X2X COURIER
DATA PROTECTION POLICY
Protecting personal data across our delivery operations

Document ref.	Version	Effective date	Review date
X2X-DPP-001	1.0	8 September 2026	8 September 2027

Prepared by	Approved by	Classification
Data Protection Lead	Managing Director	Internal — all staff

This policy sets out how X2X Courier obtains, uses, stores, shares and deletes personal data. It applies to all employees, agency workers, self-employed couriers working under our control, contractors and anyone else who handles personal data for the company. It should be read with our privacy notice, staff privacy notice, CCTV notice and information security rules.

1. Purpose and scope

X2X Courier is a courier and last-mile delivery business. To collect, sort, transport and deliver consignments we necessarily process personal data about senders, recipients, customers, drivers and other staff. That data includes names, addresses, telephone numbers, email addresses, delivery instructions, signatures, proof-of-delivery photographs, tracking events, vehicle and handheld-device location data, payment and account records, and employment information.

We are committed to processing personal data lawfully, fairly and transparently, and to protecting it against unauthorised access, loss or misuse. This policy explains the standards we apply so that we comply with:

- the UK General Data Protection Regulation (UK GDPR);
- the Data Protection Act 2018;
- the Privacy and Electronic Communications Regulations 2003 (PECR), where we send electronic marketing;
- other applicable privacy, e-privacy and security law.

This policy covers personal data in any form: paper consignment notes, handheld scanners, routing software, emails, CCTV, telematics, phones, and cloud systems. It does not replace the need for a public-facing privacy notice or for contracts with customers and processors.

2. Key definitions

- **Personal data:** any information relating to an identified or identifiable living person.
- **Special category data:** data revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic or biometric data used to identify someone, health data, or data about sex life or sexual orientation. We process this only where a specific legal condition applies.

- **Processing:** anything done with personal data, including collecting, recording, storing, using, sharing, viewing on a scanner and deleting.
- **Data subject:** the person the data is about — for example a recipient, a customer contact or a courier.
- **Controller:** the organisation that decides why and how personal data is processed.
- **Processor:** an organisation that processes personal data on a controller's instructions, such as a software host or payroll bureau.
- **Personal data breach:** a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

3. Data protection principles

We will apply the UK GDPR principles. Personal data must be:

- **Lawful, fair and transparent:** we identify a lawful basis before we process, and we tell people what we do with their data.
- **Purpose-limited:** we collect data for specified delivery, account, employment and safety purposes, and we do not use it for incompatible new purposes without a further lawful basis.
- **Data-minimised:** we collect only what we need. Couriers must not photograph people, children, interiors of homes or unrelated documents "just in case".
- **Accurate:** we keep addresses, contact numbers and account details up to date and correct errors promptly when they are reported.
- **Storage-limited:** we do not keep personal data longer than we need it. Retention periods are set out in section 12.
- **Secure:** we use technical and organisational measures appropriate to the risk, including access control, encryption in transit where available, and staff training.
- **Accountable:** we can demonstrate compliance through this policy, records of processing, contracts, training records and incident logs.

4. Roles and responsibilities

4.1 Controller and processor roles

Our role depends on the work:

- **Controller:** we are the controller of our own staff data, supplier contacts, CCTV on our premises, telematics on our vehicles, website enquiries, and our own customer account records.
- **Processor or joint controller:** when we deliver for a business customer, that customer is usually the controller of sender and recipient data. We process that data on their instructions to complete the delivery. The contract with the customer must say this clearly. If we decide additional purposes of our own (for example our own fraud prevention or network analytics), we may be a controller or joint controller for those purposes.

Staff must not treat customer delivery data as X2X's to use for marketing, resale or any purpose outside the delivery contract.

4.2 Managing Director

The Managing Director is accountable for data protection and will:

- approve this policy and provide the resources needed to comply;
- appoint a Data Protection Lead;
- ensure the company is registered with the Information Commissioner's Office (ICO) where required and that the fee is paid;
- receive reports of serious incidents and data-subject complaints.

4.3 Data Protection Lead

X2X Courier has appointed a Data Protection Lead (not necessarily a statutory Data Protection Officer). That person will:

- maintain this policy, the record of processing activities and the retention schedule;
- advise on lawful bases, data-sharing and new systems;
- handle, or coordinate, data subject requests and ICO correspondence;
- log, assess and where required report personal data breaches;
- arrange training and spot-check compliance in the depot and on the road;
- review processor contracts and international transfers.

Contact details will be confirmed at induction and published in the privacy notice. External enquiries can be sent to the address or email stated in that notice.

4.4 Managers and dispatch

Managers and dispatch staff will:

- only give couriers the personal data they need for the day's work;
- not read out full addresses or phone numbers in public or over unsecured radio where it can be overheard;
- remove access promptly when someone leaves or changes role;
- escalate suspected breaches the same day.

4.5 All staff and couriers

Everyone who handles personal data must:

- use it only for the job in hand and not copy it onto personal phones, notebooks or messaging apps;
- lock screens, log out of scanners and not leave consignment notes, handhelds or keys unattended;
- not post delivery details, recipient names, addresses or proof-of-delivery images on social media;
- not look up, share or take home personal data out of curiosity;
- report lost devices, wrong-address disclosures and any other suspected breach immediately;
- complete data-protection training when asked.

A serious or repeated breach of this policy may result in disciplinary action and, for contractors or self-employed couriers, removal from work. Deliberate misuse of personal data can be a criminal offence.

5. What we process and why

The table below summarises the main processing in a courier operation. The live record of processing activities is held by the Data Protection Lead and must be updated when systems change.

Data and people	Examples	Purpose	Typical lawful basis
Recipients and senders	Name, address, phone, email, delivery instructions, signature, POD photo, tracking events	Collect, route, deliver, prove delivery, handle failed attempts and claims	Contract with the customer; legitimate interests in running a secure network. Where we are processor, we rely on the customer's basis.
Business customers	Account contacts, billing address, contract, payment records, service queries	Win, manage and bill the account; recover debt	Contract; legitimate interests; legal obligation (tax and accounting)
Drivers and staff	Identity, contact, right-to-work, licence, payroll, training, accident records, device ID	Employ or engage, pay, roster, train, meet legal duties	Contract; legal obligation; legitimate interests
Telematics and scanners	GPS location, route, speed events, scan timestamps, device logs	Dispatch, proof of attendance, vehicle security, investigate incidents, safety	Legitimate interests; legal obligation for health and safety. Staff are informed in the staff privacy notice.
Depot CCTV	Video images of staff, visitors and vehicles	Security of premises, parcels and people; investigate incidents	Legitimate interests. A CCTV notice is displayed.
Website and marketing	Enquiry forms, cookies, email lists	Respond to quotes; send service updates or marketing where allowed	Contract / steps prior to contract; consent or soft opt-in for electronic marketing under PECR
Claims and incidents	Loss, damage, collision and complaint files	Investigate, defend legal claims, notify insurers	Legitimate interests; legal claims; legal obligation

We do not routinely need special category data to deliver parcels. If a delivery instruction contains health information (for example "recipient has limited mobility — leave with carer"), we will use it only to complete that delivery and will not copy it into general notes more widely than needed. Staff health data is handled under employment law and, where required, the explicit-consent or employment-law conditions in the Data Protection Act 2018.

6. Fair processing information

We will tell people how we use their data in language they can understand:

- A privacy notice on our website and, where practical, on booking confirmations and account paperwork.
- A staff / courier privacy notice at induction, covering monitoring, telematics, CCTV and licence checks.
- CCTV signage at depot entrances.
- Where we act as processor, the customer is responsible for telling its own senders and recipients. We will help that customer if they ask us for wording about the delivery stage.

If we obtain recipient details from a customer rather than from the recipient, we will not send a separate privacy notice to every doorstep unless a particular campaign or service makes that necessary. Recipients can still exercise their rights by contacting us or the customer.

7. Data subject rights

People have rights over their personal data. We will respond without undue delay and within one month, extendable by two months for complex or numerous requests. We may ask for ID where we are not sure who is asking. We will not charge a fee unless a request is manifestly unfounded or excessive.

- **Access:** a copy of the personal data we hold and supporting information.
- **Rectification:** correction of inaccurate address, name or contact data.
- **Erasure:** deletion where the data is no longer needed, consent is withdrawn, or processing is unlawful. We may refuse where we must keep records for claims, accounting or legal duty.
- **Restriction:** limiting how we use data while a challenge is resolved.
- **Portability:** where processing is automated and based on consent or contract, provide data in a reusable format.
- **Objection:** object to processing based on legitimate interests, including profiling, and to direct marketing (this must be honoured immediately).
- **Withdraw consent:** where consent is our basis, it can be withdrawn at any time.
- **Not to be subject to solely automated decisions:** we do not make solely automated decisions that produce legal or similarly significant effects about individuals without a human review route.

Requests can come through any channel — the doorstep, a driver, email or social media. Staff who receive a request must pass it to the Data Protection Lead the same working day and must not ignore it or invent an answer. Where we are only the processor, we will notify the customer controller promptly and follow the contract.

8. Information security

Security measures will be proportionate to the harm that misuse of delivery and staff data could cause (identity theft, stalking, parcel theft, fraud). As a minimum we will:

- Issue individual logins for scanning, routing and office systems. Shared passwords are not allowed.
- Apply role-based access so a courier sees only the stops they need.
- Use screen locks, PIN or biometric unlock on handhelds, and remote wipe where the device supports it.
- Encrypt laptops used for office work and avoid sending spreadsheets of addresses by unencrypted email.
- Keep paper run-sheets face down in the vehicle and return or shred them at the end of the shift.
- Site servers and routers in access-controlled areas; keep software patched.
- Vet staff appropriate to the role and remove system access on the last day of work.
- Prohibit use of personal WhatsApp, personal email or personal cloud drives for recipient lists, POD images or staff files.

Couriers must not take home printed manifests. Lost or stolen scanners, phones, laptops or paper runs are a potential personal data breach and must be reported at once.

9. Processors and data sharing

We share personal data only where we have a lawful reason. Typical recipients include:

- The customer who booked the consignment, so they can track and prove delivery.
- Subcontracted owner-drivers and partner carriers, limited to what they need to complete a specified job.
- Software providers (scanning, routing, telematics, payroll, email).
- Insurers, solicitors, loss adjusters and the police where necessary for claims, crime or legal duty.
- HMRC and other regulators where the law requires it.

Before we appoint a processor we will carry out proportionate due diligence and put in place a written contract that meets UK GDPR Article 28: documented instructions, confidentiality, security, sub-processor rules, assistance with rights and breaches, deletion or return of data at the end of the contract, and audit rights. We will not sell personal data.

10. International transfers

Some cloud suppliers store or support data outside the UK. We will not transfer personal data to a third country unless:

- the UK has found that country adequate; or
- we use an approved transfer tool such as the UK International Data Transfer Agreement or the UK Addendum to the EU SCCs, plus a transfer risk assessment; or
- a specific exception in UK GDPR applies (used sparingly).

Staff must not upload X2X delivery or staff files to personal overseas tools.

11. Personal data breaches

Examples in this business include: a scanner or manifest left in a public place; an email with a recipient list sent to the wrong customer; a proof-of-delivery photo of a person posted online; a misdelivered parcel that exposes the contents and addressee to a stranger; ransomware on office systems; or a driver looking up an address for a friend.

Anyone who discovers a suspected breach must:

- contain it if they can do so safely (remote lock, retrieve paper, recall email);
- report it immediately to their supervisor and the Data Protection Lead — do not wait until the end of the week;
- not discuss the incident on social media or with anyone who does not need to know.

The Data Protection Lead will log the incident, assess likelihood and severity of risk to people, and decide whether to notify the ICO within 72 hours and whether to tell affected individuals. A decision not to notify will be recorded with reasons. Lessons learned will feed into training and system changes.

12. Courier-specific rules

12.1 Proof of delivery and photographs

Signatures and photographs are collected to show that a consignment was delivered or that a safe-place / neighbour delivery was made. Staff must:

- photograph only the parcel and the immediate drop location, not faces, children, house interiors, documents or car registrations unless they are unavoidably in shot and needed;
- not ask a recipient to pose;
- not use “safe place” photos that reveal a hidden key or an insecure entry point that could help a thief — choose a framed shot of the parcel only;
- not send POD images to personal devices or social media.

Recipients who object to a photograph should be offered a signature or another agreed method, and dispatch should be told.

12.2 Vehicle tracking and handheld location

Location data is used to dispatch work, confirm attendance, recover stolen vehicles, investigate collisions and defend claims. It is not a tool for all-day personal surveillance. Managers will:

- access live tracking for operational reasons, not to monitor breaks without cause;
- keep historic tracks only for the period in the retention schedule;
- tell staff in the staff privacy notice that tracking is in use.

Personal use of a tracked vehicle outside working hours, if allowed, will be treated in line with the vehicle policy so that private journeys are not reviewed routinely.

12.3 CCTV

CCTV at depots is operated for security of people, vehicles and parcels. Cameras will not be hidden. Footage will be viewed only by authorised people, kept for a short default period unless needed for an investigation, and disclosed to the police where justified. Covert monitoring will not be used unless a specific investigation meets the high threshold in employment and data-protection law and has been authorised by the Managing Director.

12.4 Failed deliveries and neighbours

Leaving a parcel with a neighbour or in a nominated safe place involves disclosing that a named person is receiving goods. We will only do this where the customer or recipient has authorised it, or where it is a documented last-resort service rule that the customer has accepted. Cards left at the property must not expose extra personal data beyond what is needed to collect the item.

12.5 Children

We do not target services at children. Parcels may be addressed to a household where children live. Staff must not photograph children, must not hand a parcel to a child who cannot take responsible receipt, and must follow the customer’s age-restricted delivery rules (for example 18+ items).

13. Retention

We will keep personal data only as long as needed for the purpose, including legal, tax and claims periods. Indicative periods are below. The Data Protection Lead may apply a longer or shorter period where risk or law requires it.

Record	Typical period	Reason
Tracking events, scan history, POD signature / photo	13 months after delivery	Queries, claims window, customer contract
Customer account and invoicing	6 years after end of account year	Tax, Limitation Act claims
CCTV footage (no incident)	30 days	Security; minimisation
Telematics / GPS tracks (no incident)	90 days	Dispatch and short-term investigation
Incident, collision, claim and complaint files	6 years after closure (longer if litigation is active)	Legal claims
Staff HR files	6 years after employment ends, unless a longer duty applies	Employment and legal claims
Recruitment records (unsuccessful)	6 to 12 months	Defend hiring decisions
Marketing suppression / opt-out lists	Until the person asks us to remove the suppression, or it is no longer needed	PECR — prove we will not contact them

When the period ends, data will be securely deleted, anonymised or shredded. Backup copies will fall out of rotation. Paper waste from the depot will be shredded or placed in confidential waste, not in open recycling.

14. Direct marketing and the website

Electronic marketing to individuals (email, SMS, some in-app messages) will only be sent:

- with consent; or
- under the PECR “soft opt-in” to existing customers about similar services, with a clear opt-out at collection and in every message.

We will keep a suppression list and honour opt-outs promptly. Business-to-business contact may be treated differently under PECR but we will still offer an opt-out and respect objections under UK GDPR.

Cookies and similar technologies on our website that are not strictly necessary will be used only with consent. A cookie notice will explain what we use and how to change the choice.

15. Data protection by design

Before we introduce a new scanner platform, camera type, routing tool, AI feature, customer portal or overseas supplier, the project owner must consult the Data Protection Lead at the design stage. We will ask: what data is collected, why, who sees it, where it is stored, how long it is kept, and what happens if the supplier is breached. A data protection impact assessment (DPIA) will be completed where processing is likely to result in high risk — in particular systematic location monitoring of staff, large-scale CCTV, or new uses of POD images.

16. Training, monitoring and review

All staff and regular couriers will receive data-protection induction before they handle live personal data, and a refresher at least annually or after a serious incident. Completion will be recorded.

We will monitor compliance through access reviews, device checks, incident trends and sample audits of POD images. This policy will be reviewed at least every 12 months, and sooner after a material system change, a serious breach, ICO guidance change or enforcement action.

17. Complaints

Anyone who is unhappy with how we have used their personal data should contact the Data Protection Lead first so that we can put it right. They also have the right to complain to the Information Commissioner's Office: ico.org.uk, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, telephone 0303 123 1113.

18. Document control

This is a controlled document. Printed copies are uncontrolled after the review date. The current version is held by the Data Protection Lead.

Version	Date	Author	Summary of change
1.0	8 Sep 2026	Data Protection Lead	First issued policy for X2X Courier.

Acknowledgement

I confirm that I have received, read and understood this Data Protection Policy and that I will follow it while handling personal data for or on behalf of X2X Courier.

Name: _____ Role: _____

Signature: _____ Date: _____

This policy is a statement of X2X Courier's intent and arrangements. It does not replace the privacy notice, processor contracts or statutory duties. If any part of this document conflicts with current law, the law takes precedence.