



Vericool Service Definition

Cashless Catering EPOS & Pre-Order

Hosted service for school meal payments, EPOS ordering and operational reporting

Version: 1.0

Date: 9 January 2026

Supplier: Vericool Ltd

Contact: support@vericool.co.uk

This document describes how the Vericool service operates, including support, security and service management. Specific service levels and commercial terms are confirmed in the order form and contract.

Contents

1. What the service is
2. Data backup, restore and disaster recovery
3. Onboarding and offboarding support
4. Service constraints (maintenance windows and customisation)
5. Service levels (performance, availability and support hours)
6. After-sales support
7. Technical requirements
8. Outage and maintenance management
9. Hosting options and locations
10. Access to data (upon exit)
11. Security

1. What the service is

Vericool provides a hosted cashless catering and pre-order platform used by primary schools, secondary school, multi-academy estates and local authorities. It enables pupils and staff to pay for meals without cash, online, and supports pre-ordering to improve service efficiency and reduce waste, and provides role-based administration and reporting for catering, education and finance teams.

Key capabilities

- Point-of-sale (POS) meal payments with fast user identification (e.g., biometric recognition, card or PIN).
- Pre selection for primary schools.
- Payment system to top up account.
- Pre-ordering through web/app interfaces with configurable menus, pricing and availability rules.
- Allergen and dietary visibility at selection and service points to support safer meal provision.
- Free School Meals (FSM) handling designed to preserve pupil anonymity.
- Account top-ups and balance management, with spend limits, overdraft rules and audit trails.
- MIS synchronisation to keep student/staff records up to date and reduce manual administration.
- Operational and finance reporting (e.g., uptake, volumes, balances and exports).

Typical service users

- Catering managers and kitchen teams
- School administrators
- Finance teams
- IT administrators
- Pupils, staff and parents/carers (where enabled for top-up and pre-order)

Biometric recognition (where used)

Where biometric recognition (Fingertip/face) is configured, Vericool does not store biometric information. The service stores an encrypted, derived template (a limited set of data points) that cannot be reverse engineered into a fingerprint image and is only usable within the originating dataset.

2. Data backup, restore and disaster recovery

Vericool is ISO 9001 and ISO27001 certified and operates backup, restore and resilience controls designed to protect confidentiality, integrity and availability. Controls are aligned to our service risk profile and customer contractual commitments.

Backups and restore

- Backups are performed on a scheduled basis (typically three times daily) for core service data and configurations.
- Backup media is protected using encryption and access controls, and stored separately from production workloads.
- Backups are monitored for successful completion and investigated on failure.
- Restore procedures are documented and restore tests are performed periodically to validate recoverability.

Business continuity and disaster recovery

- The hosted platform is designed for resilience using cloud services with redundancy and monitored health.
- Disaster recovery procedures are maintained for key components, including recovery steps and communications.
- Recovery objectives (RPO/RTO) are agreed at order stage where required, based on service tier and customer need.

3. Onboarding and offboarding support

Onboarding

- A named project contact is assigned to coordinate mobilisation, technical setup and training.
- We confirm scope (sites, devices, modules, integrations, menus/pricing, reporting) and agree an implementation plan.
- MIS synchronisation is configured and validated; test users and key workflows are verified before go-live.

- Role-based training is delivered for catering, school admin, finance and IT, with go-live support by agreement.
- Operational documentation is provided (administration guides, checklists and support routes).

Offboarding

- We support an orderly exit, including data export in an agreed format where requested.
- Access is removed promptly, and customer-specific credentials/keys are revoked or rotated as part of closure.
- Data retention and secure deletion are applied in line with contract and regulatory requirements.

4. Service constraints (maintenance windows and customisation)

Maintenance windows

- Planned maintenance is scheduled to minimise impact on meal service times.
- Customers are notified in advance of planned maintenance that may affect availability or functionality.
- Emergency maintenance (e.g., critical security fixes) may be applied outside normal windows where required.

Customisation

- The service is configurable (menus, pricing bands, permissions, spend limits, FSM rules, reports and site branding where available).
- Bespoke developments and non-standard integrations are considered by agreement and managed under change control.
- Configuration is documented and version-controlled to support repeatable deployments and auditability.

5. Service levels (performance, availability and support hours)

Service levels are confirmed in the service schedule and contract. The example below illustrates typical targets and incident handling.

Availability and performance

- The hosted service is designed for high availability using resilient cloud components and proactive monitoring.
- Performance is dependent on site connectivity and device specifications; POS workflows are designed for fast, repeatable transactions.
- Capacity is monitored and scaled to meet demand, with planned improvements released under change control.

Support hours and incident response (example)

Priority	Examples	Target response	Update cadence
P1 - Critical	Service unavailable, major functional outage or serious security incident	Response within 1 hour	Frequent updates until stabilised
P2 - High	Key function impaired with no reasonable workaround	Response within 4 business hours	Daily or agreed cadence
P3 - Medium	Non-critical defect or degraded performance	Response within 1 business day	As required
P4 - Low	How-to queries and minor issues	Response within 2 business days	As required

Standard support is typically provided Monday-Friday during UK business hours (excluding public holidays), with enhanced coverage available by agreement.

6. After-sales support

After go-live, Vericool provides ongoing support and service review to keep the service operating effectively and to help customers get value from reporting and configuration.

- Support via agreed channels (email/telephone/service desk), with prioritisation based on severity and impact.
- Dedicated account management and periodic service reviews to discuss performance, reporting needs and roadmap items.

Vericool Ltd, Unit 6, Cirrus Court, Glebe Road, Huntingdon, Cambs, PE29 7DL
e: sales@vericool.co.uk w: www.vericool.co.uk t: 03302 020422 f: 01480 708070

Registered Office: Unit 6, Cirrus Court. Company Number: 10717195 VAT Number: 268273279

- Continuous improvement through customer feedback, enhancement requests and regular software releases.
- Guidance on best practice configuration for menus, allergens, spend controls and operational processes.

7. Technical requirements

Site and network prerequisites

- Reliable internet connectivity for cloud access although the system will work offline.
- Ability to allow outbound HTTPS/TLS traffic to the Vericool service endpoints.
- Where required, local network connectivity for POS terminals and peripherals (scanners, identification devices).

Client devices and software

- Supported POS hardware and peripherals as specified in the order form (or customer-supplied equivalents).
- A modern web browser for administrative access (current versions of Microsoft Edge/Chrome/Safari).
- Mobile app access for end-user pre-order/top-up (where enabled) on supported iOS/Android devices.

Integrations

- MIS integration requires appropriate access credentials and customer approval for data synchronisation.
- Any third-party payment services (where used).

8. Outage and maintenance management

Outage management

- Events are triaged using defined severity levels and escalation paths to technical leads and management.
- We provide status updates during major incidents and coordinate customer communications where service impact is material.
- Post-incident reviews are performed for significant incidents to identify root cause and corrective/preventative actions.

Planned maintenance

- Planned maintenance is communicated in advance where it may affect availability or functionality.
- Changes are deployed using controlled release processes with testing, approvals and rollback planning for material changes.

9. Hosting options and locations

The Vericool service is hosted in Microsoft Azure. Customer data is stored in the UK. Environments are logically segregated by customer, with role-based access controls and audited administration.

Options

- Standard hosted service (UK-hosted) for schools and multi-site estates.
- Dedicated or enhanced configurations (e.g., additional resilience, segregated resources) can be considered by agreement.

10. Access to data (upon exit)

On termination, Vericool supports access to customer data and an orderly transition. Data export and retention/deletion arrangements are confirmed contractually.

- Data exports can be provided in a mutually agreed format (e.g., CSV/Excel extracts for key datasets and reports).

- We agree a timeline for export and handover, including any dependency on third-party integrations.
- Following completion of the exit, access to the service is removed and data is retained or securely deleted in line with the contract and statutory obligations.

11. Security

Vericool is ISO27001 certified, Security is embedded across service design, delivery and operations. Vericool operates documented information security policies and processes, including access control, secure development, vulnerability management and incident response.

Access control

- Least privilege and role-based access control for administrative functions.
- Multi-factor authentication for management access and privileged accounts.
- Regular access reviews and prompt removal of access on role change or leaver events.

Data protection

- Encryption in transit using modern TLS 1.3; encryption at rest for stored data and backups.
- Segregation of customer data and audited administrative access.
- Configurable retention and secure deletion in line with contractual requirements.

Monitoring, vulnerability and incident management

- Protective monitoring using centralised logging and alerting for suspicious activity and service health.
- Risk-based vulnerability management including patching, dependency checks and periodic assurance testing.
- Documented incident response process covering containment, eradication, recovery and post-incident review.

Assurance and governance

- Security responsibilities and escalation routes are defined, with management oversight of significant risks and incidents.



- Policies are supported by staff onboarding and periodic security awareness training.
- Where applicable, third-party suppliers are assessed and monitored for security and service risk.

Vericool Ltd, Unit 6, Cirrus Court, Glebe Road, Huntingdon, Cambs, PE29 7DL
e: sales@vericool.co.uk w: www.vericool.co.uk t: 03302 020422 f: 01480 708070

Registered Office: Unit 6, Cirrus Court. Company Number: 10717195 VAT Number: 268273279