# PRIVACY POLICY

## 1. INTRODUCTION

1.1 This Privacy Policy has been prepared by Dollar Club Pty Ltd ACN 676 214 378 ABN 52 676 214 378 trading as Next Level Trucks and its subsidiary companies (Next Level Trucks, "we", "us", "our") in compliance with the *Privacy Act 1988* (Cth) as amended by the *Privacy and Other Legislation Amendment Act 2024* (the "Act") and the thirteen Australian Privacy Principles ("APPs") set forth in Schedule 1 thereof.

1.2 We are committed to the open and transparent management of personal information in accordance with APP 1 and to safeguarding the personal information we collect, use, disclose, store and handle in connection with our business operations and activities.

1.3 This Privacy Policy establishes comprehensive procedures for the collection, use, disclosure, storage, security, access and correction of personal information about individuals, as well as the mechanisms by which individuals may lodge enquiries or complaints regarding our handling of their personal information.

1.4 This Privacy Policy shall be read in conjunction with our Website Terms of Use, and any other contractual terms and conditions that govern the provision of our products and services to you. Where we make significant amendments to this Privacy Policy that materially affect your rights or our handling of your personal information, we shall endeavour to provide you with reasonable notice of such changes by publication on our website or by electronic mail.

1.5 All personal information held by us shall be governed by the most current version of this Privacy Policy as published on our website. You bear responsibility for periodically reviewing this Privacy Policy and remaining informed of any modifications thereto.

## 2. DEFINITIONS AND INTERPRETATION

2.1 For the purposes of this Policy, the following definitions shall apply:

**Personal Information** bears the meaning ascribed to it in section 6 of the Act. Personal information constitutes information or opinion about an identified individual or an individual who is reasonably identifiable from that information or opinion, whether the information or opinion is true or not and whether the information or opinion is recorded in material form or not.

**Sensitive Information** constitutes a subset of personal information that includes information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, criminal record, health information, genetic information, and biometric information. Sensitive information is subject to heightened protection under the Act.

**Health information** includes information or opinion about the health or disability of an individual, an individual's expressed wishes about the future provision of health services, a health service provided or to be provided to an individual, and other personal information collected in connection with the provision of a health service.

## 3. CATEGORIES OF PERSONAL INFORMATION COLLECTED

### 3.1 General Categories

The categories of personal information we collect shall vary according to the specific purpose for which such information is required and may include:

(a) **Customer Information**: In relation to customers procuring our products and services, we collect full legal names, residential and billing addresses, electronic mail addresses, telephone numbers, payment information including credit card details and alternative payment method credentials, government-issued identification documentation such as driver's licences, and comprehensive order and transaction histories;

(b) **Commercial Credit Information**: For commercial credit applicants, we collect information necessary to assess creditworthiness including but not limited to credit history, business history, trade references, financial statements, and related commercial information as permitted under the *Privacy (Credit Reporting) Code 2025*;

(c) **Digital Analytics Information**: Technical information and analytics data including web browser types and configurations, browsing preferences and patterns, Internet service provider details, referring and exit pages, date and time stamps, Internet Protocol addresses, time zone and geolocation data where applicable, and comprehensive usage statistics relating to our digital platforms;

(d) **Marketing Communications Information**: For individuals who have consented to receive promotional materials, we collect names, postal addresses, electronic mail addresses, and telephone numbers;

(e) **Customer Service Information**: Information provided during complaint resolution, feedback submission, enquiry processing, callback requests, and product replacement processes;

(f) **Security and Surveillance Information**: CCTV footage and recordings from premises where such technology is installed for security purposes;

(g) **Employment Information**: For prospective employees and contractors, we collect information contained in applications and curricula vitae, information recorded during interviews, results of pre-employment screening, government-issued identifiers including tax file numbers where legally required, and employment verification data; and

(h) **Supplier and Business Partner Information**: Names, business addresses, electronic mail addresses, telephone numbers, and relevant commercial information for suppliers, distributors, and other business partners.

### 3.2 Sensitive Information Collection

We do not ordinarily collect sensitive information unless such collection is required or authorised by Australian law, necessary for the performance of our functions or activities, or provided with your explicit consent. Where sensitive information is collected, we shall:

(a) provide clear notification of the collection at or before the time of collection;

(b) obtain appropriate consent in accordance with APP 3;

(c) implement additional security measures commensurate with the sensitive nature of the information; and

(d) limit use and disclosure to the specific purposes for which consent was obtained or as otherwise permitted by law.

3.3 **Anonymity and Pseudonymity**

Where practicable, individuals have the option to remain anonymous or to use a pseudonym when dealing with us. However, this option may not be available where:

(a) it is impracticable for us to deal with individuals who have not identified themselves;

(b) we are required or authorised by Australian law to deal with identified individuals; or

(c) the provision of products or services necessarily requires identification for legal, commercial, or security reasons.

## 4. METHODS OF PERSONAL INFORMATION COLLECTION

4.1 **Direct Collection**

Where reasonable and practicable, we collect personal information directly from individuals through the following means:

(a) completion of online forms, applications, and registration processes on our website and digital platforms;

(b) subscription to, purchase of, or rental arrangements for our products and services;

(c) registration for newsletters, promotional offers, events, and marketing communications;

(d) participation in surveys, competitions, promotions, and market research activities;

(e) direct communications including electronic mail, telephone conversations, face-to-face interactions, and written correspondence;

(f) employment applications and contractor engagement processes; and

(g) any other direct interaction or transaction with our organisation.

4.2 **Indirect Collection**

In limited circumstances, we may collect personal information from sources other than the individual concerned, including:

(a) publicly available sources including the Internet, directories, and public registries;

(b) third parties such as mutual contacts, referees, agents acting on your behalf, and persons making purchases on your behalf;

(c) service providers, contractors, and business partners acting on our behalf;

(d) credit reporting bodies in accordance with our Credit Reporting and Credit-Related Personal Information Policy; and

(e) promotional and marketing partners with whom we have commercial relationships.

Where personal information is collected indirectly, we shall take reasonable steps to ensure that individuals are made aware of such collection in accordance with APP 5.

## 5. DIGITAL INFORMATION COLLECTION PRACTICES

5.1 **Website Analytics and Tracking Technologies**

To optimise our digital services and enhance user experience, we employ various information collection technologies including:

(a) **System Log Files**: Automated collection of user actions, system events, and technical diagnostics relating to website usage;

(b) **Cookies and Similar Technologies**: Unique identifiers placed on user devices that enable session management, preference storage, and analytics functionality. Detailed information regarding cookie management and user controls is available at https://allaboutcookies.org/;

(c) **Web Beacons, Pixels, and Tags**: Electronic files that record information about browsing behaviour, page views, and user interactions; and

(d) **Third-Party Analytics Services**: Implementation of Google Analytics which collect session statistics, geolocation data, browser and device information, and usage analytics.

5.2 **Third-Party Service Integration**

Our digital platforms may integrate with third-party services. These services operate under their respective privacy policies, and we do not control their information collection or usage practices. Users should review the privacy policies of such services before providing personal information.

5.3 **User Controls and Opt-Out Mechanisms**

You may exercise control over digital tracking technologies through:

(a) browser settings to disable cookies and tracking technologies, though this may impact website functionality;

(b) direct opt-out mechanisms provided by advertising networks including:

(i) https://www.facebook.com/settings/?tab=ads;

(ii) https://www.google.com/settings/ads/anonymous; and

(iii) https://advertise.bingads.microsoft.com/en-us/resources/policies/personalized-ads; and

(c) industry-standard opt-out tools such as the Digital Advertising Alliance's consumer choice portal.

## 6. PURPOSES FOR COLLECTION, USE AND DISCLOSURE

6.1 **Primary Purposes**

We collect, use, hold and disclose personal information for specific purposes that are reasonably necessary for, or directly related to, our business functions and activities, including:

(a) provision of products and services and delivery of requested communications;

(b) identity verification and authentication where legally required or commercially necessary;

(c) credit assessment and risk management in accordance with our Credit Reporting and Credit-Related Personal Information Policy;

(d) personalisation of communications, services, and user experiences;

(e) direct marketing activities for which appropriate consent has been obtained;

(f) internal business operations including administrative, planning, product development, and quality assurance functions;

(g) employment and contractor assessment and management;

(h) legal and regulatory compliance including satisfaction of disclosure obligations;

(i) fraud prevention, security monitoring, and risk management;

(j) compilation of de-identified statistical data for business intelligence and reporting purposes; and

(k) any purpose expressly consented to by the individual or otherwise permitted under applicable law.

6.2 **Secondary Purposes**
Personal information collected for a primary purpose may be used or disclosed for a secondary purpose only where the individual has consented to such use or disclosure, or where such use or disclosure is otherwise permitted under the APPs.

6.3 **Categories of Recipients**
We may disclose personal information to the following categories of recipients for the purposes described above:

(a) employees, related entities, contractors, and service providers engaged in the operation of our business, provision of services, or fulfilment of customer requirements;
(b) suppliers and third parties with whom we maintain commercial relationships for business, marketing, and operational purposes;
(c) professional advisers including legal practitioners, accountants, auditors, and insurers;
(d) organisations authorised to conduct promotional, research, or marketing activities on our behalf;
(e) third parties specifically authorised by you to receive your information;
(f) debt collection agencies and credit management services where payments are outstanding;
(g) law enforcement agencies, regulatory bodies, and government authorities where required or permitted by law; and
(h) any other person or entity as required or authorised under Australian law.

6.4 **Disclosure to Related Entities and Service Providers**
Where we disclose personal information to related entities, contractors, or service providers, we implement contractual safeguards requiring such parties to handle personal information in accordance with the APPs and this Privacy Policy. Such contractual arrangements include appropriate privacy and confidentiality provisions.

## 7. DIRECT MARKETING PRACTICES

7.1 **Consent Requirements**
We may use personal information for direct marketing purposes only where we have obtained valid, informed, and specific consent from the individual. Such consent must be:

(a) voluntary and freely given;
(b) informed and specific as to the purposes for which information will be used;
(c) current and not withdrawn; and
(d) unambiguous in its terms.

Pre-selected consent mechanisms, vague consent language, or bundled consent arrangements do not constitute valid consent for direct marketing purposes.

7.2 **Marketing Communications**
Direct marketing communications may be transmitted via various channels including postal mail, short message service, facsimile, electronic mail, and social media platforms, in accordance with applicable laws including the *Spam Act 2003* (Cth) and the *Do Not Call Register Act 2006* (Cth).

7.3 **Opt-Out Rights**
All direct marketing communications include clear and prominent opt-out mechanisms enabling immediate cessation of such communications. Opt-out

requests shall be processed within five business days of receipt. Individuals may also exercise opt-out rights by contacting our Privacy Officer using the details specified in this Privacy Policy.

## 8. CROSS-BORDER INFORMATION TRANSFERS

### 8.1 Overseas Disclosure

In limited circumstances, we may disclose personal information to recipients located outside Australia. Such disclosures are made only where:

(a) reasonably necessary for our business operations;

(b) you have provided informed consent to the transfer;

(c) we reasonably believe the overseas recipient is subject to substantially similar privacy protections; or

(d) we have implemented appropriate contractual safeguards.

### 8.2 Adequacy Assessment

Prior to any cross-border transfer, we conduct assessments to determine whether the destination jurisdiction provides substantially similar privacy protections to those available under Australian law. Where such protections are not available, we implement additional contractual safeguards requiring overseas recipients to handle personal information in accordance with the APPs.

### 8.3 Notification and Consent

Where practicable, we shall notify individuals of specific overseas transfers and provide opportunities to consent to or object to such transfers. Individuals retain rights to access, correct, and request deletion of personal information that has been transferred overseas.

## 9. INFORMATION SECURITY AND RETENTION

### 9.1 Security Measures

We implement comprehensive technical, physical, and administrative safeguards to protect personal information from misuse, interference, loss, unauthorised access, modification, or disclosure. These measures include:

(a) **Physical Security**: Secure premises with access controls, locked storage facilities, and comprehensive CCTV monitoring systems;

(b) **Technical Security**: Firewalls, intrusion detection systems, encryption of data in transit and at rest, multi-factor authentication, secure password policies, and regular security assessments;

(c) **Administrative Security**: Staff training programs, access controls based on business need, confidentiality agreements, and incident response procedures; and

(d) **Cloud Security**: Implementation of industry-standard security controls for cloud-based storage and processing systems, including vendor security assessments and contractual security requirements.

### 9.2 Data Breach Procedures

We maintain comprehensive data breach response procedures in compliance with the Notifiable Data Breaches scheme under Part IIIC of the Act. In the event of an eligible data breach, we shall:

(a) conduct immediate containment and assessment procedures;

(b) notify the Office of the Australian Information Commissioner as soon as practicable and within 72 hours where feasible;

(c) notify affected individuals as soon as practicable where the breach is likely to result in serious harm; and

(d) implement remedial measures to prevent recurrence and mitigate harm.

Individuals who become aware of suspected data breaches should immediately contact our Privacy Officer using the details specified herein.

9.3 **Retention Periods**

We retain personal information only for the period reasonably necessary to fulfil the purposes for which it was collected, unless a longer retention period is required or permitted by law. Specific retention periods are determined by reference to:

(a) the nature and sensitivity of the information;
(b) legal and regulatory requirements;
(c) business and operational needs;
(d) contractual obligations; and
(e) the purposes for which the information was collected.

Upon expiry of the applicable retention period, personal information shall be securely destroyed, de-identified, or anonymised using industry-standard procedures including secure deletion protocols, physical destruction of hard copy records, and cryptographic erasure of electronic data.

## 10. INDIVIDUAL RIGHTS AND ACCESS PROCEDURES

10.1 **Right of Access**

Individuals may request access to personal information held about them by submitting a written request to our Privacy Officer. We shall provide access in accordance with APP 12 unless:

(a) providing access would pose a serious threat to the life, health, or safety of any individual;
(b) providing access would have an unreasonable impact on the privacy of others;
(c) the request is frivolous or vexatious;
(d) the information relates to existing or anticipated legal proceedings;
(e) providing access would reveal our intentions in relation to negotiations with the individual;
(f) providing access would be unlawful; or
(g) access is otherwise refused under APP 12.

Where access is refused, we shall provide written reasons for the refusal within thirty (30) days of the request.

10.2 **Right of Correction**

We shall take reasonable steps to ensure that personal information we collect, use, and disclose is accurate, up-to-date, complete, and relevant. Individuals may request correction of personal information by providing:

(a) sufficient details to identify the information requiring correction;
(b) evidence supporting the requested correction; and
(c) preferred method of notification regarding the outcome of the request.

We shall respond to correction requests within thirty days and, where correction is made, notify relevant third parties to whom the information has been disclosed where reasonable and practicable.

10.3 **Right to Deletion**

Individuals may request deletion of personal information where such information is no longer necessary for the purposes for which it was collected, consent has been withdrawn, or the information was unlawfully collected. Deletion requests shall be assessed against:

(a) legal and regulatory retention requirements;

(b) legitimate business interests;
(c) the interests of other individuals; and
(d) our obligations under other applicable laws.

10.4 **Processing Fees**
We may charge reasonable administrative fees for processing access and correction requests. Such fees shall be calculated to cover only the reasonable costs of retrieval, copying, and dispatch, and shall not exceed the amounts prescribed under the *Privacy Regulation 2013*.

## 11. AUTOMATED DECISION-MAKING

11.1 Where we utilise automated decision-making processes including algorithmic systems that could reasonably be expected to significantly affect individual rights or interests, we shall include in this Privacy Policy information about such automated decision-making processes. This information shall include:

(a) the circumstances in which automated decision-making is used;
(b) the types of personal information used in such processes;
(c) the logic involved in the automated decision-making;
(d) the consequences of such processing for individuals; and
(e) rights available to individuals in relation to automated decisions.

## 12. COMPLAINTS RESOLUTION PROCEDURES

12.1 **Internal Complaints Process**
Individuals may lodge complaints about breaches of the APPs or registered APP codes by contacting our Privacy Officer using the contact details specified herein. Our internal complaints process includes:

(a) acknowledgment of complaints within five business days;
(b) investigation of complaints within thirty days;
(c) provision of written responses outlining findings and any remedial action;
(d) escalation procedures for unresolved complaints; and
(e) maintenance of complaint records for quality assurance and regulatory purposes.

We may require additional information to investigate complaints effectively and may be delayed in providing responses in complex cases. Where delays are anticipated, we shall notify complainants and provide regular updates.

12.2 **External Review Rights**
Where individuals are not satisfied with our response to their complaint, they may lodge a complaint with the Office of the Australian Information Commissioner:

**Office of the Australian Information Commissioner**
GPO Box 5218
Sydney NSW 2001
Email: enquiries@oaic.gov.au
Telephone: 1300 363 992

12.3 **Anonymous Complaints**
Individuals are entitled to make anonymous complaints or enquiries. However, we may require identification where:

(a) required by law;
(b) necessary for effective investigation; or
(c) impracticable to deal with anonymous complainants.

## 13. PRIVACY GOVERNANCE AND ACCOUNTABILITY

### 13.1 Privacy Officer Responsibilities

We have appointed a Privacy Officer responsible for ensuring compliance with the APPs and handling privacy-related enquiries and complaints. The Privacy Officer's responsibilities include:

(a) developing and maintaining privacy policies and procedures;
(b) conducting privacy impact assessments;
(c) providing privacy training and guidance to staff;
(d) investigating privacy incidents and complaints;
(e) liaising with regulatory authorities; and
(f) monitoring compliance with privacy obligations.

### 13.2 Privacy by Design

We embed privacy considerations into the design of our information handling practices, systems, and processes. This includes:

(a) conducting privacy impact assessments for new projects and systems;
(b) implementing data minimisation principles;
(c) designing systems with privacy controls and safeguards;
(d) providing privacy training to personnel; and
(e) conducting regular privacy audits and reviews.

### 13.3 Regulatory Compliance

We maintain ongoing compliance monitoring and review processes to ensure adherence to evolving privacy laws and regulatory expectations. This includes regular review of:

(a) privacy policies and procedures;
(b) staff training and awareness programs;
(c) technical and physical security measures;
(d) third-party contracts and service arrangements; and
(e) cross-border transfer arrangements.

## 14. PRIVACY ENQUIRIES AND COMPLAINTS

14.1 All enquiries, requests for access or correction, and complaints relating to this Privacy Policy or our handling of personal information should be directed to:

**Privacy Officer**
Dollar Club Pty Ltd trading as Next Level Trucks
Unit 3, 50-56 Centenary Place, Logan Village QLD 4207
Email: joel@nextleveltrucks.com.au
Telephone: 0484 945 845
Website: https://www.nextleveltrucks.com.au/

### 14.2 Policy Updates and Notifications

This Privacy Policy may be updated periodically to reflect changes in our information handling practices, legal requirements, or business operations. Updated versions shall be published on our website with appropriate version control and effective dates.

Material changes that significantly affect individual rights shall be communicated through additional notification mechanisms including website notices and direct communication where contact details are available.

### 14.3 Accessibility and Alternative Formats

This Privacy Policy is available in alternative formats upon request, including

large print and electronic formats compatible with assistive technologies. Requests for alternative formats should be directed to our Privacy Officer.

**EFFECTIVE DATE: 1 July 2026**