- Insurers, legal advisers, accountants, debt-recovery or fraud specialists where a claim, dispute or legal issue requires it.
- Police, courts, regulators, HMRC or public authorities where disclosure is required or lawfully justified.

Lakeside does not sell customer information as a marketing database. The Northridge project branding does not mean customer identity documents are routinely shared with Northridge Equity Group.

**09 - International processing**

# Can information leave the UK?

Some providers may process or support information outside the UK. This can include identity, payment, hosting, communications, security or support providers. Didit states that verification data may be processed outside the country where the verification begins; Stripe and TrueLayer also publish their own international-transfer information in their privacy notices.

Where a restricted international transfer occurs, Lakeside and its provider must use an applicable safeguard, such as adequacy regulations, approved contractual terms or another lawful transfer mechanism.

**10 - Retention**

# How long do we keep information?

We keep personal information only for as long as reasonably needed for the purpose, legal record, dispute or claim. The periods below are normal targets. A shorter period may apply, or a longer legal hold may be needed for an active complaint, investigation, insurance matter, tax enquiry or court claim.

| Record | Normal retention target | Reason |
|---|---|---|
| Contact enquiries with no booking | Up to 24 months after the enquiry closes. | Customer support, follow-up and complaint evidence. |
| Account and profile information | While active, then normally up to 6 years after the last booking or account closure where linked to a transaction. | Contract history, fraud prevention, claims and business records. |
| Bookings, Hire Agreement evidence, invoices, payments and refunds | Normally up to 6 years after the relevant hire or for the accounting period required by law, whichever is appropriate. | Accounting, tax, contract and dispute records, including agreement version, acceptance timeline and agreement-open telemetry. |
| Condition photos, handover, locker or console events, faults, damage and complaints | Normally up to 6 years after the hire closes, or until a related claim or dispute ends. | Safety, evidence, insurance and legal claims. |
| Didit identity documents, selfies, liveness and biometric verification or authentication media | Lakeside target: no longer than 180 days from the relevant verification/authentication session, unless deleted earlier or a lawful hold is needed. | Keeps the live verification cycle workable without retaining identity media indefinitely. |

| Record | Normal retention target | Reason |
|---|---|---|
| Full-verification validity | Normally 180 days from approval. A later quick face authentication does not reset this period. | Reduce repeat document collection while still requiring periodic refreshed identity verification. |
| Verification or authentication result, date, status, session reference and consent/audit record | Normally up to 6 years after the last relevant hire. | Show that the named hirer was checked and support fraud, contract and legal records. |
| Routine equipment-location or security-tracking logs | Normally up to 12 months after the relevant hire. Relevant extracts may be kept up to 6 years where needed for a dispute, theft, recovery, insurance or legal claim. | Asset security, recovery, incident investigation and evidence while avoiding unnecessary long-term movement history. |
| Website and security logs | Normally up to 12 months, unless needed for an active security or fraud investigation. | Security, abuse prevention and incident investigation. |
| Marketing preferences | Until consent is withdrawn or the preference is no longer needed; a minimal suppression record may be kept. | Respect opt-outs and avoid sending unwanted marketing. |

**Didit retention setting**
Didit currently allows customers to configure general verification-data retention per application. Lakeside's public target is 180 days for verification/authentication media needed for the current identity cycle. The live Didit application must therefore be configured to match this policy as closely as the provider permits; separate audit/result records may be retained longer where needed for contract, fraud, consent or legal evidence.

**11 - Cookies and similar storage**

# What does the website store on your device?

The website may use essential cookies or similar storage to keep the basket working, maintain a secure login, remember booking or session information, protect forms and prevent fraud. These are necessary for requested website functions.

Non-essential analytics, advertising or marketing technologies should only be used with the appropriate notice and consent control where required. You can also manage cookies through your browser, although blocking essential cookies may break the basket, checkout, account or verification journey.

**12 - Your rights**

# What can you ask us to do?

Depending on the information, purpose and lawful basis, you may have the following rights. They are not all absolute, and the law may permit or require us to retain some records.

## Access

Ask for a copy of personal information and related details.

## Correction

Ask us to correct inaccurate or incomplete information.

## Erasure

Ask for deletion where there is no lawful reason to continue keeping it.

## Restriction

Ask us to limit use while accuracy or lawfulness is reviewed.

### Object

Object to processing based on legitimate interests or direct marketing.

### Portability

Receive certain information in a reusable format where the right applies.

### Withdraw consent

Withdraw consent for future processing without affecting earlier lawful use.

### Human review

Ask us to review a significant decision that appears to rely on automation.

We may need to confirm your identity before responding so that personal information is not disclosed to the wrong person. For a Didit verification session, contact Lakeside first; Didit may support us in responding where it acts as our processor.

**13 - Security**

## How do we protect information?

- Access to customer and identity information is restricted to people who need it.
- Full card information is handled by specialist payment providers rather than stored in Lakeside systems.
- Website, account and verification services use technical controls supplied by their providers.
- Condition and customer records are separated where practical, using booking or asset references.
- GPS, locker and biometric-authentication access is restricted and logged where the provider supports it.
- Passwords, permissions, updates, backups, logging and multi-factor authentication are used where available and appropriate.
- Suspected loss, misuse or unauthorised access is investigated and reported where the law requires.

No internet or storage system can be guaranteed completely secure. Customers should also protect account credentials and tell Lakeside promptly about suspicious access.

**14 - Children**

## The hire service is for adults.

The named hirer must be at least 18. Lakeside does not knowingly ask a child to complete the customer identity-verification flow for an equipment hire. A person under 18 may browse the public website, but must not create or complete a hire as the named customer.

**15 - Contact, complaints and updates**

## Questions or a privacy request?

Contact Lakeside using the Contact page . Include enough information to identify the relevant account, booking or verification session, but do not send a full card number or an unnecessary copy of your identity document in an ordinary message.

You can complain to the Information Commissioner's Office . We would appreciate the opportunity to investigate your concern first, but contacting us does not remove your right to complain.

We may update this policy when the service, providers, legal requirements or data practices change. The effective date and version at the top will be updated when a material revision is published.

# Provider privacy links

These provider notices are supplied for transparency. The provider used for a particular transaction or verification may process data under its own notice as well as under Lakeside's instructions.

**Didit Verification Privacy Notice**
https://didit.me/terms/verification-privacy-notice/

**Didit Privacy Policy**
https://didit.me/terms/privacy-policy/

**Didit End User Terms for Identity Verification**
https://didit.me/terms/identity-verification/

**Stripe Privacy Policy**
https://stripe.com/gb/privacy

**Stripe Privacy Center**
https://stripe.com/gb/legal/privacy-center

**TrueLayer Privacy Notice**
https://truelayer.com/privacy

**TrueLayer End User Terms**
https://truelayer.com/enduser_tos

**Information Commissioner's Office - data protection complaints**
https://ico.org.uk/make-a-complaint/data-protection-complaints/data-protection-complaints/

# Document control

Policy version: 1.3
Effective date: 7 September 2026
Provider links checked: 7 September 2026
Controller: Lakeside Handy Hire Ltd, Company No. 17362091.