Privacy & Data Protection Policy (UK GDPR Compliant)

Policy Statement

Ascent Fire is committed to protecting the privacy, confidentiality, and integrity of personal data. We process personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

We recognise that effective data protection is essential to maintaining trust, ensuring legal compliance, and supporting our business operations.

Scope

This policy applies to all personal data processed by Ascent Fire, including data relating to employees, customers, suppliers, contractors, and other third parties. It applies to all employees and individuals who process personal data on behalf of the organisation.

Key Principles

We adhere to the core data protection principles and ensure that personal data is:

- Processed lawfully, fairly, and transparently
- Collected for specified, legitimate purposes and not used incompatibly
- Adequate, relevant, and limited to what is necessary
- Accurate and kept up to date
- Retained only for as long as necessary
- Protected through appropriate security measures
- Processed in accordance with individuals' rights

Lawful Processing

Personal data will only be processed where there is a valid legal basis, including:

- Consent
- Performance of a contract
- Legal obligation
- Legitimate business interests
- Protection of vital interests

Where consent is relied upon, it will be freely given, specific, informed, and capable of being withdrawn.

Data Security

Ascent Fire implements appropriate technical and organisational measures to protect personal data from unauthorised access, loss, or misuse. These include:

- Access controls and data minimisation
- Secure storage and transfer methods
- Staff training and awareness
- Regular review of security controls

All employees are responsible for safeguarding personal data and must follow company procedures at all times.

Data Subject Rights

Individuals have rights in relation to their personal data, including:

- The right to access their data
- The right to rectification or erasure
- The right to restrict or object to processing
- The right to data portability (where applicable)
- The right to withdraw consent
- The right to lodge a complaint with the Information Commissioner's Office (ICO)

All requests must be handled promptly and in accordance with legal requirements.

Data Breaches

Any suspected or actual data breach must be reported immediately in line with company procedures. The organisation will investigate and, where required, notify the ICO and affected individuals.

Third Parties and Data Sharing

Personal data will only be shared with third parties where necessary and where appropriate safeguards are in place. All third-party processors must comply with data protection requirements and contractual obligations.

Transfers of personal data outside the UK will only take place where appropriate safeguards are in place.

Responsibilities

Management is responsible for ensuring compliance with this policy and providing adequate resources. All employees must:

- Handle personal data responsibly
- Follow data protection procedures
- Report any concerns or breaches

A designated data protection lead is responsible for overseeing compliance and providing guidance.

Training and Awareness

All employees will receive appropriate data protection training to ensure understanding of their responsibilities and legal obligations.

Monitoring and Review

This policy will be regularly reviewed to ensure ongoing compliance with legislation and best practice. Improvements will be made where necessary to strengthen data protection controls.

Signature: *Brian Pickering*
Position: Director
Date: 01/04/2026
Review Date: 31/03/2027