



PRIVACY POLICY

Helicopter Performance Monitoring
& Analytics Tool

Effective Date:	5 May 2026
Last Updated:	7 Oct 2026
Version:	1.2

GST First Pty Ltd trading as BC System Solutions
heli-x.au

1. Introduction

GST First Pty Ltd ACN 696418612 trading as BC System Solutions (“we”, “our”, or “us”) operates Heli-X, a professional helicopter performance monitoring and analytics platform (“the Platform”) accessible via web browser at app.heli-x.au and through native mobile applications (“the App”). The Platform enables helicopter operators, pilots, engineers, and maintenance repair organisations (MROs) to track aircraft performance, manage trend monitoring data, record electronic flight duty records (eFDRs), manage defects, conduct power checks, and access analytics.

This Privacy Policy explains how we collect, use, disclose, store, and protect your personal information in accordance with the Privacy Act 1988 (Cth) (“Privacy Act”) and the 13 Australian Privacy Principles (“APPs”). We are committed to handling your personal information responsibly and transparently.

By accessing or using the Platform, you acknowledge that you have read and understood this Privacy Policy. If you do not agree with the practices described herein, please discontinue use of the Platform.

2. Information We Collect

We collect personal information that is reasonably necessary for the provision and improvement of our Platform. The types of information we collect fall into the following categories.

2.1 Account and Identity Information

When you register for an account or are invited by a company administrator, we collect:

- Full name and username
- Email address
- Phone number (optional)
- Password (stored in hashed form; we never store plaintext passwords)
- Role and job role within your organisation (e.g., admin, user, viewer, pilot, engineer)
- Authorisation number (ARN), where applicable

2.2 Company and Organisational Information

For company accounts, we collect:

- Company name and company logo
- Account type (operator, MRO, or both)
- Subscription tier and billing information
- Onboarding progress and settings preferences

2.3 Aircraft and Operational Data

To deliver our core helicopter performance monitoring services, we collect and process:

- Aircraft registration numbers, make, model, and serial numbers
- Engine and airframe hours, cycle counts, and counter data
- Trend monitoring data including temperature, torque, gas generator speed (Ng), power turbine speed (Np), and other performance parameters
- Power check results, templates, and associated reference documents
- Maintenance events and maintenance records

- Defect reports, defect photos, and defect resolution data

2.4 GPS and Location Data

We do not use GPS or Precise Location data for advertising, third-party tracking, or sale to data brokers. Location data is used solely for core Platform functionality.

Certain features of the Platform collect and process location data. This data is considered sensitive and is handled with particular care:

- **GPS Flight Path Breadcrumbs:** when enabled by your company administrator, the Platform records GPS coordinates at configurable intervals (30 seconds to 5 minutes) during active flights. This data is stored with your flight record and is visible only to members of your company.
- **GPS Auto-Timer:** if enabled, the Platform monitors device GPS speed (not coordinates) to detect aircraft movement and prompt flight-start actions. No location coordinates are stored or transmitted by this feature.
- **SAR/SOS Last Known Position:** when Search and Rescue (SAR) tracking or SOS Sudden-Stop Detection is active, the Platform records the aircraft's last known GPS position. In an emergency event, this position may be included in alert emails sent to designated SAR contacts.
- **Aircraft Location (MRO Fleet View):** for MRO-connected aircraft, approximate location and operational status may be displayed on fleet map views using mapping services.
- Where SAR, compass, heading, movement, or impact-detection features are enabled, the App may process motion, acceleration, speed, and directional data from the device.
- This data is used only for flight safety, SAR/SOS functionality, map orientation, and operational analytics.

2.5 Photographs and Uploaded Images

The Platform allows users to upload photographs and images in several contexts:

- Defect photos attached to defect reports (stored in secure cloud storage with signed-URL access)
- Power check photographs documenting gauge readings or cockpit instruments
- Bug report screenshots submitted through the in-app support form
- Reference documents (PDFs and images) uploaded to power check templates

Uploaded images may contain embedded metadata (EXIF data) including GPS coordinates, device information, and timestamps. We do not strip EXIF metadata from uploads at this time.

Users should ensure that uploaded images do not contain unnecessary personal or sensitive information, including embedded location metadata, unless required for operational purposes.

2.6 Search and Rescue (SAR) Data

When SAR tracking is enabled, we collect:

- SAR contact details (names and email addresses of designated emergency contacts, who may be third parties outside your organisation)
- Expected flight duration and buffer period settings
- SOS detection configuration (speed thresholds, grace periods)
- SAR activation timestamps and emergency trigger events

2.7 Electronic Flight Duty Records (eFDR) Data

When the eFDR module is enabled, we collect:

- Flight records including flight times, engine times, and landing counts
- Flight routes and associated airport data
- Pilot-in-command details and signatory information
- Digital signatures for record sign-off
- Fuel records and drop-tracking data (where enabled)
- Billing client information associated with flights

2.8 Usage and Technical Data

We automatically collect certain technical information when you use the Platform:

- Browser type, operating system, and device information
- IP address and approximate geographic location
- Pages visited, features used, and session duration
- Authentication events and login timestamps
- Theme preferences and user interface settings
- Security and session signals derived from browser or device characteristics (such as user agent, screen size, time zone, and similar technical information) are used solely for authentication, fraud prevention, session security, and service reliability.
- These signals are not used to track users across third-party apps or websites.

2.9 Payment Information

Subscription payments are processed through Stripe, our third-party payment processor. We do not store full credit card numbers, CVVs, or other sensitive payment instrument details on our servers. Stripe handles all payment card data in accordance with PCI DSS requirements. We retain a Stripe customer identifier linked to your company account for subscription management purposes.

2.10 Communications Data

If you contact us or submit a bug report through the Platform, we may collect the content of your correspondence along with your name and email address.

2.11 Mobile App Permissions

The App may request access to certain device features depending on functionality used, including:

- Location (GPS) – for flight tracking, SAR/SOS, and map features
- Camera and Photos – for defect reporting and documentation
- Files/Storage – for uploading documents and records
- Motion and Sensors – for detecting movement, speed, heading, or sudden stops
- Notifications – for alerts, safety notifications, and system updates

These permissions are used solely to support Platform functionality and operational safety features.

Users can manage or revoke permissions at any time through their device settings.

3. How We Collect Personal Information

We collect personal information through the following means:

- **Directly from you:** when you register an account, update your profile, enter data into the Platform, submit forms, or communicate with us.
- **From your company administrator:** when they invite you to join the Platform, assign you a role, or manage your access permissions.
- **Automatically:** through cookies, server logs, and analytics tools when you interact with the Platform.
- **From third-party services:** such as Supabase (authentication and database hosting), Stripe (payment processing), and Resend (transactional email delivery).

We do not collect personal information by unlawful or unfair means. We only collect information that is reasonably necessary for the functions and activities described in this policy.

4. Purposes of Collection, Use, and Disclosure

We collect, hold, use, and disclose your personal information for the following purposes:

4.1 Service Delivery

- Providing access to the Platform and its features
- Enabling aircraft trend monitoring, performance analytics, and alerting
- Generating and managing electronic flight duty records
- Processing power checks and managing reference documentation
- Facilitating defect reporting, tracking, and resolution
- Enabling MRO connection management and shared data access

4.2 Account Management

- Authenticating users and managing sessions
- Processing user invitations and role assignments
- Managing subscription tiers, billing, and payment processing
- Enforcing access controls and row-level security

4.3 Communication

- Sending transactional emails (e.g., user invitations, eFDR reports, alert notifications)
- Responding to support enquiries and bug reports
- Providing system notifications about Platform changes or maintenance

4.4 Safety and Compliance

- Maintaining audit logs for eFDR sign-offs and counter adjustments
- Supporting aviation regulatory compliance and record-keeping obligations
- Detecting, preventing, and addressing fraud, security incidents, or technical issues

4.5 Improvement and Analytics

- Analysing usage patterns to improve Platform functionality and user experience
- Monitoring system performance and reliability
- Developing new features and services

4.6 No Tracking Across Apps or Websites

- Heli-X does not track users across third-party apps or websites for advertising, marketing attribution, data brokerage, or cross-context behavioural profiling.
- We do not sell personal information, Precise Location data, aircraft location data, or operational records to advertising networks, data brokers, or third-party tracking providers.
- All data collected by Heli-X is used solely for platform functionality, safety features, operational analytics, and service improvement.

5. Disclosure of Personal Information

We may disclose your personal information to the following categories of recipients:

5.1 Within Your Organisation

Company administrators within your organisation can view and manage team member profiles, including names, emails, roles, and activity within the Platform. This is necessary for organisational management and access control.

5.2 MRO Connections

If your company establishes an active connection with a Maintenance Repair Organisation (MRO) through the Platform, the connected MRO may access specified aircraft data, trend monitoring information, defect records, and maintenance history for the aircraft covered by that connection. MRO access is governed by connection status controls and row-level security policies.

5.3 Third-Party Service Providers

We engage the following third-party service providers who may process personal information on our behalf:

Provider	Service	Data Processed	Location
Supabase	Authentication, database hosting, file storage, edge functions	Account data, operational data, uploaded files	United States
Stripe	Payment processing and subscription management	Company billing details, Stripe customer ID	United States
Resend	Transactional email delivery	Recipient email addresses, email content	United States
Google (Maps Static API)	Map imagery in SOS emergency alert emails	GPS coordinates of last known aircraft position	United States

5.4 SAR Emergency Contacts

When Search and Rescue (SAR) tracking or SOS Sudden-Stop Detection is enabled and an emergency event is triggered, the Platform will send alert emails to the SAR contacts configured by your company administrator. These contacts may be individuals outside your organisation. The alert emails may contain the aircraft registration, last known GPS position, a static map image of that position, and the pilot or signatory name associated with the active flight record. Your company administrator is responsible for ensuring that designated SAR contacts have been appropriately informed of this data sharing.

5.5 Legal and Regulatory Disclosure

We may disclose personal information where required or authorised by:

- An Australian law, court order, or tribunal order
- An enforcement body for the investigation of an offence or regulatory matter
- The prevention of a serious threat to life, health, or safety
- The establishment, exercise, or defence of a legal claim

5.6 Business Transfers

In the event of a merger, acquisition, or sale of all or a portion of our assets, personal information may be transferred as part of that transaction. We will notify affected users and ensure that the receiving entity is bound by privacy obligations at least as protective as those set out in this policy.

6. Cross-Border Disclosure of Personal Information

In accordance with APP 8, we inform you that your personal information may be disclosed to overseas recipients. Our primary third-party service providers (Supabase, Stripe, Resend, and Google) are headquartered in the United States of America and process data in that jurisdiction.

Before disclosing personal information to an overseas recipient, we take reasonable steps to ensure the recipient does not breach the APPs in relation to that information. Each of our third-party providers maintains privacy and security practices that are at least substantially similar to the protections required under the Privacy Act.

Countries in which overseas recipients are likely to be located: United States of America.

7. Data Security

We take reasonable steps to protect personal information from misuse, interference, loss, and from unauthorised access, modification, or disclosure. Our security measures include:

7.1 Technical Safeguards

- Encryption of data in transit using TLS/HTTPS
- Encryption of data at rest within our database infrastructure
- Row-level security (RLS) policies enforced at the database level, ensuring users can only access data belonging to their company
- Role-based access controls (admin, user, viewer) with principle-of-least-privilege enforcement
- Secure password hashing through Supabase Auth (bcrypt)
- JWT-based authentication with token expiration and secure session management
- Signed URLs for private file access with configurable expiry periods

7.2 Organisational Safeguards

- Audit logging for critical operations including eFDR sign-offs, counter adjustments, and role changes
- Sanitised error handling that prevents exposure of database structure, file paths, or internal server details to end users
- Security event logging for monitoring and incident response

- Separation of service-role and user-level database access

7.3 Data Breach Response

In the event of an eligible data breach as defined under Part IIIC of the Privacy Act, we will comply with the Notifiable Data Breaches (NDB) scheme. This includes conducting an assessment of the suspected breach and, where the breach is likely to result in serious harm, notifying the Office of the Australian Information Commissioner (OAIC) and affected individuals as soon as practicable.

8. Data Retention and Destruction

We retain personal information only for as long as it is needed for the purposes for which it was collected, or as required by law. Specific retention practices include:

- Active account data is retained for the duration of your account or your company's subscription.
- Electronic flight duty records and associated audit logs are retained in accordance with aviation regulatory requirements, which may mandate retention for several years beyond the operational period.
- Trend monitoring data and power check records are retained as long as your company account remains active, or as required by applicable aviation regulations.
- Payment transaction records are retained as required by Australian taxation and financial reporting obligations.
- Upon account deletion or subscription cancellation, we will take reasonable steps to destroy or de-identify personal information that is no longer needed, unless retention is required or authorised by law.
- Certain aviation, safety, audit, and regulatory records may be retained for extended periods as required by law, even after account closure.

9. Accessing and Correcting Your Personal Information

In accordance with APPs 12 and 13, you have the right to request access to the personal information we hold about you and to request correction of any information that is inaccurate, out-of-date, incomplete, irrelevant, or misleading.

9.1 How to Access Your Information

Much of your personal information is directly accessible through your account settings within the Platform. You can view and update your name, email, phone number, theme preferences, and other profile details at any time.

For information not directly accessible through the Platform, or if you require a comprehensive summary of all personal information we hold about you, please submit a written request to info@heli-x.au.

9.2 Response Timeframes

We will respond to access and correction requests within 30 days of receiving the request. If we require additional time, we will notify you and provide reasons for the delay.

9.3 Refusing Access

We may refuse access to personal information in limited circumstances permitted by the Privacy Act, such as where providing access would pose a serious threat to life, health, or

safety, or would unreasonably impact the privacy of other individuals. If access is refused, we will provide you with written reasons for the refusal and the mechanisms available to you to make a complaint.

10. Cookies and Similar Technologies

The Platform uses cookies and similar technologies to support essential functionality including authentication, session management, and user preference storage (such as theme selection). These are strictly necessary cookies required for the Platform to function correctly.

We may also use analytics cookies to understand how users interact with the Platform and to improve our services. You can manage cookie preferences through your browser settings. Disabling essential cookies may impair Platform functionality.

We may use first-party analytics and server logs to understand feature usage, system performance, and reliability.

We do not use analytics tools to track users across third-party apps or websites, and we do not use analytics data for third-party advertising.

11. Anonymity and Pseudonymity

In accordance with APP 2, we acknowledge that individuals should have the option of dealing with us anonymously or by using a pseudonym. However, due to the nature of our Platform — which manages aviation safety records, regulatory compliance data, and authenticated user accounts — it is impracticable for us to provide our services without verifying your identity. Identified access is required for aviation record-keeping integrity, audit trail requirements, and role-based access controls.

12. Direct Marketing

We do not use your personal information for direct marketing purposes unless you have expressly consented. Any marketing communications we send will include a clear and simple mechanism for you to opt out of receiving further communications.

Transactional and operational emails (such as eFDR reports, alert notifications, and user invitations) are not considered marketing communications and are necessary for the operation of the Platform.

13. Children's Privacy

The Platform is designed for use by aviation professionals and is not directed at individuals under the age of 18. We do not knowingly collect personal information from children. If we become aware that we have inadvertently collected personal information from a child, we will take reasonable steps to delete that information promptly.

14. Automated Decision-Making

The Platform uses automated processes in the following areas. All automated features are designed to support — not replace — human decision-making by qualified aviation personnel. No automated decisions with legal or similarly significant effects are made about individuals through the Platform.

- **Trend Monitoring Alerts:** the Platform automatically generates alerts when aircraft engine parameters exceed configurable thresholds. These alerts are informational and are sent to company members and designated email recipients.
- **GPS Auto-Timer:** when enabled, the Platform uses device GPS speed readings to detect aircraft movement and automatically prompt the user to start or stop flight timers. This feature monitors speed only and does not store location coordinates.
- **SOS Sudden-Stop Detection:** when enabled during SAR-tracked flights, the Platform monitors GPS speed and triggers an emergency alert if the aircraft's speed drops to zero while airborne, after a configurable grace period. This automated trigger sends email notifications to designated SAR contacts including the aircraft's last known GPS position.
- **Fuel Starvation Warnings:** the Platform may display warnings when calculated fuel levels fall below configured thresholds, based on recorded fuel additions and estimated consumption rates.

15. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or for other operational reasons. When we make material changes, we will:

- Update the "Last Updated" date at the top of this policy
- Make the updated policy available through the Platform's Agreements section in Settings
- Where appropriate, notify users via email or an in-app notification

We encourage you to review this policy periodically. Continued use of the Platform after changes are posted constitutes your acceptance of the revised policy.

16. Complaints

If you believe that we have breached the Australian Privacy Principles or handled your personal information inappropriately, you have the right to lodge a complaint.

16.1 Lodging a Complaint with Us

In the first instance, please submit your complaint in writing to info@heli-x.au. We will acknowledge receipt of your complaint within 7 business days and will investigate and respond within 30 days. If the complaint is complex, we may require additional time and will notify you accordingly.

16.2 Escalation to the OAIC

If you are not satisfied with our response, you may lodge a complaint with the Office of the Australian Information Commissioner (OAIC).

Organisation	Office of the Australian Information Commissioner (OAIC)
Website	www.oaic.gov.au
Phone	1300 363 992
Email	enquiries@oaic.gov.au
Post	GPO Box 5218, Sydney NSW 2001

17. Contact Us

If you have any questions, concerns, or requests regarding this Privacy Policy or our handling of your personal information, please contact us:

Entity	GST First Pty Ltd ACN 696 418 612 trading as BC System Solutions
Platform	Heli-X Analytics
Website	heli-x.au
Privacy Contact	info@heli-x.au
General Support	info@heli-x.au

18. Definitions

For the purposes of this Privacy Policy, the following terms have the meanings set out below:

Term	Definition
APP	Australian Privacy Principle, as set out in Schedule 1 of the Privacy Act 1988 (Cth)
BC System Solutions	The trading name of GST First Pty Ltd, the entity that develops and operates the Platform
eFDR	Electronic Flight Duty Record, a digital record of flight operations including flight times, routes, and crew details
MRO	Maintenance Repair Organisation, a company that provides maintenance services for aircraft operators
OAIC	Office of the Australian Information Commissioner, the independent regulator responsible for privacy and freedom of information
Personal Information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable, as defined by the Privacy Act 1988
Platform	The Heli-X web application (app.heli-x.au) and associated mobile applications, operated by GST First Pty Ltd trading as BC System Solutions
RLS	Row-Level Security, a database security mechanism that restricts data access based on the authenticated user's company membership
Trend Data	Engine performance parameters recorded over time for monitoring aircraft health and detecting anomalies

19. Governing Law

This Privacy Policy is governed by and construed in accordance with the laws of the Commonwealth of Australia, including the Privacy Act 1988 (Cth). Any disputes arising under or in connection with this policy shall be subject to the exclusive jurisdiction of the courts of Queensland, Australia.

End of Privacy Policy
Heli-X — Fly Smarter, Not Harder