Privacy Policy

Last updated: 11 November 2026

The short version

- We keep your name, email, student number (students only) and your orders, to run your account and your orders. Card numbers never reach us.
- The cafeteria you order from sees your name, your order and your notes. It does not see your email, your student number or your credit.
- Usage and crash reports are off unless you switch them on, in Profile, Privacy. To switch them off again, email support@unidash.food.
- No ads, no selling your data, no location tracking.
- Delete your account in the App whenever you like. Order records stay for four years without your name, because tax law requires it.
- Questions, requests or complaints: **support@unidash.food**, answered by our Data Protection Officer.

UniDash ("the App", "we", "us") is a pre-order and pickup service for university cafeterias in Jordan. It has two apps: **UniDash: Order Ahead**, for university students and for guests who order from cafeterias open to the public, and **UniDash Staff**, for cafeteria staff, managers and administrators. This policy explains what personal data we collect, why, who receives it, how long we keep it, and the rights you have under the Jordanian **Personal Data Protection Law No. 24 of 2023 (PDPL)**.

> **Data controller:** Al Hujra Information Technology LLC (publisher name: Al Hujra Information Technology), Amman, Jordan (Companies Control Department registration no. 83622)
> **Data Protection Officer:** Bader Al Haj Hamad, reachable at **support@unidash.food**
> **Contact for privacy requests and complaints:** support@unidash.food (see section 7)
> **Where your data is held:** our database and sign-in service run in the European Union (Frankfurt, Germany); see section 4 for the other providers

1. Data we collect

Account data

Data	Why we collect it
Full name	Identifying your order at pickup
Email address (a university email for student accounts; any email for guest and staff accounts)	Account login, verification and password-reset codes, order and credit notifications
Student/matriculation number (student accounts only)	Verifying university affiliation, preventing duplicate accounts
Account type (student, guest, staff, manager or administrator) and, for staff accounts, the cafeteria you work at	Access control
The language you choose in the App	Sending notifications in your language
A record of each consent you give (section 2): which purpose, which version of our policies, the language it was shown in, when, and, for usage and crash reports, when you switched it off	Showing that you gave your consent, as the PDPL requires

Order data

Data	Why we collect it
Items ordered, their options, quantities, prices	Fulfilling your order
Pickup time slot	Scheduling preparation
Notes you type for the order or for an item	Preparing your order correctly (do not enter sensitive information here)
Your answer when a cafeteria offers a replacement for an unavailable item	Completing or cancelling the order as you choose
Payment method (card or UniDash credit), payment result and payment reference	Settling the order, refunds and payment disputes
Order status history, timestamps and the rating you give an order	Order tracking, dispute resolution, service quality

Credit and favourites

Data	Why we collect it
UniDash credit balance	Credit from your orders, usable for UniDash orders only (see the Refunds Policy)
Credit history (credits and orders paid with it)	Your ledger, refund processing, fraud prevention
Favourite cafeterias	Showing your favourites first

Card payments (including Apple Pay and Google Pay) are processed by **Mastercard Payment Gateway Services (MPGS)** for **Network International**, the acquirer of the cafeteria operator that sells you the food, through secure card fields provided by the gateway. The cafeteria operator is the merchant for your card payment: it receives the payment, and Network International's records of it. Your full card number goes directly to the gateway, so it is **never** seen or stored by UniDash. With each card payment we record the result and reference of the payment and a few details about the card that we need for accounting, refunds and payment disputes: its brand and type, the issuing bank and its country, and the first six digits of the card number, which identify the bank and not you. We do not keep the name on the card, the rest of its number or its expiry with your orders. If you choose to save a card for reuse, we also keep a non-sensitive gateway token and the card's brand, expiry and last four digits to display it; you can remove a saved card at any time. If you pay with Apple Pay or Google Pay, Apple or Google handles your card under its own privacy terms and passes the gateway an encrypted payment token. When a card payment needs your bank's check, information about your phone is sent to your card's bank, through Mastercard, to confirm the payment is really yours.

Technical data

Data	Why we collect it
Push notification token (Firebase Cloud Messaging)	Sending order-status, credit and service-announcement notifications to your device
Crash and diagnostic data (Firebase Crashlytics), **only if you switch on usage and crash reports**	Fixing bugs and keeping the App stable
App usage, **only if you switch on usage and crash reports**: which screens are opened, session starts, whether a sign-in or sign-up completed, and an approximate location (country and city) that Google derives from your connection (Firebase Analytics, UniDash: Order Ahead only)	Understanding which parts of the App are used so we can improve them. This is tied to a random app-install identifier, and we do not send your name, email or account ID with it. UniDash Staff never collects it
A bot-protection check (Cloudflare Turnstile), which runs in the background when the sign-in, password-reset or email-code screen opens, and on the sign-up screen once you tick the required box: IP address and browser/device signals	Protecting accounts from automated sign-in and sign-up abuse

We do **not** collect your device's precise (GPS) location, contacts, photos, or advertising identifiers, and we do **not** use your data for advertising, nor sell it, nor build a profile of you as an individual.

2. Legal basis: your consent, for each purpose

Under the PDPL, personal data may be processed with your consent or where the law permits it (Articles 4 to 6). We ask for your consent separately for each purpose and keep a record of each one (section 1):

- **Your account and your orders** (required, the first box at sign-up): you accept the Terms, the Refund and Cancellation Policy and this Privacy Policy, and confirm that you are 18 or older. Accepting this policy is your agreement that we process your account details and orders as it describes, including on servers outside Jordan (section 4), for as long as you keep your account. We record the acceptance of the Terms and the consent to processing separately. You withdraw the consent by deleting your account (section 8); an account cannot stay open without it.
- **Usage and crash reports** (optional, the second box, off unless you tick it): you can switch them on at any time in **Profile, Privacy**, and switch them off again by emailing **support@unidash.food**; they stop from the next time the App starts. Ordering never depends on them. Until you agree, the App sends no usage or crash reports at all.
- **Staff accounts:** a cafeteria's administrator creates the account, and the staff member gives their own consent on first sign-in to UniDash Staff before anything else opens, with crash reports as a separate optional choice.

- **Push notifications** follow your device's permission. You can switch them off at any time in your device settings without affecting your ability to order.
- **Service announcements**, such as a cafeteria closing early, an outage, a new cafeteria or a change to these policies, are shown in the App's inbox and sent as notifications, as part of running the service you signed up for. We do not send promotions or advertising.
- **Before you have an account**, the App collects nothing for usage measurement or crash reporting. The bot-protection check runs when you submit the sign-up form after ticking the required box, and when an existing account holder signs in or resets a password.
- **Records the law requires us to keep**: order and payment records needed for tax and accounting are kept for the period the Regulation for Organising Invoicing Affairs No. 34 of 2019 requires (section 6), on the basis of Article 6(A)(5), including after you withdraw consent or delete your account.

3. Who can see your data

- **Cafeteria staff and managers** see the name, order contents and notes, pickup time, and payment method of orders placed at their cafeteria, only what is needed to prepare and hand over your order.
- **Cafeteria administrators** (the operator that runs the cafeterias) see the same order details for all their cafeterias, and the name, email address, role and cafeteria of the staff accounts they manage. They do **not** see a customer's email address, student number or UniDash credit. Administrators, and managers for their own cafeteria, can also read our audit log's entries for their cafeterias (section 6).
- **UniDash personnel:** a small number of authorised people at UniDash can reach the data when needed to answer your request, investigate a problem or keep the service secure, and are bound to keep it confidential (PDPL Article 13).
- Customers can only ever see **their own** profile, orders, credit, and notifications. Access is enforced on our servers, not just in the app.

4. Service providers and other recipients

These providers process data on our instructions and only for the function listed, except where the table says a recipient also acts on its own responsibility. Every provider listed is bound by its data processing terms to protect your data at least as well as this policy describes.

Provider	Function	Data involved
Supabase (supabase.com)	Database, authentication, backend hosting, in the European Union (Frankfurt, Germany)	All account, order, and credit data
Mastercard Payment Gateway Services (MPGS)	The payment gateway: the card fields and the processing of card payments (including Apple Pay and Google Pay)	Card details entered in the gateway's card fields; payment amount and result; saved-card token and last four digits; for the bank's check, information about your phone
Network International (network.ae)	The acquirer of the cafeteria operator: authorises card payments made to the operator and settles them into the operator's account. It handles payment data under its own responsibility as a regulated payment provider	Payment amount, the card details it receives through the gateway, payment result and reference
The cafeteria operator (the company that runs the cafeteria you order from)	Sells you the food and is the merchant for card payments: it receives the payment through Network International, together with Network International's records of it. It acts on its own responsibility as the seller, uses your data only to prepare and hand over your order and deal with questions about it, never for marketing, does not keep it outside UniDash except in the sales records the law requires it to keep, and its staff, managers and administrators use UniDash as section 3 describes	Your order and the details listed in section 3; for card payments, the amount, result and reference of the payment and the card details Network International reports to its merchants
Google Firebase: Cloud Messaging	Delivering push notifications	Push token, notification content
Google Firebase: Crashlytics	Crash reporting, only with your consent	Device model, OS version, crash stack traces, an installation identifier
Google Firebase: Analytics	Usage measurement, only with your consent (UniDash: Order Ahead only)	Screen names, session and sign-in events, app-install identifier, device model, OS version, approximate location (country and city)
Brevo (brevo.com)	Sending account emails (verification and password-reset codes)	Email address, email content, delivery status

Cloudflare (cloudflare.com)	Bot protection on sign-up, sign-in, password reset and resending the email code. Cloudflare runs the check for us, and also uses the same signals on its own responsibility to improve its bot detection, as its Turnstile privacy policy describes	IP address and browser/device signals during the check

Transfers outside Jordan. Our database is in the European Union (Frankfurt, Germany) and Brevo is in France, both under the EU General Data Protection Regulation. Google and Cloudflare operate worldwide, including in the United States, under their data processing terms, the EU-US Data Privacy Framework and standard contractual clauses. Before transferring, we checked that each of these offers protection no lower than the PDPL requires (Article 15), you agree to the transfer when you create your account (section 2), and we keep a record of what is transferred, to whom and why (Article 14).

We do **not** sell your data. Beyond the recipients above, we disclose it only:

- where a competent Jordanian authority requires disclosure by law;
- to our professional advisers (lawyers, accountants and auditors), who are bound to keep it confidential, when needed to establish or defend a legal claim, settle a payment dispute or meet an audit requirement;
- to a company that takes over the UniDash service through a merger, sale or restructuring. It must keep the protections in this policy, and we tell you in the App before your data moves.

5. How we protect your data

- Your data is encrypted in transit (HTTPS only) and at rest in our database.
- Card numbers are typed into the payment gateway's own fields and never reach UniDash or the cafeteria.
- Every account reaches only what its role allows, enforced inside the database itself, not only in the App.
- Changes to credit balances, roles and which account an order belongs to are recorded in an audit log that nobody can edit.
- Sign-in is protected against automated abuse, and UniDash personnel reach the data only as section 3 describes.
- UniDash will never ask you for your password or a verification code, by email, phone or message. If someone does, do not share it and tell us at support@unidash.food.
- If a breach seriously threatens your data, we will tell you within 24 hours of discovering it, with what you can do to protect yourself, and tell the Personal Data Protection Unit within 72 hours (PDPL Article 20).

6. Retention

- **Account data**, including your consent records, is kept while your account is active and deleted when your account is deleted, apart from what our audit log keeps (see below).
- **Order and payment records** are kept for **four years after the end of the year in which the order was placed**, the period the Regulation for Organising Invoicing Affairs No. 34 of 2019 requires, and longer only while a dispute about them is open; then they are deleted. When you delete your account, your name, your notes and your account link are removed from them straight away, and the rest of the record is kept without your identity for that period; our audit log keeps a record of that change (see below).
- **Credit history, favourites and saved cards** are deleted when you delete your account, and we instruct the payment gateway to delete your saved cards too. A saved card is held by the payment gateway on the merchant account of the cafeteria operator you paid; if that operator stops using UniDash, the cards saved on its account are deleted and passed to no one.
- **Our audit log** records changes to certain fields, such as a credit balance, an account's role or which account an order belongs to, and who made them. It is kept for the same four years as the order and payment records it helps explain, including after an account is deleted. For a deleted customer account it keeps the balance changes and which orders were linked to the account, under an internal account number but without the name or email address; if we ever changed your email address for you at your request, it keeps that change too. When a staff account is deleted, by its holder or by an administrator, it keeps that person's name, email address, role and cafeteria. The administrators and managers of a cafeteria can read its entries, which include the order entries but not customers' balance changes.
- **Push tokens** are deleted when you log out, and after you uninstall the App they are removed as soon as a notification to that device fails.
- **Our record of the account emails we sent you** (address and delivery status) is deleted after 90 days.
- **Crash data**, if you switched it on, is kept for 90 days (Firebase Crashlytics' rolling window). Reports not yet sent are deleted from your device when you switch it off.
- **Usage measurement**, if you switched it on, is kept for the retention period set in our Firebase project, at most 14 months, after which only aggregate totals remain.

7. Your rights, requests and complaints

Article 4 of the PDPL gives you the right to:

- **Know about and access** the personal data we hold about you, and obtain a copy;
- **Withdraw your consent** at any time: usage and crash reports by emailing support@unidash.food; push notifications in your device settings; the rest by deleting your account. Withdrawal does not affect processing already carried out;
- **Correct, complete or update** your data (your name can be edited in the App; for your student number or email, contact us);
- **Limit** the processing of your data to a specific scope;

- **Erase or conceal** your data, including by deleting your account (section 8);
- **Object** to processing or profiling that is unnecessary for the purpose it was collected for, excessive, discriminatory, unfair or unlawful;
- **Transfer** a copy of your data to another controller;
- **Be told** of any breach affecting the security or integrity of your data (section 5).

Using these rights has no financial or contractual consequence for you.

Decisions made automatically

Some outcomes of an order are decided automatically by fixed rules that apply to everyone: an order the cafeteria does not take up in time is cancelled and refunded; an order whose replacement request goes unanswered is cancelled and refunded; a ready order not collected within 60 minutes is closed; and a cancellation is settled as the Cancellation Policy sets out. These rules look only at the order, never at a profile of you. You can ask for any such decision to be reviewed by a person by writing to support@unidash.food.

How to make a request or a complaint

1. Write to **support@unidash.food** from the email address on your account, saying what you want. Our Data Protection Officer handles every privacy request and complaint.
2. We respond within **5 working days** and may ask you to confirm your identity. We carry out a request within **15 working days** of receiving it.
3. If you are not satisfied with our answer, or we do not answer, you can complain to the **Personal Data Protection Unit** at the Ministry of Digital Economy and Entrepreneurship: **PDP@modee.gov.jo**, pdp.gov.jo.

8. Account deletion

You can delete your account and personal data at any time: **in UniDash: Order Ahead** via **You → Delete account**, which opens unidash.food/delete (you can also go there directly; you sign in again and confirm with a code we email you), **in UniDash Staff** by asking your cafeteria's administrator, or **by request** for either app (see the account deletion page). An account cannot be deleted while one of its orders is in progress; once the order has been collected or has ended, it can. Deletion is irreversible. UniDash credit can only be used for orders and is never paid out in cash, so any credit left is lost; the App shows the exact amount before you confirm. Order and payment records we must keep, and our audit log, are kept as section 6 describes. If you tell us why you are leaving, we keep that answer without your name or email, so it is not linked to you.

9. Age

UniDash: Order Ahead accounts are for people aged 18 or older, and you confirm your age when you create one. UniDash Staff accounts are created by a cafeteria's administrator only for people aged 18 or over who work at that cafeteria, and are deleted on the day the person stops working there; the

App itself does not ask staff for their age. Neither app is directed at children, and we do not knowingly collect data from anyone under 18.

10. Changes to this policy

We will post any changes here, in English and Arabic, and update the "Last updated" date; each version can be downloaded as a PDF from the top of this page, and we keep every earlier version and send a copy on request. For material changes we will notify you in the App before they take effect, and if a change affects what you consented to, we will ask for your consent again.