Privacy Notice

refuel.cafe | Version 1.2 | Effective from 13 November 2026

1. Who we are

Refuel Catering & Facilities Ltd (company number 15330662, England and Wales). Registered office: 35a Shrubbery Road, Bromsgrove, England, B61 7BQ.

We are the controller of your personal data. This notice covers the refuel.cafe ordering website and related emails.

Contact for privacy questions: hello@refuel.cafe or write to us at 35a Shrubbery Road, Bromsgrove, England, B61 7BQ. For help with a specific order, email orders@refuel.cafe. ICO registration number: C2081049.

2. What we collect and why

We collect data you give us, and some data created when you use the site.

- **Orders:** name, email, phone (optional), location code, order contents, delivery or collection time, and whether you ordered from a phone, tablet or computer. We use these to take, make and deliver your order.
- **Payments:** Stripe handles your card details. We never see or store your card number. We keep a payment reference (payment intent ID), the order total, the platform fee, and a record of each hold, payment, release and refund. Stripe also receives the billing details you enter at checkout.
- **Changes to orders:** when you change an order, we take a new card hold or payment for the new total first, and then release or refund the old one. We keep a record of each change request: the items, the totals and the result.
- **Group orders:** the payer gives us names of 2 to 100 recipients. We use them to label and deliver each person’s food.
- **Allergen and calorie data:** stored for each order item and printed on food labels.
- **Order management:** every order has a private management link. We keep it only as a hashed token, with an event log (created, changed, cancelled, charged).
- **Location code requests:** company name, contact name, email, address and estimated group size.
- **Marketing sign-up:** email, name, the time you agreed, the wording you agreed to, where you signed up, your IP address and status.
- **Staff action log:** what staff do in the admin area, with a hashed version of the staff member’s IP address.
- **Security events:** the type of event (for example a failed sign in), the page it happened on, a count, and a hashed version of the IP address.
- **Staff accounts:** admin username, email, password hash, encrypted two-factor secret and session data.
- **Admin notifications and kitchen emails:** your name, order total and order contents, sent to our team when you order.
- **Technical logs:** our host keeps server logs of requests and errors. We take steps to keep personal details out of them.

3. Lawful bases

- **Contract:** taking, preparing, delivering and charging for your order, and changing or cancelling it.
- **Legal obligation:** keeping accounting and tax records.
- **Legitimate interests:** preventing fraud and abuse, keeping the site secure, handling group order recipient names, and keeping records to deal with complaints or claims. We have weighed this against your rights. You can object (see section 11).
- **Consent:** marketing emails only. You opt in with a box that is unticked by default. You can withdraw at any time.
- **Health information:** the app does not ask you for health information. If you tell us about an allergy or dietary need by phone or email, we use it only to keep you safe.

4. Data, purpose, basis and retention

Data	Purpose	Lawful basis	Retention
Order details, contact details, location code, device type	Fulfil order, support, refunds	Contract	12 months from order date, then deleted or anonymised
Payment reference, totals, platform fee, hold, payment, release and refund records	Accounts, reconciliation, disputes	Legal obligation	6 years
Order change requests (items, totals, result)	Change your order, audit	Contract, legitimate interests	Items and personal details 12 months with the order. Amounts 6 years
Group recipient names	Label and deliver food	Legitimate interests	12 months with the order, then deleted
Allergen and calorie data per item	Food safety, labels	Legal obligation, contract	12 months with the order
Order management token (hashed) and event log	Let you manage and cancel; audit	Contract, legitimate interests	Personal details 12 months from the order date, or from the delivery date for a pre-order. Amounts 6 years
Marketing contact record (email, name, time, wording, source, IP, status)	Prove consent, send marketing	Consent	Deleted 12 months after your last order, whether you are still subscribed or have unsubscribed. Any order counts, including a cancelled one. If you have never ordered, 12 months from the day you signed up
Unsubscribe code (a one way scrambled code made from your email address)	Make sure we do not email you again	Legal obligation (PECR), legitimate interests	Kept with no end date
Location code requests	Set up your site	Legitimate interests	12 months after last contact
Staff action log (hashed IP)	Accountability, security	Legitimate interests	12 months
Security events (type, page, count)	Security and abuse prevention	Legitimate interests	12 months. The hashed IP address in them is removed after 90 days
Staff accounts and sessions	Staff access	Legitimate interests	While the person works for us. A session ends after 12 hours, or after 6 hours without activity
Admin notifications	Alert staff to orders	Legitimate interests	12 months
Server logs	Keep the site running and secure	Legitimate interests	30 days (set by our host)

When a period ends, a daily automatic job deletes or anonymises the data. Anonymising an order replaces the name and email so the person can no longer be identified, and keeps the amounts. Data can remain in our database backups until they expire, which is up to 7 days after it is deleted.

5. Who we share data with

We use these providers to run the service. They act on our instructions, except where noted.

- **Stripe:** card payments and fraud checks. Stripe is also a controller for some of its own fraud and compliance uses.
- **Hosting provider:** Replit (hosting, database, file storage).
- **Email provider:** Resend, for all our emails: order, pre-order, kitchen, password reset and staff reports.
- **cron-job.org:** triggers our scheduled payment capture. It sends a secret header only. It receives no customer data.
- **Google Fonts:** may load fonts from Google, which means your IP address is sent to Google.
- **Our delivery and kitchen staff:** see your name, order, location and allergen details.

- **Professional advisers, regulators and law enforcement:** where the law requires or to protect our rights.

We do not sell your data.

6. Group orders

If you place a group order, you give us the names of other people. You must have the right to share them. You must tell them we will use their names to label and deliver their food. We use the names for nothing else. Recipients can contact us to use their rights.

7. Allergens

Allergen and calorie data comes from our menu and is stored with each order item. It is printed on labels. If an item shows “ask staff”, we have not confirmed its allergens. Ask us before you order. Always tell staff about a serious allergy before ordering. Our kitchen administrator enters and checks this data. Menu data is not a guarantee against cross-contact.

8. Cookies and similar technology

When you order, our site does not set cookies on your device. Staff who sign in to the admin area get one strictly necessary session cookie, which ends with the session. It needs no consent. We use no analytics or advertising cookies. If this changes, we will add a consent banner first.

While you pay, your browser keeps a temporary copy of your order and the contact details you entered, in its session storage, so that we can still save your order if the page reloads after payment. It is strictly necessary, is sent only to us, and is removed when your order is saved or you close the tab.

Stripe, which takes your payment, may set its own cookies or use similar signals at checkout to prevent fraud. See its notice. Fonts load from Google, which receives your IP address.

Adding Refuel to your phone. Our site offers a small settings file (a web app manifest) and registers a small helper script (a service worker) in your browser, so that you can add Refuel to your home screen. The script is only there to allow installation. It does not store your name, email or order details, does not track you, does not store pages, and does not make the app work offline. We do not use it for analytics or advertising. You can remove the app from your phone, or clear the site data in your browser, at any time.

9. IP addresses, consent records and security logs

When you sign up for marketing, we store your IP address with the consent record. We do this to prove you agreed. The staff action log and security events hold hashed IP addresses only, so we cannot read the original address from them.

We have not sent marketing emails yet. If you tick the marketing box, we will only email you about our food and offers after we have checked your consent, and every email will have an unsubscribe link. Email marketing follows PECR, and we email you only if you opted in. If you unsubscribe, we keep a one way scrambled code made from your email address, not the address itself. We use it only to make sure we do not email you again. Earlier sign-ups from our pilot are not used for marketing, and are deleted by the same 12 month rule as other marketing records.

10. International transfers

Some providers (Stripe, Google, Resend, Replit) may process data outside the UK. When they do, we rely on UK adequacy rules, the UK Addendum to standard contractual clauses, or the UK-US data bridge where the provider is certified.

11. Your rights

- **Access:** ask for a copy of your data.
- **Rectification:** ask us to correct it.
- **Erasure:** ask us to delete it, unless we must keep it by law. If you have an order that is still active, whether it is waiting to be charged or has already been charged but not yet delivered, collected or cancelled, we complete or

cancel it first and then erase your details. We keep order amounts for accounting, and the unsubscribe code if you opted out.

- **Restriction:** ask us to pause using it.
- **Portability:** ask for data you gave us in a usable format, where we use it by contract or consent.
- **Object:** object to use based on legitimate interests.
- **Withdraw consent:** at any time, for example by the unsubscribe link. This does not affect earlier use.

Email hello@refuel.cafe. We reply within one month. We may ask you to prove who you are. It is free, unless a request is clearly unfounded or excessive.

12. Complaints

Please contact us first. You can also complain to the Information Commissioner’s Office: ico.org.uk/make-a-complaint, telephone 0303 123 1113.

13. Automated decisions

Stripe Radar checks every card payment for fraud and may block it or ask for extra checks. This is automated. For pre-orders we also read Stripe’s risk level before taking payment. A flagged pre-order is reviewed by a person. If it is not reviewed before your location’s cutoff, we cancel it and release the hold on your card. If a payment is blocked or a pre-order is cancelled, contact us and ask for a person to review it. You can give your view and challenge the result. We do not use Radar for anything else.

14. Children

Our service is for people aged 16 and over. We do not knowingly collect data from anyone under 16. If you think we have, contact us and we will delete it.

15. Security

We use encryption in transit, hashed passwords and tokens, required two-factor login for all staff, and access limits. No system is risk free. Where a breach must be reported, we will tell the ICO within 72 hours of becoming aware of it, and we will tell you where the law requires.

16. Changes

We may update this notice. The date at the top shows the latest version. For major changes, we will tell you by email or on the site.