
DATA PROTECTION & PRIVACY POLICY

1. Policy Statement

H-K-L Specialists Limited (the 'Company') enforces an uncompromising commitment to the protection of personal privacy and corporate information integrity. The Company operates in strict compliance with the **Data Protection Act 2018** and the **UK General Data Protection Regulation (UK GDPR)**. This policy mandates secure data procedures across all administrative teams, engineering estimators, project management staff, contractors, and supply chain partners who access personal or project-sensitive data on our behalf.

2. Scope & Data Processing Principles

To ensure operational efficiency, the Company collects and handles essential data regarding members of the public, current, past, and prospective employees, clients, customers, sub-contractors, and material suppliers. Regardless of whether this data is stored on physical paper records, cloud servers, or on-site electronic devices, it must be handled in full accordance with the six core principles of Article 5 of the UK GDPR:

- 1) **Lawfulness, Fairness, and Transparency:** Processed lawfully, fairly, and transparently in relation to the data subject.
- 2) **Purpose Limitation:** Collected for explicit, specified, and legitimate commercial purposes and not further processed in an incompatible manner.
- 3) **Data Minimisation:** Adequate, relevant, and strictly limited to what is operationally necessary for fulfilment,
- 4) **Accuracy:** Maintained accurately and kept up to date; inaccurate data must be erased or rectified without delay.
- 5) **Storage Limitation:** Retained in an identifiable form for no longer than is necessary for the specified purposes.
- 6) **Integrity and Confidentiality:** Processed securely using appropriate technical and organisational measures to prevent unauthorised access, accidental loss, damage, or destruction.

3. Responsibilities & SKEB Integration

Data protection represents an active operational responsibility for all personnel working for or with the Company, including freelancers, sub-contractors, and remote workers. Line managers must monitor team compliance. The Company integrates data protection awareness directly into its **SKEB (Skills, Knowledge, Experience, and Behaviour)** evaluation matrix, ensuring that a professional, safety-conscious mindset dictates how site personnel handle sensitive information assets.

4. Project-Level Risk Controls (Subcontractor & Principal Contractor Formats)

A. Operating as a Specialist Subcontractor

The project team will handle all proprietary design calculations, client contact files, and main contractor site directories securely. No employee or installer may upload project layouts, site photographs showing third-party personnel, or commercial metrics to unapproved personal cloud accounts or unauthorized public social platforms.

B. Operating as a Principal Contractor (PC)

The site management team will protect the data privacy of all sub-contractors and site visitors. Access logs, induction questionnaires, CSCS card copies, and mandatory medical screening records collected at the site office must be locked in a secure filing cabinet or stored on an enterprise cloud platform with restricted user access controls.



5. Technical, Physical & Tracking Security Measures

A. Physical Media and Document Security

- **Storage:** Lock printed personal or project data in drawers or filing cabinets when not in use.
- **Clear Desk:** Never leave printouts unattended on public office printers or site desks.
- **Disposal:** Shred obsolete paper data, site manifests, and layout printouts using approved confidential waste channels.

B. Electronic & Cloud Infrastructure Controls

- **Access Control:** Secure all systems using unique credentials managed via approved enterprise password managers. Shared logins are strictly prohibited to preserve a clear audit trail.
- **Password Complexity:** Passwords must be a minimum of **12 characters**, containing a mix of uppercase, lowercase, numbers, and special symbols. Continuous rotation is not required unless a breach is suspected.
- **MFA Triggers:** Multi-Factor Authentication (MFA) is **mandatory** for all corporate email accounts, cloud infrastructure environments, remote VPN connections, and third-party vendor platforms.
- **Device Security:** Enforce full-disk encryption (minimum AES-256 standard) on all endpoints, laptops, and mobile devices. Never save sensitive corporate data to unauthorized personal devices or unencrypted removable media.
- **Network Protection:** Store data exclusively on designated corporate servers or approved cloud services. Execute all remote connections over secure firewalls and encrypted networks.
- **Hosting Assets:** Primary corporate servers are hosted in secure data centres managed by verified specialist partners, including [Greenfrog Computing](#).

C. Website Cookies and Tracking Assets

The Company uses website cookies and tracking tokens under three compliance pillars:

- **Essential Cookies:** Deployed automatically to enable basic portal functions, including navigation, secure communication, and order completion. Disabling these blocks core website features.
- **Analytics Cookies:** Track user habits, page views, and errors to passively evaluate and improve system performance.
- **Targeting Cookies:** Measure corporate marketing performance and deliver contextual information tailored to commercial user requirements.

6. Subject Access Requests (SAR)

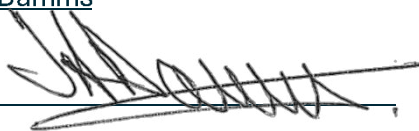
Individuals possess the statutory right to view, amend, export, or delete any personal data held by the Company. Data validation or deletion requests must be directed to the main administration team at hello@hklspecialists.co.uk.

Custody and accountability for the execution, maintenance, and annual review of these corporate policies remain vested in the Managing Director.

NAME: Terry Damms

POSITION: Managing Director

SIGNED: _____



DATED: 13/08/26

