Road Collision Support Network Ltd

Data Processing Policy

June 2026

1 INTRODUCTION

This Policy is a supporting document to the Data Protection Policy of Road Collision Support Network Ltd, a company registered in the United Kingdom under number 16480486, whose registered office is at Unit 4b Boldero Road, Bury St. Edmunds, IP32 7BS ("the Company") regarding data protection and the rights of data subjects, e.g. staff, customers, business contacts etc.

This Policy sets out rules and guidance for all employees, agents, contractors, or other parties working on behalf of the Company regarding the handling of personal data.

2 DEFINITIONS

"consent"	means the consent of the data subject which must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they (by a statement or by a clear affirmative action) signify their agreement to the processing of personal data relating to them;
"Data Protection Legislation"	means all applicable data protection and privacy laws including, but not limited to, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the "UK GDPR"), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation;
"data subject"	means a living, identified, or identifiable individual about whom the Company holds personal data;
"personal data"	means any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification

	number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject. Unless otherwise stated, references in this Policy to "personal data" shall also include special category personal data;
"personal data breach"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed;
"processing"	means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"special category personal data"	means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, biometric, or genetic data.

3 DATA PROTECTION RESPONSIBILITY & SCOPE OF POLICY

Although the Company is not required to appoint a formal Data Protection Officer under Article 37 UK GDPR, Neil Clarke fulfils this role internally and is responsible for ensuring compliance with applicable data protection legislation.

All staff or other parties working on behalf of the Company comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.

Any questions relating to this Policy, the Company's collection, processing, or holding of personal data, or to the Data Protection Legislation should be referred to the Director responsible for Data Protection.

4 DATA PROTECTION

The Company collects and processes the personal data set out in the RCSN Data Protection Plan.

The Company only collects, processes, and holds personal data for the specific purposes set out in the RCSN Data Protection Plan (or for other purposes expressly permitted by the Data Protection Legislation).

The Company will only collect and process personal data for and tothe extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed).

Employees, agents, contractors, or other parties working on behalf of the Company may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy and the Company's Data Protection Policy. Excessive personal data must not be collected.

Employees, agents, contractors, or other parties working on behalf of the Company may process personal data only when the performance of their job duties requires it. Personal data held by the Company cannot be processed for any unrelated reasons.

The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject.

If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Policy.

For more details about the Company's approach to Data Protection and the obligations which apply to the Company and to all employees, agents, contractors, or other parties working on behalf of the Company, please refer to the Company's Data Protection Policy which includes sections on:

The data protection principles;

- The rights of data subjects;
- Consent;
- The accuracy of personal data and keeping personal data up-to-date;
- Personal data retention;
- Accountability and record-keeping;
- Data protection impact assessments;
- Privacy by design;
- Keeping data subjects informed about their personal data and our use of it;

Data subject access requests;

a) Rectification of personal data;
b) Erasure of personal data;
c) Restricting personal data processing;
d) Personal data portability;
e) Objections to personal data processing;
f) Automated personal data processing, decision-making, and profiling;
g) Marketing;
h) Details of the personal data collected, held, and processed by the Company;
i) Data security;
j) Organisational security;
k) Transferring personal data to countries located outside of the UK; and
l) Handling data breaches;

4.1 DIRECT MARKETING AND ELECTRONIC COMMUNICATIONS

The Company recognises that direct marketing activities are subject to the requirements of the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), the FCA Claims Management: Conduct of Business Sourcebook (CMCOB) and the Consumer Duty.

Prior to undertaking any marketing activity, the Company will determine the appropriate lawful basis for processing personal data and ensure that any electronic marketing complies with PECR.

Before any marketing communication is sent, the Company will ensure that:

- the recipient has provided valid consent where consent is required by law; or
- another lawful basis applies and the marketing activity is permitted under PECR;
- appropriate privacy information has been provided;
- the individual has not exercised their right to object to marketing;
- the individual has not withdrawn any consent previously given;
- telephone numbers are screened against the Telephone Preference Service (TPS) and Corporate Telephone Preference Service (CTPS) where applicable;
- appropriate records are retained demonstrating the lawful basis relied upon.

The Company will ensure that all marketing communications are clear, fair and not misleading and comply with the requirements of CMCOB.

4.1.1 MARKETING PROCEDURE

Prior to commencing any marketing campaign the Company will:

- identify the intended target market;
- determine the lawful basis for processing;
- review the communication to ensure compliance with CMCOB 3;
- ensure vulnerable customers are appropriately considered;

- ensure any claims management communication is clear, fair and not misleading;
- confirm that appropriate suppression lists have been checked;
- verify that recipients have not opted out of marketing;
- retain an audit trail of the campaign including the date, source of data, lawful basis and method of communication.

Marketing campaigns will be reviewed periodically to identify complaints, unsubscribe requests, customer feedback and any potential regulatory concerns.

Prior to approval of any marketing communication the Company will assess whether the communication:

a) is clear, fair and not misleading;

b) accurately describes the claims management services offered;

c) does not omit material information;

d) does not exaggerate likely compensation or outcomes;

e) does not create unrealistic expectations;

f) clearly identifies the Company;

g) does not exert undue pressure or exploit vulnerable consumers;

h) is appropriate for the intended target market.

No financial promotion or marketing communication may be published until it has been reviewed and approved by the Director or another suitably trained individual responsible for regulatory compliance. Records of approval will be retained.

Complaints relating to marketing, lead generation, consent or unsolicited communications will be analysed to identify trends and any remedial action required.

Marketing communications will be designed having regard to the needs of vulnerable consumers and will avoid exploiting characteristics of vulnerability including age, financial distress, bereavement, illness or limited financial capability.

Existing financial promotions will be reviewed at least annually, or sooner where there are changes to legislation, FCA rules, business processes, services offered, or where monitoring identifies that amendments may be required. Any promotion found to be inaccurate, misleading or out of date will be amended or withdrawn without undue delay.

The Company remains responsible for ensuring compliance with applicable FCA requirements where marketing or lead generation activities are undertaken by third parties acting on its behalf and will monitor those arrangements on an ongoing basis.

4.2 DATA SECURITY

The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are set out below in Part 6.

Data security must be maintained at all times by protecting the confidentiality, integrity, and availability of all personal data as follows:

a. only those with a genuine need to access and use personal data and who are authorised to do so may access and use it;

b. personal data must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed; and

c. authorised users must always be able to access the personal data as required for the authorised purpose or purposes.

4.3 DATA HANDLING/PROCESSING

All personal data must be handled in accordance with the requirements of the Data Protection Legislation, the Company's Data Protection Policy, and other related policies.

All emails containing personal data must be encrypted using TLS.

All emails containing personal data must be marked "confidential".

Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.

Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable.

Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. All temporary files associated therewith should be deleted.

Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data.

Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using DHL.

All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked “confidential”.

All electronic copies of personal data should be stored securely using passwords and HTTPS data encryption.

All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar.

All personal data stored electronically should be backed up in real time with backups stored offsite.

All backups should be encrypted HTTPS.

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Company’s Data Retention Policy.

No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise.

No personal data should be transferred to any computer or device personally belonging to an employee, agent, contractor, or other party working on behalf of the Company and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Data Protection Legislation (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

No personal data may be shared informally and if an employee, agent, contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from the Director responsible for Data Protection

No personal data may be shared with or transferred to any employee, agent, contractor, or other party, whether such parties are working on behalf of the Company or not, without the authorisation of the Director responsible for Data Protection only then if the sharing or transfer is secure, lawful, and fair. Personal data shared with third parties must be covered by a suitable written agreement to ensure compliance with the Data.

Where personal data is obtained from third parties rather than directly from the individual, the Company will ensure that the requirements of Articles 14 UK GDPR are met, including providing appropriate privacy information within the required timescales unless an exemption applies.

Any actual or suspected personal data breach must be reported immediately to the Company's Data Protection Lead. The Company will assess whether notification to the Information Commissioner's Office or affected individuals is required in accordance with UK GDPR.

4.3.1 SECURE HANDLING OF PERSONAL DATA

Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, contractors, or other parties at any time.

If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.

Where personal data is processed for marketing purposes, the the Director responsible for Data Protection will ensure that all marketing activities comply with UK GDPR, PECR and CMCOB.

Prior to sending any marketing communication the Company will verify:

- the lawful basis relied upon;
- whether consent has been obtained where required;
- whether the individual has previously objected to marketing;
- whether consent has been withdrawn;
- whether the recipient is registered with the TPS or CTPS where applicable;
- that the communication contains an appropriate method of opting out.

The Company maintains suppression lists to ensure individuals who have opted out are not contacted again for marketing purposes.

All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers.

Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords.

Under no circumstances should any passwords relating to Company systems and/or personal data be saved on any computer or device that is not Company-owned. This includes saving passwords in internet browsers and in third-party password manager applications.

Under no circumstances should any computer or device used for accessing or handling personal data be used without the correct security functions enabled including, as appropriate, passwords, PIN codes, biometric security (e.g. fingerprint), and any additional security software provided by the Company.

All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Company's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so.

All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the Data Protection Legislation and under all applicable Company policies, including (but not limited to) this Policy and the Data Protection Policy.

Only employees, agents, contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company.

All sharing of personal data shall comply with the information provided to the relevant data subjects and, if required, the consent of such data subjects shall be obtained prior to the sharing of their personal data.

All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so.

All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised.

All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise.

Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed.

All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy.

The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed.

All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Data Protection Legislation and this Policy by contract.

All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Data Protection Legislation.

Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

Individuals have the right to object to the processing of their personal data for direct marketing purposes at any time.

Where an objection is received:

- marketing activity will cease immediately;
- the individual's record will be updated;
- the individual will be added to the Company's suppression list;
- no further direct marketing communications will be issued unless a new lawful basis exists;
- a record of the objection will be retained for compliance purposes.

4.3.2 REQUESTS FOR ERASURE

Where an individual exercises their right to erasure, the Company will:

- acknowledge the request promptly;
- verify the identity of the requester;
- assess whether any legal or regulatory obligations require retention of the information;
- erase personal data where appropriate;
- notify any processors or third parties where required;

- confirm completion of the request to the individual.

Where information must be retained for legal or regulatory purposes, the individual will be informed of the reasons.

4.4 THIRD PARTY LEAD PROVIDERS

Prior to accepting personal data or referrals from any third-party lead provider, the Company will undertake appropriate due diligence.

This will include:

- verifying whether the lead provider requires FCA authorisation and, where applicable, confirming their permissions on the Financial Services Register;
- reviewing how personal data has been obtained;
- confirming compliance with UK GDPR, the Data Protection Act 2018 and PECR;
- reviewing the lead provider's privacy information and consent mechanisms;
- ensuring an appropriate data sharing agreement is in place where required.

The Company will maintain written due diligence records for each lead provider and review those arrangements periodically. The more frequently leads are received from a particular provider, the more frequently those arrangements will be reviewed to ensure continued compliance.

Where concerns arise regarding lead quality, customer complaints, consent validity or compliance with UK GDPR, PECR or FCA requirements, acceptance of leads from that provider will be suspended until those concerns have been investigated and resolved.

The Company will periodically review lead quality by monitoring conversion rates, customer complaints, evidence of valid consent, customer understanding of how their details were obtained, and any regulatory issues identified. Findings will be documented and, where appropriate, corrective action taken.

4.5 WEBSITE ENQUIRIES

Where personal data is collected through the Company's website:

- an appropriate privacy notice will be displayed;
- any marketing consent will be obtained using a clear affirmative action;
- consent for marketing will be separate from consent to submit an enquiry;
- website forms will clearly explain how personal data will be used;
- all information submitted through the website will be transmitted securely.

4.6 ACCOUNTABILITY AND RECORD-KEEPING

The Director responsible for Data Protection is responsible for administering this Policy and for developing and implementing all applicable related policies, procedures, and/or guidelines.

The Company shall follow a privacy by design approach at all times when collecting, holding, and processing personal data. Data Protection Impact Assessments shall be conducted if any processing presents a significant risk to the rights and freedoms of data subjects.

All employees, agents, contractors, or other parties working on behalf of the Company shall be given appropriate training in data protection and privacy, addressing the relevant aspects of the Data Protection Legislation, this Policy, the Company's Data Protection Policy, and all other applicable Company policies.

The Company's data protection compliance shall be regularly reviewed and evaluated by means of Data Protection Audits.

The Company shall keep written internal records of all personal data collection, holding, and processing.

4.7 MARKETING RECORDS

The Company will retain appropriate records demonstrating compliance with UK GDPR, PECR and CMCOB including:

- marketing consents;
- lawful basis assessments;
- objections;

- withdrawals of consent;
- deletion requests;
- suppression lists;
- marketing campaign records;
- lead provider due diligence records;
- marketing complaints.

5 IMPLEMENTATION OF POLICY

This Policy shall be deemed effective as of 11/06/2026. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.