



DATA PROTECTION & SECURITY POLICIES

OUR POLICIES | OUR COMMITMENT | A SAFER, STRONGER BUSINESS



VEHICLE
SERVICING



DIAGNOSTICS
& REPAIRS



TYRES &
EXHAUSTS



BRAKES



BATTERIES



AIR CONDITIONING



RM Auto Repairs Ltd
TA NRP Autocentre
Unit 4 Wallend Farm
Lower Road
Minster
ME12 3RR



Version: 1.0

Last updated: September 2026

Review date: September 2027

Keeping You on the Move

DATA PROTECTION & SECURITY POLICIES

RM Auto Repairs Ltd TA NRP Autocentre
Unit 4 Wallend Farm, Lower Road, Minster, ME12 3RR
01795 877966 | office@nrpautocentre.uk

Privacy, workplace monitoring, IT security and breach response

Purpose and application

This policy document provides a practical framework for RM Auto Repairs Ltd TA NRP Autocentre. Read it alongside relevant contracts, risk assessments, customer terms and privacy notices. It does not remove statutory rights; applicable law takes precedence.

Data Protection and Confidentiality

- Personal information may include customer contact details, vehicle registrations and repair history, bookings, payment records, complaints, employee and supplier records.
- Use personal data lawfully, fairly, securely and only for legitimate purposes. Share it only where there is a business or legal reason, and retain it only as long as necessary.
- Securely dispose of records when no longer needed, subject to legal and business retention requirements.

Employee Privacy, CCTV and Monitoring

- Provide an employee privacy notice explaining data held, purposes, lawful bases, recipients, retention and rights.
- Monitoring must have a defined purpose, lawful basis and be necessary and proportionate. Tell workers what is monitored and why. Restrict access and retain recordings only for a justified period.
- CCTV should not normally cover private areas. Audio recording is highly intrusive and should not be routine. Consider a Data Protection Impact Assessment where monitoring may create high risk.

IT and Cyber Security

- Use strong unique passwords, enable multi-factor authentication where available, lock devices when unattended and never share logins.
- Be cautious with unexpected links, attachments and requests to change supplier bank details. Do not install unauthorised software. Back up important data securely.
- Report phishing, malware, lost devices, compromised passwords and suspected unauthorised access immediately.

Data Breach Procedure

- Report suspected breaches immediately, including misdirected emails, lost paperwork/devices, unauthorised access or malware.
- Contain the incident, identify affected data and people, assess risks, record actions and decide whether ICO or individual notification is required.
- Where legally required, notify the ICO within 72 hours of becoming aware of a reportable personal data breach.

Physical Security and Records

- Keep paperwork, customer keys, devices and access credentials secure and restrict access to authorised staff.
- Use photographs or recordings only for stated legitimate purposes such as security, vehicle condition, repair evidence or dispute handling.

Document control

Version 1.0 | Issue date: October 2026 | Planned review: October 2027

Review this document when legislation, guidance, business operations or working practices change.