CRAWFORDS

Privacy Policy

Version:	1.0
Dated:	13 April 2026
Document Owner:	Ahmed Kamara – IT/DPO / ISMS Manager

Revision History

Version	Date	Revision Author	Summary of Changes
V 1.0	April 2026	A Kamara	Original Policy

Approval

Version	**Approval Board**	**Date of Approval**
V 1.0	Jimmy Lazarou (CEO)	April 2026

1. Purpose

Mistybridge Ltd, trading as CDS, and Crawford Cars Ltd, trading as Crawfords, are committed to protecting personal data and respecting the privacy rights of customers, passengers, employees, drivers, couriers, applicants, suppliers and other individuals whose information they process.

This Privacy Notice explains:

- what personal data may be collected;
- why it is processed;
- the lawful bases relied upon;
- who it may be shared with;
- how long it may be retained;
- how it is protected;
- the rights individuals have in relation to their personal data;
- how privacy questions or concerns can be raised.

This notice should be read alongside any more specific privacy information supplied for a particular service or processing activity.

2. Definitions

The Companies
Mistybridge Ltd, trading as CDS, and Crawford Cars Ltd, trading as Crawfords.

References to “we”, “us” and “our” in this notice mean the relevant Company responsible for the particular processing activity, unless expressly stated otherwise.

Personnel
Directors, employees, workers, drivers, couriers, contractors, agency personnel and other persons working for or on behalf of either Company.

Personal data
Information relating to an identified or identifiable living individual.

Special category personal data
Personal data revealing or concerning matters such as health, racial or ethnic origin, religion or belief, biometric information used for identification, sex life or sexual orientation.

Processing

Any operation performed on personal data, including collecting, recording, storing, accessing, using, sharing, updating, retaining or deleting it.

Controller

The legal entity that determines why and how personal data is processed.

Processor

An organisation that processes personal data on behalf of a controller.

Data subject

The individual to whom personal data relates.

3. Scope

This Privacy Notice applies to personal data processed by Mistybridge Ltd, trading as CDS, and Crawford Cars Ltd, trading as Crawfords.

It may apply to personal data concerning:

- customers;
- passengers;
- account customers;
- website visitors;
- drivers and chauffeurs;
- couriers;
- employees and workers;
- job applicants;
- contractors;
- suppliers;
- business contacts;
- complainants;
- visitors to Company premises;

- members of the public interacting with either Company.

It applies to personal data processed through systems and services including, where relevant:

- booking and dispatch systems;
- Freedom X and associated mobile applications;
- Coda Navigator;
- Microsoft 365;
- email;
- SharePoint and OneDrive;
- Sage;
- 3CX;
- websites and online booking facilities;
- CCTV;
- vehicle and operational systems;
- HR and recruitment records;
- complaint and lost-property records;
- supplier and contract records.

Where a processing activity belongs only to one Company, that Company remains responsible for the data-protection obligations applicable to that activity.

The use of this shared notice does not transfer controller responsibility from one Company to the other.

4. Who is the data controller?

This section must reflect the Companies' actual arrangements.

4.1 Crawford Cars Ltd

Crawford Cars Ltd, trading as Crawfords, is the controller for personal data where it determines the purposes and means of processing in connection with its own services and activities.

This may include activities such as private-hire bookings, passengers, drivers and complaints **where those activities are operated by Crawford Cars Ltd**.

4.2 Mistybridge Ltd

Mistybridge Ltd, trading as CDS, is the controller for personal data where it determines the purposes and means of processing in connection with its own services and activities.

This may include courier, delivery or other CDS activities **where those activities are operated by Mistybridge Ltd**.

4.3 Shared processing

The Companies use some shared Personnel, premises, systems, infrastructure and support arrangements.

Shared systems do not, by themselves, make the Companies joint controllers.

Where both Companies genuinely determine the purposes and means of a particular processing activity jointly, the relationship must be documented appropriately and the relevant privacy information provided to affected individuals.

5. Privacy contact

Questions about this Privacy Notice or the use of personal data should be directed to:

Data Protection Contact / DPO: Ahmed Kamara
Email: ahmed@crawfords.co.uk
Telephone: 020 8752 8000
Postal address: Unit 8, Concord Business Centre, Concord Road, W3 0TR

Where a request relates to a particular Company, it will be handled on behalf of the relevant controller.

6. Personal data we may collect

Depending on the relationship and service involved, the Companies may process the following categories of personal data.

6.1 Identity information

This may include:

- name;
- title;
- date of birth where necessary;

- photograph;
- signature;
- identification-document information.

6.2 Contact information

This may include:

- home or business address;
- email address;
- telephone number;
- emergency contact information.

6.3 Booking and journey information

This may include:

- pickup address;
- destination;
- booking date and time;
- passenger name;
- contact details;
- journey instructions;
- booking reference;
- account information;
- driver and vehicle allocation;
- journey status;
- customer-service notes.

6.4 Courier and delivery information

This may include:

- sender details;
- recipient details;
- collection and delivery addresses;
- telephone numbers;
- delivery instructions;
- job reference;
- proof of delivery;
- courier allocation.

6.5 Financial information

This may include:

- payment records;
- invoices;
- account information;
- billing details;
- transaction history;
- refund information.

Payment-card information should only be processed to the extent required by the approved payment service and applicable security arrangements.

6.6 Driver, chauffeur and courier information

This may include:

- contact details;
- licence details;
- vehicle information;
- insurance details;
- identification documents;

- right-to-work evidence where applicable;
- training records;
- performance information;
- booking or job history;
- complaints;
- incident records.

6.7 Employee and applicant information

This may include:

- employment history;
- references;
- right-to-work information;
- payroll information;
- bank details;
- training records;
- attendance information;
- performance records;
- disciplinary and grievance information;
- recruitment records.

Additional workforce privacy information may be provided separately where appropriate.

6.8 Communications

This may include:

- emails;
- telephone records;
- customer-service communications;

- complaints;
- website enquiries;
- correspondence.

6.9 CCTV and security information

Where CCTV is operated, personal data may include:

- images;
- date and time;
- location;
- incident-related footage.

6.10 Technical information

This may include:

- IP address;
- device information;
- system login information;
- audit logs;
- application activity;
- security-event information.

6.11 Special category and sensitive information

Where necessary and lawful, the Companies may process information relating to:

- health or disability;
- accessibility requirements;
- safeguarding;
- other sensitive matters connected with employment, passenger safety or service provision.

Such information will receive additional protection.

7. How personal data is collected

Personal data may be collected:

- directly from the individual;
- from an account customer;
- from a passenger booking made on another person's behalf;
- through websites or online booking services;
- through telephone or email;
- through drivers or couriers;
- through recruitment processes;
- from suppliers and Business Partners;
- through CCTV;
- from operational systems;
- from public authorities where lawful;
- from publicly available sources where appropriate.

Where another person provides personal data on an individual's behalf, they should have authority or a legitimate reason to do so.

8. Why we process personal data

Personal data may be processed for the following purposes.

8.1 Providing services

To:

- accept and manage bookings;
- allocate drivers, vehicles or couriers;
- coordinate passenger journeys;
- manage collections and deliveries;
- communicate service information;

- confirm completion;
- issue invoices;
- process payments and refunds.

8.2 Customer service and complaints

To:

- respond to enquiries;
- investigate complaints;
- manage lost property;
- resolve service issues;
- monitor customer satisfaction;
- improve services.

8.3 Safety and safeguarding

To:

- protect customers and Personnel;
- investigate serious incidents;
- manage safeguarding concerns;
- cooperate with emergency services or regulators;
- maintain relevant evidence.

8.4 Business administration

To:

- manage customer accounts;
- maintain accounting records;
- manage suppliers;
- administer contracts;

- conduct internal reporting;
- maintain business records.

8.5 Employment and recruitment

To:

- recruit Personnel;
- manage employment or engagement;
- administer payroll and benefits;
- assess competence;
- provide training;
- manage workplace matters;
- meet legal obligations.

8.6 Information security

To:

- manage accounts and access;
- prevent fraud;
- detect security incidents;
- protect systems;
- maintain logs;
- investigate unauthorised activity;
- support business continuity.

8.7 Legal and regulatory compliance

To:

- comply with transport or licensing requirements;
- respond to lawful regulatory requests;

- maintain statutory records;
- cooperate with police or public authorities;
- establish, exercise or defend legal claims.

9. Lawful bases for processing

The lawful basis used will depend upon the specific processing activity.

Contract

Processing may be necessary to:

- provide a requested journey or delivery;
- administer an account;
- fulfil a customer contract;
- take steps before entering into a contract;
- administer employment or contractor arrangements.

Legal obligation

Processing may be required to meet obligations relating to:

- licensing;
- taxation;
- employment;
- health and safety;
- regulatory records;
- law-enforcement cooperation where legally required.

Legitimate interests

Processing may be necessary for legitimate business interests such as:

- operating and improving services;
- preventing fraud;

- maintaining information security;
- managing complaints;
- protecting business assets;
- maintaining customer relationships;
- establishing or defending legal claims.

Where legitimate interests are relied upon, the relevant Company will consider the impact on individuals.

Consent

Consent will only be relied upon where:

- it is genuinely voluntary;
- the individual has a real choice;
- it can be withdrawn;
- another lawful basis is not more appropriate.

Using a website or booking a service does not automatically mean an individual has "consented" to all processing described in this notice.

Vital interests

In exceptional circumstances, personal data may be processed where necessary to protect someone's life.

Special category data

Where special category personal data is processed, an additional lawful condition will be identified where required.

10. Children and vulnerable individuals

The Companies may process information relating to children or vulnerable individuals where they are passengers, customers, dependants or otherwise connected with a service.

Only information reasonably necessary for:

- safe service delivery;
- safeguarding;

- accessibility;
- emergency response;
- legal compliance

should be processed.

Additional care must be taken when sharing or recording such information.

11. Who personal data may be shared with

Personal data may be shared with authorised recipients where necessary.

These may include:

- drivers and chauffeurs;
- couriers;
- account customers;
- IT and cloud providers;
- booking-system providers;
- payment providers;
- accountants or auditors;
- insurers;
- professional advisers;
- recruitment or HR providers;
- approved suppliers and subcontractors;
- law enforcement;
- Transport for London;
- local authorities;
- courts;
- regulators;

- emergency services.

Only the information necessary for the purpose should be shared.

12. Drivers and couriers

Drivers, chauffeurs and couriers may receive information needed to perform an assigned booking or job.

This may include:

- passenger/customer name;
- pickup or collection location;
- destination;
- contact details;
- relevant journey or delivery instructions.

They must not:

- use the information for unrelated purposes;
- retain it unnecessarily;
- disclose it to unauthorised persons;
- use passenger or customer information for personal contact;
- share screenshots or booking details without authority.

13. Data processors and suppliers

Where a supplier processes personal data on behalf of a Company, appropriate contractual controls must be established.

These may include requirements relating to:

- confidentiality;
- security;
- permitted processing;
- subcontracting;
- incidents;

- deletion or return of data;
- assistance with data-subject rights.

Supplier access must be limited to what is required for the service.

14. International transfers

Some suppliers or cloud services may process information outside the United Kingdom.

Where personal data is transferred internationally, the relevant Company will ensure that appropriate safeguards are used where required.

These may include:

- adequacy regulations;
- approved contractual safeguards;
- supplementary security measures.

The Companies should maintain evidence of applicable international-transfer arrangements within their supplier and privacy records.

15. Information security

The Companies use proportionate technical and organisational measures designed to protect personal data.

These may include:

- access controls;
- unique user accounts;
- MFA;
- encryption;
- endpoint security;
- secure cloud services;
- backup and recovery;
- information classification;
- secure physical storage;

- logging;
- staff training;
- supplier controls;
- incident management.

No security measure can remove all risk, but controls are reviewed and improved as appropriate.

16. Personal devices

Personal data should only be accessed from personal devices where authorised under approved BYOD or remote-access arrangements.

The current privacy documents refer to information potentially being stored on employee-owned devices. This should not remain as an unrestricted statement. Personal devices may only process Company personal data where the device and access method meet the Companies' approved security requirements.

17. Data retention

Personal data will not be retained for longer than necessary.

Retention periods will be determined according to:

- legal requirements;
- regulatory obligations;
- contractual requirements;
- limitation periods;
- operational need;
- complaint and incident requirements;
- insurance requirements;
- data-protection principles.

The detailed periods must be maintained in the **Retention and Destruction Policy / Data Retention Schedule**.

This avoids conflicts between the privacy notice and other controlled records policies.

Examples of records requiring defined retention include:

- booking records;
- complaints;
- lost-property records;
- employee records;
- driver records;
- CCTV;
- financial information;
- recruitment records;
- supplier records;
- security logs.

Where information is subject to an investigation, legal claim or regulatory requirement, routine deletion may be suspended.

18. Secure destruction

At the end of the approved retention period, personal data will be:

- securely deleted;
- securely destroyed;
- anonymised;
- or otherwise disposed of using an approved method.

Methods may include:

- secure electronic deletion;
- cryptographic erasure;
- confidential shredding;
- certified hardware destruction;
- approved disposal providers.

19. Data accuracy

The Companies will take reasonable steps to keep personal data accurate and up to date.

Individuals should tell the relevant Company where:

- contact information changes;
- account information is inaccurate;
- another correction is required.

Inaccurate information will be corrected where appropriate.

20. Individual rights

Depending upon the circumstances, individuals may have rights including:

- **right of access** – obtaining information about and a copy of personal data;
- **right to rectification** – correcting inaccurate or incomplete information;
- **right to erasure** – requesting deletion in certain circumstances;
- **right to restrict processing** – requesting limited processing in certain circumstances;
- **right to object** – objecting to certain processing, including some legitimate-interest processing;
- **right to data portability** – receiving certain information in a portable format where the requirements apply;
- **rights concerning automated decision-making** where applicable;
- **right to withdraw consent** where processing genuinely relies on consent.

These rights are not absolute and may be subject to legal exemptions.

21. Access requests

Individuals may request access to their personal data by contacting the DPO / privacy contact.

Before disclosing information, the relevant Company may:

- verify the requester's identity;
- clarify the scope of a request where necessary;
- redact information relating to other individuals;
- apply applicable legal exemptions.

Requests must be recorded and managed within the applicable statutory timeframe.

22. Requests made on behalf of another person

Where someone makes a request for another individual, evidence of authority may be required.

Examples include:

- signed authority;
- power of attorney;
- parental responsibility where applicable;
- another legally recognised authority.

The Companies must take appropriate steps to protect information from unauthorised disclosure.

23. Personal data breaches

A personal data breach may include:

- information sent to the wrong recipient;
- lost paperwork;
- lost or stolen devices;
- unauthorised access;
- inappropriate disclosure;
- accidental deletion or loss;
- ransomware;
- compromised accounts.

Personnel must report actual or suspected breaches immediately through the approved incident-reporting route.

The DPO will assess:

- the nature of the breach;
- affected data;
- affected individuals;

- likely consequences;
- containment;
- notification requirements.

Where required, the relevant controller will notify the Information Commissioner's Office and/or affected individuals within the applicable statutory requirements.

24. Automated decision-making

The Companies will provide appropriate information where a decision producing legal or similarly significant effects is made solely by automated means.

Routine use of software to:

- allocate jobs;
- route vehicles;
- prioritise work;
- generate reports

does not necessarily constitute automated decision-making of this type.

Where significant automated decision-making is introduced, the processing must be reviewed before implementation.

25. Marketing

Direct marketing will only be carried out where there is an appropriate lawful basis and applicable electronic-marketing requirements are met.

Individuals may opt out of marketing communications at any time.

Opting out of marketing does not prevent communications that are necessary for:

- bookings;
- contracts;
- safety;
- account administration;
- legal or regulatory purposes.

26. Cookies and website technologies

Where Company websites use cookies or similar technology, separate cookie information should explain:

- what is used;
- why it is used;
- whether it is necessary;
- how preferences can be managed.

Non-essential cookies should be handled according to applicable consent requirements.

27. Complaints about privacy

Privacy concerns should first be raised with:

Ahmed Kamara – DPO / Privacy Contact
Email: ahmed@crawfords.co.uk
Telephone: 020 8752 8000

The Companies will investigate concerns and seek to resolve them appropriately.

Individuals also have the right to complain to the **Information Commissioner's Office (ICO)**.

28. Records of processing

The Companies should maintain appropriate records describing their personal-data processing.

These should identify, where applicable:

- the relevant Company/controller;
- category of data subjects;
- categories of personal data;
- processing purpose;
- lawful basis;
- recipients;
- international transfers;
- retention period;

- security controls;
- processor arrangements.

This is particularly important because the two legal entities share systems and operational support.

29. Data protection by design and default

New systems, services and significant changes involving personal data must consider privacy requirements before implementation.

This may include:

- identifying the controller;
- minimising data;
- defining lawful basis;
- limiting access;
- defining retention;
- assessing suppliers;
- configuring security;
- completing a Data Protection Impact Assessment where appropriate.

30. Data Protection Impact Assessments

A DPIA should be considered where processing is likely to result in a high risk to individuals.

Examples may include:

- significant new surveillance;
- large-scale sensitive data;
- new tracking technologies;
- significant automated decision-making;
- novel processing of vulnerable individuals;
- new technologies creating material privacy risks.

DPIA decisions and outcomes must be documented.

31. CCTV

Where CCTV is used, it must be operated for defined and legitimate purposes.

Controls must address:

- appropriate signage;
- restricted access;
- retention;
- disclosure;
- security;
- incident preservation;
- individual rights.

CCTV footage must not be used for unrelated purposes without an appropriate lawful basis.

32. Call recording

Where telephone calls are recorded, the Companies must:

- identify the purpose;
- identify a lawful basis;
- inform callers appropriately;
- limit access;
- define retention;
- protect recordings;
- respond appropriately to access requests.

Call-recording arrangements should be documented separately where applicable.

33. Employment and workforce privacy

Employees, workers and applicants may require more detailed privacy information than can reasonably be included in this public notice.

The Companies should therefore maintain an appropriate:

Employee and Recruitment Privacy Notice

covering matters including:

- HR records;
- payroll;
- sickness and absence;
- recruitment;
- performance;
- training;
- disciplinary records;
- workplace monitoring;
- legal obligations.

Where the two Companies employ different Personnel, the employing legal entity must be clearly identified as controller.

34. Driver and courier privacy

Where drivers, chauffeurs or couriers are engaged by either Company, their privacy information should explain processing relating to:

- onboarding;
- licences;
- insurance;
- identity;
- job allocation;
- location information;
- performance;
- complaints;
- incidents;

- payments;
- compliance checks.

If the contractual relationship differs between Mistybridge Ltd and Crawford Cars Ltd, the relevant controller must be identified clearly.

35. Changes to this Privacy Notice

This notice will be reviewed periodically.

It may be updated following:

- changes to services;
- new systems;
- new suppliers;
- changes to controller arrangements;
- legal or regulatory change;
- audit findings;
- significant privacy incidents.

Material changes will be communicated where appropriate.

36. Related documents

- Information Security Policy
- Information Classification Policy
- User Access Control Policy
- Acceptable Use Policy
- Retention and Destruction Policy
- Information Security and Privacy Training Policy
- Incident Management Procedure
- Personal Data Breach Procedure
- Complaints Policy and Procedure

- Lost Property Policy and Procedure
- Remote Access Policy
- Cloud Technology Policy
- CCTV Policy / Procedure
- Data Retention Schedule
- Record of Processing Activities
- Data Protection Impact Assessment Procedure
- Employee and Recruitment Privacy Notice
- Driver and Courier Privacy Notice

37. Review and document control

This Privacy Notice will be reviewed:

- at least annually;
- following material changes to processing;
- following changes to controller responsibilities;
- following material legal or regulatory changes;
- after significant privacy incidents;
- following audit findings.

Superseded versions must be removed from active publication and retained in accordance with documented-information controls.

Approved by: Jimmy Lazarou (CEO)
Date: 13th April 2026
Review Frequency: Annual