Privacy Policy

Updated Date: 14 February 2026

This Privacy Policy explains what information The Growth Collective Limited trading as Kindo (TGCL, Kindo and Ezlunch) collects, how it is used and stored, and the steps we take to protect it. We are committed to safeguarding personal information and complying with the New Zealand Privacy Act 2020.

Terms used in this policy have the same meaning as in the Account Holder Terms and Conditions, available on the Kindo website. We may update this policy from time to time, and the "Updated Date" indicates when it was last revised.

1. Information we collect and receive

TGCL and the website gather the following information from the registered Account Holder and in some cases from the Institution a Member attends:

- **Account Holder Name and phone number:** this is used to make contact in the event of an issue or clarification requirement for an Order.
- **Email address:** this is used as your login and will be used to send any notices to you, including receipts.
- **Password:** this is a security measure to ensure that only you can place orders using your account.
- **Member (Customer) Name:** this is the name of a person attending a particular Institution. Each person for which you will be placing Orders, including yourself (if applicable), will need to be listed here. This information is used for delivery.
- **Payment details:** Payment information is collected for the purpose of processing orders and transactions. Payments are processed securely by Stripe, our third-party payment processor. When payment details are entered, that information is transmitted directly to Stripe and is not stored in full on Kindo's systems. Kindo does not store full credit card numbers. Where an account holder chooses to save a payment method, Kindo retains only a limited, non-sensitive reference to the card. Stripe processes payment information in accordance with its own privacy and security policies. Kindo takes reasonable steps to protect payment-related information and operates in accordance with applicable PCI-DSS requirements.
- **Organisation:** this information is used for delivery by external suppliers. If your Institution is registered it will be available to be selected. If your Institution is not registered, you will not be able to use the Service.
- **Room, Address, Student ID:** This information is used to deliver orders. Where required, classroom or location details must be kept up to date. In some cases, the Institution may update this information directly. If a Member collects their order on site, an identifier such as a Student ID may be required. If an order is sent by post or courier, a delivery address will be collected.
- **Student Year Level:** where the Institution is a school, this is the student year level that the Member is enrolled in at that Institution.
- **Student Type:** where the Institution is a school, this is the student type that the Institution has enrolled the Member as, such as foreign fee paying Student. This is used to enable management of fees to be applied or not applied based on the student type selected by the school.
- **Group:** where the Institution is a school, this is the group or groups that the Institution has allocated for the Member, such as Year 9 Science or a sports group. This is used to enable management of fees to be applied based on group membership.
- **Allergens:** this information is provided to suppliers for reference only. Suppliers are responsible for their own food preparation processes, and individuals with severe allergies should contact suppliers directly to confirm suitability.

When you use our websites or applications, we may automatically collect certain technical information. This includes recording IP addresses against each user session for security purposes, device and software version information to assist with fault resolution, and standard web server logs for traffic analysis, which record each request to the server along with HTTP headers and IP addresses.

2. Cookies and similar technologies

We use cookies and similar technologies across our websites and applications, including Kindo, Ezlunch and our online shop platforms.

What are cookies?

Cookies are small data files placed on your computer or device when you visit a website. They help websites function effectively and provide information about how the site is used.

Cookies may be set by us (first-party cookies) or by trusted third-party providers whose services we use (third-party cookies).

In some cases, cookies may collect information that can be considered personal information if it can be linked to an identifiable individual.

Why we use cookies

We use cookies and similar technologies for the following purposes:

1. Essential functionality
To enable secure login, maintain user sessions, prevent fraud and ensure the proper operation of our websites and applications. These cookies are necessary for the service to function.

2. Security
To help detect and prevent malicious activity, including automated access or misuse of our systems (for example, bot detection tools).

3. Performance and analytics
To understand how users interact with our websites and applications so we can improve functionality, performance and user experience, we may use third-party analytics services, such as Google Analytics. Information collected through analytics is used in aggregated form to help improve our services.

4. Embedded services and integrations
Where we embed or integrate third-party services (such as video content or customer service tools), those providers may set cookies necessary for those services to function. We do not use cookies to directly identify individuals for marketing profiling, and we do not sell personal information collected through cookies.

Types of cookies we use

Depending on the website or application accessed, cookies may include:

- Session cookies (which expire when you close your browser)
- Persistent cookies (which remain for a defined period)
- Analytics cookies (such as Google Analytics)
- Security-related cookies (such as bot detection tools)

The specific cookies used may vary depending on the service accessed.

Managing cookies

Most web browsers allow you to control cookies through browser settings. You can choose to block or delete cookies; however, doing so may impact the functionality of certain features of our websites or applications. You can usually find cookie management options in your browser's settings or help menu.

Other tracking technologies

We may use similar technologies such as web beacons or tracking pixels to help measure website performance, understand usage patterns, and improve our services. These technologies often rely on cookies to function.

3. Information collected from third parties

In some cases, we collect personal information about individuals from third parties rather than directly from the individual.

This may include personal information provided to us by:

- schools or other educational institutions (including through Student Management Systems),
- account holders (such as parents or caregivers), or
- organisations that engage us to provide services.

The personal information collected may include names, contact details, identifiers such as student ID, enrolment or group information, and other information necessary to provide our services.

Where we collect personal information from a third party, we take reasonable steps to ensure that individuals are made aware:

- that their personal information has been collected,
- the purpose for which the information is used,
- the source of the information, and
- how they may access or request correction of their personal information.

In most cases, this notification is provided through:

- the relevant school's or organisation's privacy notice, and/or
- this Privacy Policy, which is publicly available on our website.

Where required by law, we may also provide direct notification to individuals.

4. Data from an Institution's SMS

Calls to Student Management System (SMS) APIs provide only the data necessary for the Kindo service (see "Saved data" below). Only data which is relevant to the Kindo service is stored or utilised by Kindo, all other information is discarded at code level by Kindo software as it is received from the SMS.

Kindo requests roll data from the SMS service, and requests are made on a per-school basis. This data is received from a secure internet connection (https) by Kindo software, which ensures that only the saved data items below are stored by Kindo.

Saved data:

> **Core student attributes:** an identifier, such as Student ID (but not NSN per Privacy Act regulations); legal name; preferred name; year level; student type; groups; organisation and room.

> **Core caregiver attributes**: an identifier, such as the Caregiver ID; name; email; phone number.

Notable 'not saved' data includes:

- emergency caregiver records
- non-core student details
- non-core caregiver details

The standard Kindo "seed" roll. This includes students; caregivers (a combination of SMS contact and caregiver data); associations (between students and Kindo caregiver).

This dataset is available to the school facing Kindo web user interface, but not to the end-user web user interface or apps. It is accessed occasionally by Kindo help desk to resolve problems linking Kindo members to student records.

Additional attributes, not required by the seed roll, may be saved from the SMS data sent to Kindo and made available to Kindo technical staff only, to resolve data issues and for debugging problems.   This includes student date of birth (to potentially disambiguate students); siblings; student home phone; EOTC Permissions. This dataset is not available to the user interface. Schools may request a copy of this dataset at any time.

5. Kindo storage and management of data

TGCL works with some third-party systems, such as Student Management Systems, and use API's to receive data for providing the Kindo service. The following relates to the storage and management of this data:

- All web traffic is over secure http (i.e. https) and is terminated at Kindo servers.
- Kindo serves all traffic from Kindo servers (rather than trust third party content delivery networks).
- User passwords in the Kindo database are stored as 'hashes' only (per standard best practice).
- Backups made by Kindo are encrypted.
- Manual data exchange with schools uses a secure facility provided by Microsoft Office 365 and this is kept to a minimum.

A list of third-party service providers (sub-processors) can be found on our website.

Kindo's website and production database are hosted in Australia within an enterprise-grade AWS cloud environment. We may update or modify our hosting and infrastructure arrangements from time to time as part of our normal operations and service improvement processes.

6. How we use your information

TGCL uses personal information supplied by you, or in some cases by your Institution, for the following purposes:

- to process and fulfil orders and transactions;
- to process and manage payments, including fraud prevention and transaction security measures;
- to communicate with you about your account, orders, service updates, or relevant information about our services;
- to respond to enquiries, resolve complaints, or provide customer support;
- to comply with legal, regulatory and contractual obligations;
- to enforce or apply our Terms and Conditions;
- to maintain, analyse and improve our services, systems and user experience; and
- for any other purpose authorised by you or permitted by law.

We will not use personal information for purposes unrelated to the services we provide without your consent, unless required or permitted by law.

7. Who we share your information with

TGCL does not disclose personal information except as described below or where permitted or required by law.

- Suppliers for the sole purpose of providing the Orders. The supplier contact details are provided on the Order receipt, on the website, and by contacting the TGCL helpdesk and may be the Institution itself or an external supplier.
- Payment processing providers (including Stripe) for the purpose of securely processing transactions and managing payment-related services, including fraud detection and dispute handling.
- Any governmental or regulatory body or agency, or any party with statutory enforcement powers, where required or permitted by law.
- Any registered charity that provides funding to TGCL to financially support an Account Holder or a Member.
- Professional advisors and consultants who have entered confidential undertaking with TGCL to provide research, administration or customer support services incidental to the Service, in which case only the minimum information required for such services will be supplied.
- Third party providers for the purposes of satisfying TGCL's legal and regulatory obligations.
- TGCL approved dispute resolution scheme for the purposes of investigating and resolving complaints.
- Any other third party where required to do so by law or instructed to do so by you.

TGCL collects, handles and holds all information provided by the Account Holder on the website. Such information will only be stored in secure networks and facilities.

You are entitled to access your personal information related to you or personal information relating to the relevant Member, which has previously been supplied to us. You may edit, amend or delete any such information unless prohibited by law.

In the event that TGCL, the Service or the website is sold, acquired, merged, liquidated, restructured or otherwise transferred to another party, TGCL reserves the right to transfer to the extent permissible by law its user databases, together with any personal or non-personal information contained therein to such party acquiring the assets.

8. Other information

Note: TGCL is PCI-DSS compliant and do not hold credit card details on our servers. The Account Holder Terms & Conditions (accepted during account registration by end-users such as school families) provide further specific information and should be read in conjunction with this policy statement.

Schools are responsible for their own privacy notices and may wish to refer to their use of third-party systems, including Kindo, in those notices.

TGCL has been assessed by Safer Technology 4 Schools for operation in New Zealand and Australia. A copy of this report can be requested by talking to your relevant education authority in either Australia or New Zealand. Details for this can be found on the ST4S website (https://st4s.edu.au/).

We may update this policy from time to time to reflect changes in our services, legal requirements or operational practices.

9. Use of Artificial Intelligence (AI)

Kindo uses limited artificial intelligence (AI) tools to support user navigation, customer assistance and internal operational efficiency. Where AI tools are used, we collect and process personal information in accordance with this Privacy Policy. Additional information about our use of AI technologies, including the types of data involved and the safeguards applied, is set out in our AI Privacy Addendum, which forms part of this Privacy Policy and is available on our website.

10.   Transferring your information to others

Where we disclose personal information to overseas service providers, we take reasonable steps to ensure those providers protect personal information in a manner that, in overall effect, provides safeguards comparable to the New Zealand Privacy Act 2020.

This includes contractual privacy and security obligations with those providers. A current list of the third-party service providers we use (sub-processors), including their location, is available on our website.

11.   Exercising your rights

Where we are a Processor:

Where we are just the data processor, for instance where the school is the data controller, you must contact the data controller directly in order to exercise your rights. If you contact us to exercise your rights in respect of your information in respect of which we are just the data processor, we will pass on your request to the data controller and assist them as far as possible in dealing with your request.

Where we are a Controller:

You have various rights in respect of your information which we set out in more detail below. Also not all rights are absolute so it depends on the circumstances. For example you might want information deleted, however we will not be able to delete it because we need it to fulfil our legal obligations e.g. provide statutory information to regulatory bodies.

You have the right to:

- Request access to your personal data: This enables you to receive a copy of the personal data we hold about you.
- Request correction of your personal data: This enables you to have any incomplete or inaccurate information we hold about you corrected. We may need to verify the accuracy of the new data you provide to us.
- Request erasure of your personal data: This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it.
- Object to processing of your personal data: This is where we are processing your personal data based on a legitimate interest or those of a third party and you may challenge this. In some cases, we may be entitled to continue processing your information based on our legitimate interests or where this is relevant to any legal claims.
- Request restriction of processing your personal information: This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the information's accuracy (b) where our use of the information is unlawful but you do not want us to erase it (c) where you need us to hold the information even if we no longer require it as you need it to establish, exercise or defend legal claims or (d) you have objected to our use of your information but we need to verify whether we have overriding legitimate grounds to use it.
- Request transfer of your personal information: This is where in some circumstances we will provide to you or a third party you have chosen your personal data in a structured, commonly used, machine-readable format.
- Right to withdraw consent: Where we rely on your consent to process personal information, you may withdraw that consent at any time by contacting us at privacy@kindo.co.nz. Withdrawing consent will not affect the lawfulness of any processing carried out before your consent was withdrawn. Depending on the nature of the processing, withdrawing consent may mean we are unable to provide certain services, and we will advise you if this is the case.

Process to exercise your rights.

You will not have to pay a fee to carry out your rights above. However, we may charge a reasonable fee if we deem that your request is clearly unfounded, repetitive, or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access your information or to exercise any of your other rights.

This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

We try to respond to all legitimate requests within the statutory timeframe under the Privacy Act 2020 (generally 20 working days).

Occasionally it could take us longer than 20 working days if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated as to the progress of your request.

12.   Complaints about our use of your information

If you wish to raise a complaint on how we have handled your information, you can contact us to have the matter investigated by writing to privacy@kindo.co.nz.

If you are not satisfied with our response or believe we are processing your information not in accordance with the law, you can register a complaint with the Privacy Commissioner at https://privacy.org.nz

13.   Contact

Questions, comments, and requests regarding this policy should be addressed to privacy@kindo.co.nz