NC Apex Solutions Ltd

Privacy Policy

Company Number: 16585690
Registered Office: Seymour House, 94–96 Seymour Place, London, W1H 1NB
Contact: info@ncapex.co.uk | Privacy: privacy@ncapex.co.uk
ICO Registration Number: C1888627
Data Protection Lead: Michael Coyle of Lawdit Solicitors — michael.coyle@lawdit.co.uk

Last Updated: 9 March 2026

Applies to: All NC Apex websites, applications, APIs, and services.
Drafted and finalised by Lawdit Solicitors Stay Legal service — info@staylegal.co.uk

1. Who We Are (Data Controller)

NC Apex Solutions Ltd ("NC Apex", "we", "our", "us") is the data controller for the personal data processed across all NC Apex products and services unless stated otherwise in the applicable Product Schedule.

Company name: NC APEX SOLUTIONS LTD

Company number: 16585690

Registered office: Seymour House, 94–96 Seymour Place, London, United Kingdom, W1H 1NB

Contact email: info@ncapex.co.uk

Privacy enquiries: privacy@ncapex.co.uk

ICO registration number: C1888627

Data Protection Lead: Michael Coyle, Lawdit Solicitors — michael.coyle@lawdit.co.uk

Controller vs Processor Roles

NC Apex acts as Data Controller for account authentication data, billing and subscription information, service-performance logs, business communications, security events, and operational metadata.

For Customer Data uploaded into our products, NC Apex acts as Data Processor and the Customer acts as Data Controller. Product Schedules describe product-specific variations to these roles, but all Services follow this general principle.

2. Scope of This Policy

This Privacy Policy applies to all NC Apex websites, applications, APIs, and services. It describes how we process personal data at a platform-wide level across all of our products.

Each product also has its own Product Schedule, which supplements this Privacy Policy by describing the specific data types, hosting locations, processing purposes, and retention rules relevant to that product. Where this Privacy Policy and a Product Schedule differ, the Product Schedule applies for that product only.

Nothing in a Product Schedule replaces the global principles outlined in this Privacy Policy unless explicitly stated.

3. What Data We Collect

Different products collect different types of data. We collect only what is necessary for each product to function.

3.1 Data You Provide Directly

Depending on the product and feature set, we may collect: name, business contact details, login details (Microsoft, Google, or local accounts), uploaded files (e.g. photographs or media for inspections), estate, asset or compliance details, financial inputs for planning tools, support requests, and preferences.

Uploaded files may include incidental personal data or special category data (e.g. faces, identifiable individuals, or health-related items) depending on the Customer's use of the Service. Customers are responsible for ensuring they have a lawful basis to upload such content.

3.2 Data Collected Automatically

Across our services we may collect: IP address, device and browser information, usage logs, event timestamps, diagnostics and crash data, service-performance data, and security-related logs (including authentication metadata and rate-limit events) for security, abuse prevention, and reliability.

3.3 Location Data

Some NC Apex products may offer optional location-based features (for example, RoamCast). If you choose to use such features, the Service may process device or browser location information solely for the purpose of delivering the requested functionality.

Location data is processed only when you actively request a location-based action and is not used for tracking or profiling. Any product-specific behaviour relating to how location data is handled is described in the relevant Product Schedule.

3.4 Cookies and Similar Technologies

We use essential cookies and browser storage (cookies, localStorage, and sessionStorage) for authentication state, session management, rate-limit counters, UI preferences, and security. Analytics cookies (e.g. Google Analytics) are disabled by default and used only with your consent. For full details see the Cookie Policy in the Website and Services Terms document.

3.5 Data Provided By Your Organisation or Third Parties

If your organisation uses our Services, administrators may provide your business contact details to create or manage your account. We may also receive information from identity providers (e.g. Microsoft or Google) when you sign in, or from third-party services that you choose to integrate with a product. This information is limited to what is necessary for authentication or service functionality.

4. Lawful Bases for Processing

We process personal data under one or more of the following UK GDPR lawful bases, depending on the context and the specific Service. These lawful bases apply where NC Apex acts as Data Controller. Where NC Apex acts as Data Processor, the Customer is responsible for determining and communicating the applicable lawful basis.

- (a) Contract — to deliver the services you request, manage your account, provide support, and operate subscription features.
- (b) Legitimate Interests — for purposes such as ensuring the security and integrity of the Services, preventing fraud or abuse, rate-limiting and protecting infrastructure, monitoring service performance, diagnostics and error handling, and improving user experience. These interests are balanced against your rights and freedoms.
- (c) Consent — for optional activities such as analytics cookies, certain marketing communications to individuals, optional location-based functionality, or opt-in data uses described within relevant Product Schedules.
- (d) Legal Obligation — to comply with laws such as tax, accounting, invoicing, and regulatory requirements.

The table below sets out our processing activities and the lawful bases we rely on:

Purpose / Activity	Type of Data	Lawful Basis
Register you as a new user	Identity; Contact	Contract
Process and deliver your order / subscription	Identity; Contact; Financial; Transaction	Contract; Legitimate Interests (debt recovery)
Manage our relationship with you	Identity; Contact; Profile	Contract; Legal Obligation; Legitimate Interests
Administer and protect our Services and infrastructure	Identity; Contact; Technical	Legitimate Interests (IT security, fraud prevention); Legal Obligation
Provide support and respond to enquiries	Identity; Contact; Profile	Contract; Legitimate Interests
Process payments and manage subscriptions	Identity; Contact; Financial	Contract; Legal Obligation
Send essential service communications	Identity; Contact	Contract; Legal Obligation
Monitor, maintain, and improve performance	Technical; Usage	Legitimate Interests (improving our services)
Analytics — where consented	Technical; Usage	Consent
Marketing communications — where permitted	Identity; Contact; Marketing & Comms	Legitimate Interests (soft opt-in); Consent
Comply with legal and regulatory obligations	Identity; Contact; Financial; Transaction	Legal Obligation

5. How We Use Personal Data

We use personal data for the following purposes, depending on the context and the specific Service:

- To operate, maintain, and deliver our Services, including core platform functions, authentication, account management, and customer administration.
- To provide support, respond to enquiries, and help troubleshoot issues.
- To process payments, manage subscriptions, and administer billing, where applicable.
- To send essential service communications, such as security alerts, account notices, subscription updates, and changes to the Services.
- To ensure security and integrity of the Services, including fraud and abuse prevention, rate-limiting, monitoring for unusual activity, and maintaining operational logs.
- To monitor, maintain, and improve performance, availability, reliability, and user experience across our platform.
- To comply with legal, regulatory, tax, and accounting obligations.

We do not sell personal data.

6. Hosting, Infrastructure and Subprocessors

We use trusted third-party providers to host our Services, deliver core platform capabilities, and support our internal business operations. We require all providers that process personal data on our behalf to implement appropriate contractual, security, and confidentiality safeguards.

Product-specific subprocessors and integrations are described in the relevant Product Schedule and do not replace the global providers listed below. Where these providers involve international transfers, such transfers are handled in accordance with Section 7.

Provider	Purpose	Processing Location	Safeguard
Hostinger	Global edge hosting infrastructure	Global (frontend only; DB ops excluded)	Data Processing Agreement
Supabase	Authentication, database, edge functions, security and rate-limiting logs	EU region	Data Processing Agreement
Microsoft Azure (UK West)	Application compute, storage, Azure Blob Storage, platform services	UK (primary)	Microsoft DPA / SCCs
Azure OpenAI	AI-powered features (NLP, content generation, analysis)	Azure-hosted (UK/EU)	Microsoft DPA
Brevo (Sendinblue)	Transactional and account-related email delivery	EU	Data Processing Agreement
Stripe	One-off card payments	UK / US	Stripe DPA
GoCardless	Recurring subscription payments	UK / EU	GoCardless DPA
Dynamics 365	Customer relationship management and administration	Microsoft-hosted (EU/UK)	Microsoft DPA
Xero	Invoicing and financial reconciliation (where applicable)	New Zealand (adequacy decision)	Xero DPA
Microsoft 365 (Exchange/Outlook, Teams, SharePoint, OneDrive for Business)	Customer communications, meeting hosting, document management	EU / UK	Microsoft DPA

Note: Payment card and bank details are handled directly by Stripe and GoCardless and are not stored in our applications.

Note: Personal OneDrive accounts are never used to store customer information.

6.1 Third-Party APIs

We may use third-party APIs or services to provide certain features of our products. Any product-specific third-party integrations (for example, those used for weather data, mapping, or specialised domain functionality) are documented in the applicable Product Schedule.

6.2 Subprocessor Changes

We maintain an up-to-date list of our subprocessors and will provide notice of material changes in accordance with the NC Apex Master Terms of Use.

7. International Transfers

Some of our service providers operate global infrastructure or may process data in locations outside the UK. For example, frontend hosting delivered through global content delivery networks, certain email or CRM services, and Microsoft 365 collaboration tools may involve transfers outside the UK. Supabase processes data within the EU. Azure services used by our platform are hosted primarily in the UK.

Whenever personal data is transferred outside the UK, we ensure that appropriate safeguards are in place. These may include:

- UK adequacy regulations, where the destination country has an approved adequacy decision (for example, New Zealand for Xero);
- the UK Addendum to the EU Standard Contractual Clauses, used with providers located in countries without adequacy decisions;
- risk-based assessments and contractual protections designed to ensure an equivalent level of protection for personal data.

8. Retention Periods

We retain personal data only for as long as necessary to provide the Services, comply with legal and regulatory obligations, resolve disputes, enforce agreements, and support business operations. Retention periods vary depending on the type of data, the nature of the Service, and any legal or contractual requirements.

Each Product Schedule includes the product-specific retention rules that apply to that Service.

Where NC Apex acts as Data Processor, we retain Customer Data only for the duration of the Customer's use of the Service and delete or return it following the Customer's instructions and applicable law, unless a longer retention period is required by legal or regulatory obligations.

Operational and administrative records (such as billing, subscription information, security logs, or customer communications) may be retained for longer periods where necessary for compliance, fraud prevention, recordkeeping, or to exercise or defend legal claims.

By law we are required to keep basic information about our customers (including contact, identity, financial and transaction data) for a minimum of six years after they cease being customers, in accordance with applicable tax and accounting legislation.

9. Security Measures

We implement appropriate technical and organisational measures to protect personal data, taking into account the nature of the data, the scope and context of processing, and the risks to individuals. These measures include:

- TLS encryption for data in transit;
- Access controls and multi-factor authentication (MFA) where available;
- Role-based access and least-privilege permissions;
- Regular backups (per provider);
- DDoS protection at the hosting layer;
- Monitoring and audit logging;
- Secure secret management.

We use trusted service providers and require all subprocessors to implement appropriate security safeguards consistent with UK GDPR requirements. We review our security practices periodically and update measures where necessary.

You are responsible for keeping your credentials secure, managing access to your account, and configuring your own systems in a secure manner.

10. Special Category Data

We do not require or encourage the submission of special category data. Special category data includes information such as biometric identifiers, health-related information, data revealing racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, genetic data, or sexual orientation.

If customers choose to upload or capture such information as part of their workflows (for example, inspection photography that incidentally captures identifiable individuals or health indicators), the customer acts as the Data Controller and is responsible for ensuring a lawful basis and an Article 9 UK GDPR condition for processing. NC Apex acts as Data Processor for this content and processes it only on the customer's documented instructions.

We do not use special category data for analytics, product improvement, AI training, or any purpose other than delivering the relevant Service. We apply appropriate technical and organisational safeguards to any special category data processed within our platform.

11. Your Rights (UK GDPR)

You have the following rights under UK data protection law:

- Right of access — to ask for copies of your personal data.
- Right to rectification — to ask us to correct inaccurate personal data.
- Right to erasure — to ask us to erase your personal data in certain circumstances.
- Right to restriction of processing — to ask us to restrict processing in certain circumstances.
- Right to object to processing — to object to our processing in certain circumstances.
- Right to data portability — to ask us to transfer your personal data to another organisation or directly to you.
- Right to withdraw consent — at any time, for example for analytics cookies or optional features.

You have the right to lodge a complaint with the UK Information Commissioner's Office (ICO):

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Helpline: 0303 123 1113 | Website: www.ico.org.uk

We may need to verify your identity before responding to a request. We aim to respond within one month, although this may be extended by up to two additional months for complex or multiple requests as permitted by law.

Where NC Apex acts as Data Processor, rights requests should be directed to your organisation, the Data Controller. We will assist the Data Controller in responding to such requests as required under UK GDPR.

12. End of Service, Export and Deletion

12.1 General Export Requirements

For subscription products, Customers must export any data they require before the end of their Subscription. Product-specific export formats and tooling are described in the relevant Product Schedule. NC Apex does not guarantee that Customer Data can be exported after access to the Service ends.

12.2 Termination with Notice

If a Customer provides valid notice to terminate a Subscription, access to the Service continues throughout the applicable notice period. The Customer is responsible for downloading any required data during this time. After the termination date, account access ends and NC Apex may delete or anonymise Customer Data in accordance with this Policy and applicable retention rules.

12.3 Non-Payment and Failed Payments

If a Subscription ends due to non-payment, NC Apex may suspend or lock the Customer's account immediately. A grace window of seven (7) days may be provided for payment resolution. If payment is not

resolved within the grace period, the Subscription will be deemed terminated and NC Apex may delete or anonymise Customer Data without further obligation.

12.4 One-Off Purchases

For one-off purchases, access to the purchased Service or output is provided for the period described at the point of purchase. Customers must download or export any data during this access window. After this window ends, NC Apex may revoke access and is not required to provide further downloads. NC Apex retains only information required by law (such as invoicing or transaction records).

12.5 Backups, Logs and Subprocessors

Deletions propagate to backups during the next scheduled rotation cycle. Certain operational or security logs may be retained for a limited period for diagnostic, security, or compliance purposes. Subprocessors engaged by NC Apex will be instructed to delete Customer Data in accordance with their contractual obligations.

12.6 Identity and Authority Verification

NC Apex may require identity or authority verification before actioning export or deletion requests. Where NC Apex acts as Data Processor, we will act only on instructions from the appropriate Data Controller.

13. Cookies, Similar Technologies and PECR Compliance

We use cookies and similar technologies (including localStorage and sessionStorage) to operate our websites and apps, maintain security, manage sessions, and, where enabled, analyse service performance. We follow the UK Privacy and Electronic Communications Regulations (PECR) and ICO guidance on cookies and storage/access technologies.

Strictly Necessary Technologies

We set technologies that are required to provide a service you request (for example, authentication, session management, security, rate-limiting, or remembering your cookie choices). These do not require consent.

Analytics (Google Analytics)

We use Google Analytics for usage and performance insights. Google Analytics is not essential and therefore requires your prior consent under PECR. We block all Google Analytics cookies and scripts until you provide consent via our cookie banner or settings, and you may withdraw consent at any time.

DUAA 2025 Carve-Outs

The Data (Use and Access) Act 2025 introduced new exceptions for certain low-risk statistical or appearance-related technologies. Where we use such low-risk first-party technologies, we may rely on these exceptions and provide a simple, free-of-charge way to object. Google Analytics is not covered by these exceptions and still requires explicit consent.

Advertising and Behavioural Tracking

We do not currently set advertising cookies or behavioural tracking technologies without explicit consent. If we introduce advertising technologies in the future (for example, in the Weather Application), we will request prior consent before any advertising or measurement cookies are placed. We will use a Google-certified CMP integrated with the IAB Transparency and Consent Framework to capture and maintain consent preferences. Users can refuse advertising cookies and still access the relevant Service.

Your Choices

Our cookie banner and settings allow you to accept, reject, or withdraw consent for non-essential cookies at any time. Consent records are maintained and refreshed when our purposes or providers change.

14. Marketing Communications

We may send service-related or administrative messages without consent, such as security alerts, account notices, subscription information, or changes to the Service. These messages are not considered direct marketing under PECR.

We send marketing emails only where permitted under PECR. This means:

- With your consent; or
- Under the commercial soft opt-in, where your contact details were collected during a sale or negotiation for a sale, you were offered a clear opt-out at that time, and the marketing relates to our own similar products or services.

You can opt out of marketing at any time by using the unsubscribe link in any marketing message or by contacting us directly. We may send marketing to corporate subscribers (business email addresses) without consent, but we honour all objections and maintain suppression lists as required under PECR.

NC Apex sends marketing communications only where it acts as Data Controller. We do not send marketing on behalf of Customers and do not use Customer Data (where we act as Processor) for NC Apex marketing purposes.

15. Contact and Complaints

If you have questions about this Privacy Policy or wish to exercise your data protection rights, please contact our Data Protection Lead:

Email: privacy@ncapex.co.uk

Postal: NC Apex Solutions Ltd, Seymour House, 94–96 Seymour Place, London, W1H 1NB

If we process your personal data on behalf of your organisation (for example, where your employer uses one of our products and acts as Data Controller), please direct any rights requests to your organisation. We will assist them as required under UK GDPR.

If you have concerns about how we handle personal data, you can also lodge a complaint with the UK Information Commissioner's Office (ICO) — see Section 11 for contact details.

We may require identity verification before responding to certain requests.