Summit Timber Group Ltd :
Data Protection & Social Media Policy

1. Introduction

Summit Timber Group Ltd ("the Group") is committed to managing **personal data responsibly, securely, and transparently**, in line with the **UK General Data Protection Regulation (GDPR)** and the UK Data Protection Act 2018.
This policy applies to all personal data collected from employees, customers, clients, suppliers, and other third parties, and covers data obtained through:

- Sales and ordering systems
- CCTV recordings
- Transport and delivery records
- Employee and recruitment records
- Customer feedback and complaints
- Website analytics and cookies
- Telephone and email communications
- Information shared with third-party service providers

The objectives of this policy are to:

- Provide clear guidance on UK GDPR compliance;
- Outline employee responsibilities in handling personal data;
- Prevent unauthorised retention, disclosure, alteration, or destruction of personal data;
- Ensure transparency with data subjects regarding how their information is used.

---

2. Key Definitions

- **Data Controller:** The entity that determines how and why personal data is processed. Summit Timber Group Ltd is the Data Controller for all personal data it holds.
- **Data Subject:** Any individual whose personal data is held by a Group Company, including employees, contractors, clients, and customers.
- **Personal Data:** Any information relating to an identifiable living individual.
- **Sensitive Personal Data:** Personal information requiring extra protection, including racial or ethnic origin, political or religious beliefs, trade union membership, health, sexual orientation, criminal records, or court proceedings.
- **Data Processor:** Any external organisation processing data on behalf of the Company.
- **Data Protection Officer (DPO):** The person authorised to oversee compliance with data protection laws, authorise data processing, and respond to data subject requests.
- **Designated Person(s):** Individuals appointed to assist the DPO in managing personal data in accordance with regulations.

---

3. Data Protection Principles

All personal data must be:

1. Processed lawfully, fairly, and transparently;
2. Collected for specified, explicit, and legitimate purposes;
3. Adequate, relevant, and limited to what is necessary;
4. Accurate and kept up to date;
5. Retained only as long as necessary;
6. Processed in accordance with data subjects' rights;
7. Protected by appropriate technical (e.g., encryption, passwords) and organisational measures (e.g., restricted access, secure filing);
8. Not transferred outside the UK unless a legal basis exists;
9. Processed in a manner that is transparent to the data subject, including providing rights to access, correction, and erasure of personal data.

---

4. Handling Personal Data

- Personal data stored on company devices must be secured with encryption and password protection.
- Portable storage media (USB drives, DVDs, etc.) must be encrypted and securely handled.
- Personal data must not be transmitted via unsecured channels, and third-party transfers must use secure methods.
- Paper records must be stored securely, and a **clear desk policy** should be observed.
- Employees must not leave personal or sensitive data unattended on screens, desktops, or physical desks.
- Company IT systems should be used primarily for business purposes; personal use is permitted at the employee's risk and may be audited.

---

5. Purpose of Processing

Personal data will only be processed for legitimate and lawful purposes. Examples include:

For Employees:

- Recruitment and HR management;
- Payroll and benefits administration;
- Legal and regulatory compliance;
- Health and safety management;
- Fraud prevention and internal investigations.

For Customers/Clients:

- Processing orders and deliveries;
- Managing customer accounts and communications;
- Handling complaints, feedback, and service improvement;
- Preventing and detecting fraud.

Any additional processing purposes will be clearly communicated to the data subject.

6. Sensitive Personal Data

Sensitive personal data will generally only be processed with the **express consent** of the employee, except where required for:

- Health and safety;
- Legal obligations or proceedings;
- Administering justice;
- Monitoring equality and diversity compliance.

7. Data Subject Rights

Individuals whose personal data is held by a Company within the Summit Timber Group Ltd have the right to:

- Be informed whether their data is being processed and for what purposes;
- Access their personal data;
- Correct inaccuracies;
- Request erasure where applicable;
- Receive information about the sources of their data;
- Restrict processing or object to certain processing activities.

Requests must be submitted **in writing** (including email) to the relevant Group Company Data Protection Officer. The Company may charge a **maximum fee of £10** per request and will respond within **40 calendar days**.

Disclosure to third parties will only occur in line with legal obligations, such as:

- Preventing or detecting crime;
- Protecting the vital interests of individuals;
- Ensuring health and safety;
- Legal or regulatory requirements.

8. Social Media Use

Employees must use social media responsibly, both personally and professionally.

Employees must not:

- Disclose confidential information about colleagues, clients, suppliers, or the Company;
- Make defamatory, disparaging, or offensive statements about a Group Company, employees, or clients;
- Share business-sensitive information that could harm the Group's reputation;
- Represent the Group or a Group Company without express authorisation.

Employees must comply with **all confidentiality, equality, and data protection obligations** when posting online.

9. Security

- Employees must not attempt to access personal data without authorisation.
- Personal data must not be shared with unauthorised third parties.

- The Group reserves the right to **monitor IT systems and communications**, including social media and emails, to ensure compliance.

Breaches of data security may result in disciplinary action, including dismissal.

---

10. Penalties

Non-compliance with UK GDPR and data protection obligations can lead to:

- Regulatory enforcement actions by the Information Commissioner's Office;
- Legal orders to correct or erase data;
- Criminal offences for unauthorised use or disclosure;
- Fines up to £5,000 for the relevant Company or individuals.

---

11. Raising Concerns

Employees who suspect a breach of this policy must report it to their Company **Data Protection Officer** or a senior manager. All concerns will be treated **confidentially** and investigated promptly.

The Group Board of Directors has overall responsibility for this policy and its implementation.

---

12. Approval

Approved by the Board of Directors of Summit Timber Group Ltd