Effective Date: 24th April 2024

Privacy Policy

This policy explains what information The Growth Collective Limited trading as Kindo (TGCL, Kindo, ezLunch) collects, how we store this information, and the steps we take to protect it.

TGCL is committed to protecting the privacy of all registered Account Holders and meeting its obligations under the NZ Privacy Act 2020.

The terms used in this document have the same meaning as those set out in the Account Holder Terms and Conditions. A link to the Account Holder Terms and Conditions can be found at the bottom of the Kindo homepage.

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: this information is required to facilitate payments for Orders and TGCL will take all reasonable steps to protect this information. TGCL is PCI-DSS compliant and never stores credit card data. If an account holder chooses to store their card details, TGCL only stores only a few digits of the credit card number.
- Organization: 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 for delivery of an Order. If Orders are to be distributed to a particular location or classroom at a school, the location must be inserted here and updated each year as it changes. In some cases, this will be updated directly by the Institution. If the Member will collect their Order from a site at the Institution, they may require an alternative identifier, such as Student ID. If an Order will be sent by post or courier, an 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 used to provide alerts on the printed labels and production lists for food suppliers. This may or may not be noted by suppliers and cannot be relied upon in cases of extreme allergic reactions.
- The Website will use a single cookie to maintain your identity during your session. It is deleted when you log out. Our public website also has a cookie policy that is published and available to review.
- We record IP addresses against each user session for security purposes, and device and software version information to assist with the resolution of faults.

- We maintain standard web server logs, for traffic analysis purposes. These record each request to the server, along with http headers and your IP address.

Data from an Institutions SMS

Calls to the SMS (Student Management System) APIs only provide data which is relevant to Kindo (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.

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 systems can be found on our sub processors page on our Website.

Kindo's website and production database is hosted in Australia, in an enterprise class AWS cloud environment. Customers will be notified of any relocation or expansion of the cloud infrastructure, including system components, user data and related data; and any additional access to data e.g. more staff with access to encryption keys and encrypted data, via announcement in the News section of the Kindo website.

How we use your information

TGCL will use information supplied by you, or in some cases your Institution, to:

- process an Order;
- apply payment requests correctly;
- communicate with you regarding the service or promotions;
- comply with its legal and regulatory obligations;
- enforce or apply our T&Cs;
- investigate or resolve a complaint;
- for internal research purposes; and
- for any other use that you authorise.

Who we share your information with

TGCL will not disclose any information in relation to you or the Member to any third party without consent, other than to:

- 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.
- 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.

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.

With respect to Privacy Act compliance, we strongly suggest that the school privacy statements for families include sharing data with 3rd party systems. 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/).

To reflect the fact that our business is growing constantly, we reserve the right to change this policy at any time.

Data from an Identity Verification provider

Calls to the SMS (Student Management System) APIs only provide data which is relevant to Kindo (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.

Transferring Your Information to others

Under data protection laws, where we transfer personal data outside of a country to another country there may be laws in place which states how we should transfer the data. Where this is the case, we ensure the correct safeguard mechanism is in place to protect the transfer for example, by using approved documentation by the local government or regulatory body.

A current list of the countries we operate in and third parties we use (sub processors) are listed on our Website.

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: This is where we are relying on consent to process your personal data. You have the right at any time to withdraw any consent you have given us to process Your Information. This will not affect the lawfulness of any processing carried out before you withdraw your consent. Depending on the processing activity, if you withdraw your consent, we may not be able to provide certain services to you. We will advise you if this is the case at the time you withdraw your consent.

Please note if you withdraw your consent, it will not affect the lawfulness of any processing of Your Information we have carried out before you withdrew your consent. Should you wish to do so you can contact us at any time via email to privacy@kindo.co.nz

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 timeline e.g. one month. Occasionally it could take us longer than a month 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. Do get in touch if to exercise your rights at helpdesk@kindo.co.nz.

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

Contact

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