Data Protection Policy

The principles and responsibilities we follow when handling personal data under the UK GDPR and the Data Protection Act 2018.

Document	Data Protection Policy
Organisation	NC Safety Solutions
Document owner	Nedim Custic, DipNEBOSH, CEO
Version	1.1
Effective date	12th September 2026
Next review	12th September 2027, or sooner if the law, our services or our organisation change
Revision history	1.0, 9th September 2026: first issue. 1.1, 12th September 2026: reissued under the NC Safety Solutions name, with the insurance statement updated.

1. Purpose and scope

This policy sets out how NC Safety Solutions handles personal data across the business, under the UK GDPR and the Data Protection Act 2018. It applies to all personal data we process, whether it relates to enquirers, clients, client staff, suppliers, associates or anyone else, and to everyone who works with or for us.

It sits alongside our Privacy Notice, which explains to individuals what we do with their data, and our GDPR Compliance Procedures, which set out how we act on this policy day to day.

2. Definitions

Term	Meaning
Personal data	Any information relating to an identified or identifiable living person, such as a name, email address, job title, photograph or accident record.
Special category data	Personal data revealing health, ethnic origin, religion, trade union membership, sexual orientation or similar. Health data appears in accident, occupational health and fitness-to-work records.
Processing	Anything done with personal data, including collecting, storing, reading, sharing and deleting it.
Controller	The organisation that decides why and how personal data is processed. We are a controller for our own enquiry, client and supplier data.
Processor	An organisation that processes personal data on a controller's instructions. In some engagements we act as a processor for a client's staff data.

3. The principles we follow

We process personal data in line with the seven UK GDPR principles:

- **Lawfulness, fairness and transparency.** We only process data where we have a lawful basis, and we tell people what we do with it.

- **Purpose limitation.** We collect data for clear reasons, such as answering enquiries and delivering engagements, and do not reuse it for something incompatible.
- **Data minimisation.** We collect only what we actually need.
- **Accuracy.** We keep records up to date and correct them when told they are wrong.
- **Storage limitation.** We keep data only as long as needed, then delete it securely.
- **Integrity and confidentiality.** We protect data with appropriate technical and organisational measures.
- **Accountability.** We can show how we meet these principles through this policy, our records of processing and our procedures.

4. Lawful bases

Before processing personal data we identify the lawful basis and record it in our record of processing. The bases we most commonly rely on are performance of a contract, compliance with a legal obligation (for example health and safety record-keeping and tax law), legitimate interests, and consent. Where we process special category data, such as health information in accident records, we also identify a condition under Article 9 UK GDPR, most often that processing is necessary for obligations under employment and health and safety law.

5. Client engagement data

Health and safety work often involves personal data belonging to our clients' staff, for example in accident records, training registers, competence records, occupational health referrals or audit findings. We:

- Treat that data as confidential and process it only as needed for the engagement.
- Act on the client's documented instructions where we are a processor, and enter into a written data processing agreement where the client requires one.
- Anonymise or pseudonymise data in reports wherever the purpose can be met without naming individuals.
- Return or securely delete the data when the engagement ends, unless we are required to keep it by law or professional obligation.

6. Security

- Data is stored with reputable providers offering encryption in transit and at rest.
- Access is limited to those who need it for their work, and accounts use strong passwords and multi-factor authentication where available.
- Devices used for our work are protected with authentication, encrypted where possible and kept updated.
- Personal data is not stored on removable media or sent through personal accounts.
- Paper records, where unavoidable, are stored securely and destroyed by shredding when no longer needed.
- Emails containing sensitive personal data are sent only to verified recipients, with attachments protected where appropriate.

7. Retention

Retention periods for each category of data are set out in our Privacy Notice and record of processing. When a period expires the data is deleted or anonymised. Where data must be kept for legal reasons it is restricted to that purpose only.

8. Individual rights

We respect the rights of individuals to access, rectify, erase, restrict, port and object to the processing of their data, and to withdraw consent. Requests are handled under our GDPR Compliance Procedures within one calendar month.

9. Sharing and suppliers

We share personal data only with suppliers under written contracts containing the processor obligations required by Article 28 UK GDPR, with specialist partners at the client's request, and with regulators, insurers or advisers where required. International transfers are made only with appropriate safeguards.

10. Breaches

Any actual or suspected personal data breach must be reported to the CEO immediately. Breaches are assessed, contained, recorded and, where required, reported to the Information Commissioner's Office within 72 hours and to affected individuals without undue delay, as described in our GDPR Compliance Procedures.

11. Training and awareness

Everyone who works with or for us is made aware of this policy and the procedures that support it when they join, and reminded whenever the policy changes.

12. Responsibilities and contact

Responsibility for data protection rests with Nedim Custic, CEO. Any questions, concerns or requests about personal data can be sent to **nedim@ncsafetysolutions.co.uk**.

13. Review

This policy is reviewed at least annually and whenever our processing, suppliers or the law change in a way that affects it.

Approved and issued by

Nedim Custic, DipNEBOSH - CEO
NC Safety Solutions
12th September 2026