

LOGISTICS CONNECT LIMITED

KARGONET

Driver / Rider Privacy Notice and Terms of Use

For Kargonet Rider App, delivery tools and field operations

Document Type	Driver/Rider Privacy Notice and Terms of Use
Company / Brand	Logistics Connect Limited / Kargonet
Applies To	Drivers, riders, delivery agents, dispatch riders, contractors and field personnel using Kargonet systems
Systems Covered	Rider app, tracking system, scanner/mobile device, client portal-related delivery updates, dispatch tools and company communication channels
Effective Date	June 2026
Version	1.0
Owner	Operations / Transport / HR / IT
Approved By	General Manager

Important: This document is a practical operational draft. It should be reviewed by Ghana-qualified legal counsel before final publication or signature.

Document Control

Item	Details
Purpose	To inform drivers/riders how Kargonet collects and uses their information, and to set clear rules for use of the rider app, ERP, delivery tools and customer data.
Status	Draft for internal review and legal approval.
Review Cycle	Annually, or whenever there is a major change to the app, rider workflow, customer data processing, Ghanaian law, or courier regulatory requirements.
Distribution	Riders/drivers, dispatchers, hub supervisors, operations, transport, HR, IT and management.
Related Documents	Rider SOP, Courier SOP, employment/contractor agreement, HR disciplinary policy, vehicle and road safety policy, IT acceptable use policy, compensation/claims policy.

Plain-Language Acceptance Notice for Rider App

Suggested in-app wording: By signing in to the Kargonet rider app or using Kargonet delivery systems, you agree to follow the Driver/Rider Privacy Notice and Terms of Use. You must use customer data only for assigned delivery work, keep your login secure, update tracking honestly, capture POD/POP correctly, follow safety rules, and never collect unauthorized payments or Cash-on-Delivery unless the company gives written authorization.

Part A - Driver / Rider Privacy Notice

This Privacy Notice explains how Logistics Connect Limited, trading through Kargonet, collects, uses, stores and protects personal data relating to drivers, riders, delivery agents, contractors and field personnel who use Kargonet systems. It applies whether you access the rider app on a company device, personal device approved for work, scanner, ERP account, web portal, communication platform, or any related system used for dispatch, pickup, delivery, tracking and operational reporting.

1. Who this notice applies to

- Full-time and part-time drivers, riders, delivery agents and field staff.
- Contractors, outsourced riders, temporary riders and third-party delivery personnel authorized to use Kargonet systems.
- Dispatch, hub and transport personnel where their personal data is captured through rider/dispatch workflows.

2. Data controller and contact details

Item	Details
Data Controller	Logistics Connect Limited (Kargonet)
Address	Suit A5, 4 th Floor TDC Towers, Tema – Community Two
Privacy Contact	support@mykargonet.org
Support Contact	Vivian Osei-Anim
Data Protection Registration No.	Not available now

3. Personal data we may collect about drivers/riders

Data Category	Examples
Identity and profile data	Name, staff ID/rider ID, photograph, national ID/passport details where required, date of birth where needed for HR/contract records, emergency contact, next of kin.
Contact data	Phone number, email address, residential address or operational contact address.
Account and login data	Username, user ID, password credentials or authentication tokens, login time, failed login attempts, access role and device authorization status.

Data Category	Examples
Employment or contractor data	Role, department, hub/station, supervisor, contract status, attendance, training records, disciplinary records where applicable, payment/allowance information where processed through company systems.
Operational activity data	Assigned route, manifest, pickup jobs, delivery jobs, timestamps, scans, tracking status updates, failed delivery reason codes, cancellations, returns, RTS records, incident notes and shift logs.
Location and route data	GPS location, route progress, pickup/delivery location, time at stop, geotag linked to scans or status updates, location during active shifts or active jobs.
Proof of pickup/delivery data	POD/POP signatures, recipient/sender names, phone confirmations, delivery notes, photos of parcel/location, timestamp and staff/rider ID linked to each record.
Device and technical data	Device type, operating system, app version, IP address, browser/app logs, crash logs, scanner ID, SIM/network details where relevant, security logs and diagnostics.
Safety and compliance data	Vehicle inspection checklist, PPE checks, accident reports, security incident reports, unsafe location reports, loss/damage/tampering records, road safety compliance notes.
Communications data	Operational calls, SMS/WhatsApp/app messages where used for work, complaint notes, customer inquiry notes, escalation records and supervisor instructions.

4. Sensitive or special data

Kargonet does not normally require sensitive personal data from riders through the rider app. However, limited sensitive information may be processed where necessary for safety, HR, legal, insurance, emergency response or incident management. Examples may include medical fitness information after an accident, injury reports, or law enforcement incident records. Such data must be handled with restricted access and only for the specific purpose for which it is required.

5. How we collect driver/rider data

- Directly from you during onboarding, account creation, training, HR/contractor documentation, vehicle assignment and daily operations.
- Automatically when you sign in, accept jobs, scan packages, update statuses, upload POD/POP, use the app, or use a company device/scanner.
- From supervisors, dispatchers, hub staff, customer service, clients, customers, security personnel or other employees during operational reviews, complaints, incidents and investigations.
- From lawful third parties where needed for compliance, security, insurance, audits, regulatory matters, law enforcement or claims handling.

6. Why we use driver/rider data

Purpose	Examples of Use
Account setup and access control	Create rider accounts, assign roles, verify identity, prevent unauthorized access and manage password resets.
Dispatch and route execution	Assign pickups/deliveries, plan routes, monitor progress, reassign jobs and confirm job completion.
Tracking and chain of custody	Record custody of packages, scan milestones, update tracking for customers and resolve discrepancies.
Proof of pickup and delivery	Capture POP/POD, verify delivery, handle disputes, support claims, show delivery evidence and audit performance.
Safety and security	Monitor active jobs, identify unsafe locations, respond to accidents, protect packages and support emergency escalation.
Customer service and complaints	Investigate complaints, missed deliveries, delays, damaged packages, refused deliveries, misconduct allegations and service recovery actions.
Performance and compliance	Measure scan compliance, POD/POP completeness, attendance, on-time performance, route adherence, safety compliance and training needs.
Payments and administration	Process rider allowances, reimbursements, payroll inputs, contractor fees or other approved operational payments where applicable.
Legal, regulatory and audit obligations	Comply with Ghanaian laws, courier regulatory obligations, data protection obligations, insurance requirements, audit requests and lawful investigations.
System security and improvement	Detect misuse, troubleshoot errors, improve app reliability, manage backups, investigate suspicious access and maintain cyber security.

7. Location tracking rules

The rider app or company device may collect location data when you are signed in, assigned to a job, marked available, out for pickup, in transit, out for delivery, returning to hub, or otherwise actively performing Kargonet work. Location data is used for dispatch, customer updates, safety, chain of custody, dispute resolution and operational reporting.

- Location tracking should be limited to operational use and should not be used for improper personal surveillance.
- Riders must not disable location permissions, GPS, data connectivity or scanning features during assigned work unless instructed by a supervisor or required for safety.

- If a rider uses an approved personal device, the company should not access private photos, messages, contacts or non-work files unless the rider voluntarily submits them for a work-related purpose.
- Where location data is used in investigations, access should be limited to authorized management, HR, operations, transport, IT or legal/compliance personnel.

8. Legal basis for processing

Kargonet processes rider data where necessary for employment or contractor administration, performance of assigned duties, legitimate operational interests, legal and regulatory obligations, safety and security, claims handling, system security, and compliance with applicable data protection laws in Ghana. Where consent is legally required for a specific processing activity, the company should request clear consent separately and allow withdrawal where applicable.

9. Sharing of driver/rider data

Kargonet may share limited rider data where necessary and lawful, including with:

- Customers or clients, where a rider name/ID, delivery status or contact channel is necessary for the delivery service.
- Internal teams such as operations, transport, dispatch, hub supervisors, customer service, HR, finance, IT, management and audit.
- Technology providers hosting or supporting the rider app, cloud storage, authentication, analytics, backups, SMS/email and support tools.
- Insurance providers, auditors, professional advisers and dispute/claims handlers.
- Regulators, courts, law enforcement or government agencies where required by law or necessary to protect people, packages, company property or legal rights.

Kargonet should only share the minimum information necessary for the stated purpose and should use appropriate confidentiality, access control and security measures.

10. Data security

- Role-based access should be applied so riders only see the customer/package information needed for assigned work.
- Passwords, OTPs, access tokens and devices must not be shared.
- POD/POP photos, signatures and customer contact details should be stored only in approved Kargonet systems, not in personal galleries or personal cloud accounts unless the company has approved the workflow.
- Lost or stolen devices must be reported immediately to Operations/Transport/IT so access can be disabled and data can be protected.
- System logs, audits, backups and encryption may be used to protect records and investigate unauthorized access or misuse.

11. Data retention

Record Type	Suggested Retention Approach
Rider account and access logs	Keep while the rider is active and for a reasonable period after deactivation for audit, security and dispute resolution.

Record Type	Suggested Retention Approach
Package, tracking and POD/POP records	Keep for the period required by company policy, legal obligations, audit, claims handling and dispute resolution. Kargonet SOPs currently refer to at least 5 years for package and delivery records.
Incident, accident and security reports	Keep long enough for investigation, insurance, regulatory, legal, HR and safety management purposes.
Training and competency records	Keep while the rider is active and for a reasonable period afterward to evidence training and compliance.
Inactive accounts	Disable promptly when no longer needed. Retain necessary records, then delete/anonymize when no longer required.

12. Your responsibilities as a data subject and system user

- Keep your information accurate and promptly inform HR/Operations of changes to phone number, address, emergency contact, license status or other required work information.
- Use customer personal data only for assigned pickup, delivery, tracking, customer communication and incident reporting tasks.
- Do not copy, screenshot, export, sell, share or misuse customer data, package data, app data or company records.
- Report suspected data breaches, lost devices, unauthorized access, wrong customer details, suspicious messages or accidental disclosures immediately.

13. Driver/rider data rights

Subject to applicable law and company procedures, riders may request access to their personal data, correction of inaccurate data, deletion or restriction where legally available, and information about how their data is used. Some requests may be limited where records must be kept for legal, HR, operational, safety, audit, insurance, claims or dispute-resolution reasons.

Requests should be sent to: support@mykargonet.com

14. Changes to this Privacy Notice

Kargonet may update this Privacy Notice when there are changes to the rider app, courier operations, legal requirements, regulatory expectations, technology providers or internal policies. Riders will be notified of material changes through the app, email, WhatsApp, notice board, training session or other appropriate channel.

Part B - Driver / Rider App Terms of Use and Conduct Rules

These Terms of Use set the rules for drivers/riders using Kargonet systems. They should be read together with the rider SOP, employment or contractor agreement, HR policies, transport policies, safety rules and any instructions issued by Operations, Transport, Dispatch, Hub Supervisors, IT or Management.

1. Acceptance of terms

- By signing in, accepting a job, scanning a package, uploading POD/POP, using a company device, or accessing Kargonet systems, you agree to follow these Terms of Use.
- If you do not understand these terms, ask your supervisor before using the system.
- These terms do not replace your employment contract, contractor agreement or HR policy. If there is a conflict, the stricter operational, legal, safety or confidentiality requirement will normally apply unless management confirms otherwise in writing.

2. Authorized use only

- You may use Kargonet systems only for approved company work.
- You may access only jobs, packages, customer records, routes, photos, signatures and reports assigned to you or made available to your role.
- You must not use the app for personal deliveries, side jobs, unauthorized customer contact, competitor work, private business or non-company purposes.

3. Login, password and account security

- Use only your assigned login credentials. Do not share your password, OTP, token, PIN, device or account with anyone.
- Do not sign in for another rider or allow another person to scan, update, deliver, accept or close jobs under your account.
- You are responsible for actions recorded under your account unless you promptly reported unauthorized access or device loss.
- Report suspicious login alerts, password compromise, lost/stolen devices or unauthorized access immediately.

4. Accurate scanning and tracking updates

- All scans and status updates must reflect the actual event, location and time.
- Do not back-date, bulk-update, fake, guess, skip or falsify status updates.
- Required statuses may include Picked Up, Received at Facility, Out for Delivery, Delivered, Failed Delivery Attempt, Returned to Hub, RTS, Cancelled or system equivalents.
- If scanning fails because of device, barcode, battery, network or system issues, inform Dispatch/Hub Supervisor immediately and follow approved offline/manual logging procedures.

5. Package custody and handling

- Once you accept a package by scan or manifest sign-off, you are responsible for maintaining chain of custody until proper handover, delivery, return to hub or authorized transfer.
- Do not open, tamper with, repackage, relabel, break seals or inspect contents beyond approved visual checks.
- Do not leave packages unattended or hand packages to unauthorized persons.
- Follow special handling instructions for fragile, perishable, express, high-value or other controlled items.

6. Proof of pickup and proof of delivery

- POD/POP must be captured accurately and linked to the correct tracking number.
- Signatures must come from the sender, recipient or authorized representative. You must not sign on behalf of a customer.
- Names, phone numbers, timestamps and delivery notes must be entered truthfully and clearly.
- Photos should show the parcel/location clearly but avoid unnecessary capture of faces, IDs, private documents, private premises or sensitive personal information.
- POD/POP must be uploaded promptly, preferably at the time of the event or by end of shift if approved offline procedures apply.

7. Customer contact and communication

- Use customer contact details only for assigned pickup, delivery, access confirmation, rescheduling instructions from Dispatch/CS, and operational support.
- Keep communication polite, professional and brief. Do not argue with customers, gate/security staff or the public.
- Do not discuss pricing, compensation, refunds, insurance coverage, internal policy disputes or blame. Refer such matters to Customer Service or your supervisor.
- Do not save customer numbers for personal use, send unsolicited messages, contact customers outside work, or share customer contacts with third parties.
- Where communication occurs through WhatsApp/SMS/calls, document required operational notes in the approved system.

8. No cash collection / no unauthorized COD

Unless Kargonet issues a separate written COD policy and assigns you a COD job through the system, riders must not collect cash, mobile money, tips, bribes, delivery fees, penalties, storage charges, customs charges or any other payment from customers.

- If a customer offers payment, politely decline and refer them to Customer Service or the approved payment channel.
- If a shipment appears to require payment at the door, stop and contact Dispatch/Operations before handover.
- Unauthorized collection, solicitation or retention of customer money may lead to disciplinary action, repayment obligations, account suspension, termination and/or referral to law enforcement where appropriate.

9. Device, app and company equipment rules

- Company phones, scanners, vehicles, bags, uniforms, helmets, vests, power banks and access cards must be used carefully and returned when required.
- Do not install unauthorized apps, bypass security controls, root/jailbreak devices, disable device management, remove tracking/security tools or use company devices for inappropriate content.
- Keep device batteries charged and carry required chargers/power banks for the shift.
- Report damaged, faulty, missing or stolen equipment immediately.

10. Personal device use

- If Kargonet permits use of a personal device, the rider is responsible for keeping the device secure, updated, password-protected and available for assigned work.
- The rider must allow required app permissions for operational features such as camera, notifications and location during active work.

- Customer records, POD/POP images and package data must be stored in the app or approved company system, not retained in personal galleries or shared through personal accounts except as authorized.
- The company may restrict, suspend or revoke personal device use where there is a security, privacy, reliability or compliance concern.

11. Safety, road conduct and duty readiness

- Safety takes priority over speed. Obey traffic laws, speed limits and company road safety instructions.
- Wear required PPE, including helmet for motorbike riders, high-visibility vest, closed shoes and other equipment instructed by the company.
- Do not use a phone while riding/driving except in a safe stopped position or through approved hands-free procedures where lawful and safe.
- Do not report for duty or operate a vehicle under the influence of alcohol, drugs or any substance that impairs safe work.
- Complete daily vehicle pre-trip checks and do not depart with an unsafe vehicle.

12. Failed delivery, cancellations, returns and exceptions

- Failed delivery attempts must be recorded with the correct reason code and supporting notes.
- Do not abandon packages, leave them with unauthorized persons, or promise reattempt times independently.
- All cancellations, reroutes, returns and RTS actions must be confirmed by Dispatch/Operations and updated in the system.
- Damage, suspected tampering, loss, prohibited/suspicious items, unsafe locations, customer refusal, access denial and security incidents must be escalated immediately.

13. Prohibited conduct

Prohibited Conduct	Examples
Data misuse	Copying customer contacts, sharing addresses, posting POD photos online, selling customer data, taking screenshots for personal use.
False records	Fake scans, false failed delivery attempts, forged signatures, back-dated updates, wrong recipient names, closing jobs not completed.
Payment misconduct	Collecting unauthorized money, tips demanded from customers, COD outside approved process, mobile money into personal accounts.
Package misconduct	Opening parcels, tampering with seals, theft, unauthorized handover, leaving parcels unattended, using parcels for leverage in disputes.
System misuse	Sharing login, bypassing access controls, using another rider account, disabling tracking, deleting required evidence, unauthorized exports.
Customer misconduct	Insults, threats, harassment, discrimination, arguments, unauthorized personal contact, inappropriate messages or social media contact.

Prohibited Conduct	Examples
Safety misconduct	Dangerous riding/driving, ignoring PPE, operating unsafe vehicle, phone use while riding/driving, substance impairment.

14. Monitoring, audits and investigations

Kargonet may monitor and audit app use, location data, scan logs, device logs, POD/POP records, route progress, customer communications recorded in systems, access logs, vehicle records and package records for legitimate operational, safety, security, compliance and investigation purposes. Monitoring should be proportionate, access-controlled and limited to authorized personnel.

- Riders must cooperate with reasonable audits, discrepancy checks, claims investigations, customer complaint reviews, security investigations and legal/regulatory inquiries.
- Attempts to delete, hide, alter or destroy records may be treated as serious misconduct.

15. Suspension or restriction of access

Kargonet may suspend, restrict or terminate a rider's account where there is a suspected security risk, unauthorized access, device loss, privacy incident, misconduct, safety concern, falsified record, operational breach, termination of engagement or other legitimate business reason. Account restriction does not remove the rider from any separate obligation to cooperate with investigations, return equipment, complete handover or protect confidential information.

16. Confidentiality

- Customer information, package information, pricing, routes, dispatch plans, system access, internal documents, SOPs, business data and company records are confidential.
- Confidential information must not be disclosed outside approved work channels, including to friends, family, competitors, other riders without need-to-know, social media, or customers beyond what is required for their shipment.
- Confidentiality obligations continue after employment, contract or system access ends.

17. Intellectual property and system ownership

The rider app, tracking platform, forms, templates, reports, SOPs, logos, workflows, databases and system records are owned or licensed by Kargonet or its service providers. Riders receive only limited permission to use them for approved company work. No rights are transferred to riders.

18. App Availability and System Limitations

- We aim to keep the app, portal and tracking systems available, secure and accurate, but we do not guarantee uninterrupted or error-free operation.
- Access may be affected by maintenance, updates, internet disruption, cloud provider issues, power outages, device problems, cyber incidents, user error or events outside our control.
- We may update, suspend, restrict or discontinue any feature where necessary for security, compliance, performance, business operations or legal reasons.
- System records are operational records and may be corrected where errors, duplicate entries, missing scans or inaccurate information are identified.

19. Consequences of breach

Breach of these terms may result in coaching, retraining, warning, account suspension, removal from route, recovery of losses, disciplinary action, termination of employment/contract, report to regulators, insurance notification, civil action or referral to law enforcement, depending on the seriousness of the breach and applicable law/company policy.

20. Reporting concerns

Riders must promptly report:

- Lost/stolen device, badge, scanner, manifest, parcel, or access card.
- Wrong delivery details, mis-scan, missed scan, duplicate tracking number or suspicious system activity.
- Customer threats, attempted theft, unsafe locations, accidents, injuries, damage, loss or tampering.
- Data breach, unauthorized disclosure, customer data misuse, or request from a customer/third party that feels improper.

Reports should be made to: support@mykargonet.org, kwaku.kissiedu@logisticsconnectgh.com, gladys.anaman@logisticsconnectgh.com

21. Changes to these Terms of Use

Kargonet may update these terms when systems, workflows, SOPs, technology, regulatory obligations, risk controls or business requirements change. Continued use of the rider app or company systems after notification means the rider agrees to follow the updated terms, subject to applicable law and company HR/contract procedures.

Part C - Driver / Rider Acknowledgement Form

This page may be signed physically or accepted electronically inside the rider app.

I confirm that I have received, read and understood the Kargonet Driver/Rider Privacy Notice and Terms of Use. I agree to use Kargonet systems only for authorized work, protect customer and company data, keep my login secure, update tracking records truthfully, capture POD/POP correctly, follow the no unauthorized payment/no COD rule, comply with safety requirements, and report incidents, data breaches, lost devices and operational exceptions promptly.

Driver/Rider Name	
Staff/Rider ID	
Phone Number	
Hub / Station	
Role	
Signature	
Date	
Supervisor/Witness	

Electronic acceptance note: Where accepted electronically, the system should record rider ID, name, app/account ID, version accepted, timestamp, IP/device ID where available, and acceptance method.

Appendix - Quick Rider Rules for App Display

- Use only your own login. Never share passwords, OTPs or devices.
- Use customer data only for assigned pickup or delivery work.
- Keep location, camera, notifications and scanning active during assigned jobs.
- Scan and update statuses at the actual time and location of each event.
- Never fake scans, delivery attempts, customer names or signatures.
- Capture POD/POP carefully and avoid unnecessary private information in photos.
- Never collect unauthorized cash, mobile money, tips demanded from customers or COD.
- Report lost devices, damaged packages, unsafe locations, customer conflict or data breaches immediately.
- Return undelivered, cancelled or failed-delivery packages to hub as instructed.
- Follow road safety rules, PPE requirements and supervisor instructions at all times.