General & Technical
FLOORING SERVICES

Data Protection and Privacy Policy

1. Purpose and Commitment

This policy explains how the Company collects, uses, stores, and protects personal information relating to employees, workers, contractors, volunteers, and interns (collectively referred to as *staff members*).

The Company is committed to protecting the privacy, confidentiality, and security of personal data and ensuring it is processed lawfully and fairly in accordance with the UK General Data Protection Regulation (GDPR) and other applicable data protection laws.

---

2. Key Definitions

Personal Data
Any information that identifies, or could identify, a living person. Examples include a name, address, email, contact details, job title, or opinions about an individual.

Special Category (Sensitive) Data
Personal data that reveals a person's racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sexual orientation, or genetic/biometric data.

Processing
Any activity involving personal data, including collecting, recording, storing, using, sharing, altering, or deleting it.

---

3. Fair and Lawful Processing

The Company will process personal data in line with the following principles. Personal data will be:

- Used **lawfully, fairly, and transparently**.
- Collected for **specific, legitimate purposes** and not used in any way incompatible with those purposes.
- **Relevant and limited** to what is necessary.
- **Accurate and kept up to date.**
- Retained **only as long as necessary**.
- **Stored and handled securely.**

---

4. Lawful Basis for Processing

The Company will process personal data only where a lawful basis applies, including:

- To perform a contract (e.g. employment agreement).
- To comply with a legal obligation.
- For the Company's legitimate business interests, where these are not overridden by individual rights.

Less commonly, data may be processed to protect someone's vital interests or where required in the public interest.

---

5. Processing of Special Category Data

Sensitive personal data will only be processed when one of the following applies:

- The individual has given **explicit consent**.
- It is required by law (e.g. employment, health and safety, or equality monitoring).
- It is necessary for legal claims, safeguarding, or occupational health assessments.
- The data has been made public by the individual.

Examples include:

- Managing sickness or family-related leave.
- Monitoring workplace health, safety, or diversity.
- Administering pensions or benefits.

---

6. Criminal Conviction Data

Information about criminal convictions will only be processed where lawful and appropriate, such as for certain regulated roles. This may occur during recruitment or employment and will always be handled in line with legal obligations and with appropriate safeguards.

---

7. Consent

In most cases, the Company will rely on lawful bases other than consent.
Where consent is required (e.g. medical reports), full details will be provided so staff can make an informed choice. Consent can be withdrawn at any time by notifying the MD in writing.

---

8. Data Collection and Retention

Collection
Personal data is collected through recruitment, employment, and day-to-day work activities. Additional data may be collected from third parties (e.g. previous employers, background check providers) where necessary.

Retention
Data will only be kept for as long as necessary for legal, contractual, or business purposes. Once no longer required, data will be securely deleted or anonymised.

Retention periods are determined based on:

- Legal requirements.
- Business needs.
- The nature and sensitivity of the data.
- The potential risk of unauthorised use or disclosure.

---

9. Data Security and Sharing

Security
The Company uses appropriate technical and organisational measures to prevent unauthorised access, loss, or misuse of personal data. Access is limited to those who need it for legitimate business purposes and who are bound by confidentiality obligations.

Sharing
Data may be shared with:

- Third-party providers (e.g. payroll, pensions, benefits, IT support).
- Regulators, where required by law.
- Other parties in connection with business restructuring or sale.

All third parties are required to handle data securely and in compliance with data protection law.

---

10. Your Rights

Staff members have the following rights regarding their personal data:

- **Access** – request a copy of personal information held.
- **Correction** – request that inaccurate or incomplete data be updated.
- **Erasure** – request deletion where there is no lawful reason to retain it.
- **Restriction** – request that data processing be limited in certain circumstances.
- **Objection** – object to processing based on legitimate interests.
- **Data Portability** – request transfer of data to another organisation.

Requests should be made in writing to the HR Manager. The Company may ask for identification to confirm the requester's identity.

Normally, no fee is charged unless a request is excessive or unfounded.

---

11. Data Breaches

The Company has procedures in place to manage suspected data breaches.
Where legally required, affected individuals and regulators (such as the ICO) will be notified within 72 hours.

Any staff member who becomes aware of a data breach must report it **immediately** to the MD or Data Protection Contact.

---

12. Privacy by Design

New systems or processes that involve personal data will be developed in line with GDPR principles, ensuring privacy and security are built in from the start.

---

13. Responsibilities

Company Responsibilities
The Managing Director (MD) oversees compliance with this policy and data protection legislation.

Staff Responsibilities
All staff must:

- Handle personal data securely and in line with this policy.
- Not disclose personal data unless authorised.
- Keep passwords and devices secure.
- Report data breaches or concerns immediately.
- Maintain a "clear desk" policy and protect documents containing personal data.
- Only use Company-approved and encrypted devices for work purposes.

Unauthorised disclosure or misuse of personal data may be treated as **gross misconduct** and could result in disciplinary action, up to and including dismissal.

---

14. Further Information

If you have questions or concerns about how your data is handled, contact the Managing Director.

Document Control

Policy Owner: Managing Director
Applies To: All staff, workers, contractors, volunteers, and interns

SIGNED

J.MORRISON (MD) 01/10/2025

DATE	REVISION	DETAIL	PREPARED BY	APPROVED BY
July 2020	A	New background	John Morrison	John Morrison
November 2021	B	Review – No Change	John Morrison	John Morrison
November 2022	B	Annual Review	John Dunn	John Morrison
October 2025	C	Review	John Morrison	