



DATA PROTECTION POLICY

Date: 14/08/2025

Version: 1.0

Approved by: James Moseley

Review date: 13/08/2026

0800 448 0450
info@vikingsecuritynwLtd.co.uk
www.vikingsecuritynwLtd.co.uk

1. Purpose

The purpose of this policy is to outline Viking Security NW Limited's commitment to protecting the privacy and security of personal data in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2. Scope

This policy applies to all employees, contractors, and third-party service providers of Viking Security NW Limited who have access to personal data. It covers all personal data processed by the company, regardless of format or medium.

3. Policy Statement

Viking Security NW Limited will process personal data lawfully, fairly, and transparently. Personal data will be collected only for specified, explicit, and legitimate purposes and will not be further processed in a manner incompatible with those purposes.

4. Data Protection Principles

We adhere to the following principles in accordance with the UK GDPR:

- Lawfulness, fairness, and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality.
- Accountability.

5. Responsibilities

- Management is responsible for ensuring compliance with this policy.
- The Data Protection Officer (DPO) oversees implementation and compliance.
- Employees must handle personal data in accordance with this policy and report any data breaches immediately.

6. Data Security Measures

- Use of secure systems and encryption for storing and transferring data.
- Regular password updates and multi-factor authentication.
- Access to personal data restricted to authorised personnel only.

- Regular data protection training for staff.

7. Data Subject Rights

We will uphold the rights of individuals under the UK GDPR, including:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision-making and profiling.

8. Breach Notification

Any data breach must be reported to the DPO immediately. Where required, breaches will be reported to the Information Commissioner's Office (ICO) within 72 hours and, where applicable, affected individuals will be informed.

9. Review

This policy will be reviewed annually or sooner if there are significant changes to data protection legislation.