



Qubit

# DATA PROTECTION & PRIVACY POLICY

QUBIT INTERIOR SOLUTIONS LIMITED  
PIER HOUSE, THAMES ROAD, DARTFORD, DA1 4SL



# DATA PROTECTION & PRIVACY POLICY

Company: Qubit Interior Solutions Limited (Qubit Group)

Location: Pier House, Thames Road, Crayford, DA1 4SL

Prepared By: Kyle McGimpsey

Position: Managing Director

Date Issued: 18/05/2026

Document Number: QUBI0004

Revision: 1

---

## 1. Introduction

Qubit Interior Solutions Ltd is committed to protecting the privacy, confidentiality, and security of personal data in line with the UK GDPR and Data Protection Act 2018. We handle personal data responsibly and transparently, ensuring it is processed lawfully, fairly, and securely.

This policy explains how we collect, use, store, and protect personal data of employees, contractors, clients, suppliers, job applicants, visitors, and other stakeholders.

We aim to:

- Comply with all applicable data protection laws.
- Protect the rights and freedoms of individuals.
- Maintain technical and organisational safeguards against unauthorised access or loss.
- Promote awareness and accountability for data protection across the company.

All employees, contractors, and third parties must comply with this policy. Non-compliance may result in disciplinary or legal action.

---

## 2. Scope

This policy applies the UK GDPR and the Data Protection Act 2018. References to previous legislation are not applicable.

This policy applies to:

All employees, contractors, and third-party partners of Qubit Interior Solutions Ltd. All personal data processed by the company, whether in electronic or paper format.

Data relating to clients, suppliers, employees, job applicants, and any other individuals whose data we hold.

---

### 3. Data Protection Principles

In line with the UK GDPR and the Data Protection Act 2018, we adhere to the following data protection principles when processing personal data:

- Lawfulness, fairness, and transparency – We process data fairly, legally, and in a transparent manner.
  - Purpose limitation – We only collect data for specified, legitimate purposes.
  - Data minimisation – We collect only data necessary for its intended purpose.
  - Accuracy – We ensure data is accurate and up-to-date.
  - Storage limitation – Data is kept only as long as necessary for its purpose.
  - Integrity and confidentiality – Data is protected against unauthorised or unlawful processing, accidental loss, or destruction.
- 

### 4. Types of Personal Data Collected

Qubit Interior Solutions Ltd may collect and process personal data necessary for business and legal purposes, including:

- Employees & Contractors: Name, contact details, payroll information, emergency contacts, right to work checks, performance records, training, absence, and health & safety information.
- Clients & Suppliers: Contact and company details, financial and contractual information, communication records, and project/transaction data.
- Job Applicants: Name, contact details, CV/resume, references, interview notes, qualifications, and eligibility checks.
- Visitors: Name, contact details, access logs, CCTV, and purpose/duration of visits.
- Other Data: IT system usage, marketing preferences (with consent), and any data required for legal or compliance purposes.

CCTV and monitoring: we may use CCTV and/or building access systems for security, health and safety, and the prevention and detection of crime. We may also monitor the use of company IT systems to protect our network, investigate suspected misconduct, and ensure compliance with company policies. Processing is carried out on the basis of legitimate interests and/or legal obligations where applicable. Clear notices/signage will be provided. Access to CCTV footage and monitoring records will be restricted to authorised personnel only and retained for a defined period in line with our retention schedule, unless required for an investigation or legal claim.



All personal data is collected only as necessary, stored securely, and handled in accordance with applicable data protection laws and our retention policy.

---

## 5. Legal Basis for Processing

We only process personal data where we have a lawful basis under the UK GDPR. This will usually be one or more of the following: performance of a contract; legal obligation; legitimate interests; vital interests; public task; or consent (used only where it is freely given and can be withdrawn without detriment).

In an employment context, we will rarely rely on consent due to the imbalance of power between employer and employee.

Where we process special category data (such as health information) we will also identify a separate UK GDPR Article 9 condition (for example: employment law obligations; occupational health; establishment, exercise or defence of legal claims; or explicit consent where appropriate). Where we process criminal offence data (including DBS information), we will only do so in accordance with the Data Protection Act 2018 and an applicable condition under Schedule 1, with appropriate safeguards in place.

---

## 6. How We Use Personal Data

Personal data may be used for purposes including but not limited to:

- Recruitment, HR management, and payroll processing.
- Supplier and client relationship management.
- Compliance with legal and regulatory obligations.
- Security and safety of our premises and personnel.
- Marketing and communications (where consent is obtained).

We ensure that all personal data is processed only for lawful, necessary, and proportionate purposes. Data is not used for unrelated activities or sold to third parties.

---

## 7. Data Sharing

We may share personal data with:

- Third-party service providers (e.g., payroll providers, IT services).
- Regulatory authorities where required by law.
- Professional advisors (e.g., legal, financial consultants).
- International transfers: where personal data is transferred outside the UK, we will ensure appropriate safeguards are in place in line with UK GDPR (for example, an adequacy decision where applicable, or the UK International Data Transfer Agreement



(IDTA) / UK Addendum to the EU SCCs, plus any additional risk assessments required). We will only use suppliers who can demonstrate suitable security and compliance standards.

We never sell personal data to third parties.

---

## 8. Data Retention

Personal data will be retained only for as long as necessary:

- Employee and payroll records: Up to 6 years post-employment.
- Supplier and client records: Up to 6 years after the end of the contract.
- Recruitment records: Up to 12 months after the application process ends.

We retain personal data in line with our Retention Schedule, which sets out retention periods by record type (including HR, payroll, recruitment, H&S, CCTV/access logs and IT records). Where a specific statutory or regulatory requirement applies, we will retain records for that period. At the end of the retention period, data will be securely deleted, destroyed, or anonymised.

---

## 9. Data Security

Qubit Interior Solutions Ltd implements technical and organisational measures to protect personal data, including:

- **Secure Storage:** Personal data is stored securely in locked cabinets or protected digital systems, with regular backups.
- **Access Control:** Data access is limited to authorised personnel on a need-to-know basis, with permissions regularly reviewed.
- **Staff Training:** Employees receive regular training on data protection, security protocols, and breach reporting.
- **Technical Measures:** Sensitive digital data is encrypted, systems are protected by firewalls and antivirus software, and strong password policies are enforced.
- **Monitoring & Review:** Security controls are regularly tested and updated to address risks and comply with legal requirements.
- **Supplier/processor controls** - where we use third-party processors to handle personal data on our behalf, we carry out appropriate due diligence and put in place written contracts that meet UK GDPR requirements. These contracts require processors to keep data secure and confidential, only process it on our documented instructions, assist us with individual rights requests and breach management, and delete/return data at the end of the service.



These measures ensure personal data is handled securely in line with UK GDPR and the Data Protection Act 2018.

---

## 10. Individual Rights

Under UK GDPR in line with Data Protection Act 2018, individuals have the following rights regarding their personal data:

- Right of Access – To request a copy of the personal data we hold about them (Subject Access Request).
- The right to be informed (via our privacy notices)
- Right to Rectification – To request correction of inaccurate or incomplete data.
- Right to Erasure – To request deletion of personal data where there is no lawful reason for us to retain it.
- Right to Restrict Processing – To request that we limit how their data is used in certain circumstances.
- Right to Object – To object to processing based on legitimate interests.
- Right to Data Portability (in limited circumstances) – To receive their data in a structured, commonly used format where processing is based on consent or contract.
- Right to Withdraw Consent – To withdraw consent at any time where processing is based on consent.
- Rights in relation to automated decision-making and profiling.
- Right to Complain – To lodge a complaint with the Information Commissioner’s Office (ICO).

Requests should be submitted to Managing Director / HR via Email. We may ask for proof of identity. We will respond within one month of receipt. Where requests are complex or numerous, we may extend this by up to a further two months and will explain why. We may refuse requests where an exemption applies, but we will explain the reason and inform individuals of their right to complain to the ICO.

---

## 11. Breach Reporting



Qubit Interior Solutions Ltd takes all personal data breaches seriously. A personal data breach includes any loss, unauthorised access, disclosure, alteration, or destruction of personal data.

In the event of a suspected or actual breach:

- Immediate Reporting – Employees and contractors must report the breach immediately to the HR contact.
- Investigation & Containment – The Company will assess the breach, take steps to contain it, and reduce any potential risk.
- Regulatory Notification – Where required, the breach will be reported to the
- Information Commissioner’s Office (ICO) within 72 hours.
- Notification to Individuals – Affected individuals will be informed where there is a high risk to their rights and freedoms.

All suspected or actual personal data breaches must be reported immediately to Managing Director and, if unavailable, to HR. Individuals must take immediate steps to contain the breach where safe to do so (e.g. recall emails, isolate devices, secure documents) and preserve evidence.

The Company will record all breaches (including near misses) in an internal breach register and will assess whether notification to the ICO is required within 72 hours and whether affected individuals must be informed.

---

## 12. Responsibilities

**Managing Director / Senior Management:** Ensure compliance with data protection laws and this policy, support staff training, and oversee corrective actions.

**Employees and Contractors:** Follow the policy, handle personal data securely, and report any suspected or actual breaches promptly.

**HR:** Advise on compliance, manage data requests, liaise with regulators, and monitor company-wide data protection practices.

Overall responsibility for data protection compliance sits with Managing Director. Day-to-day queries, rights requests and breach reports should be directed to HR. Where required, we will take advice from external specialists. Everyone is expected to cooperate to protect personal data and uphold legal and ethical obligations.

---

### 13. Policy Review

This policy will be reviewed annually or sooner if there are changes in legislation or business operations. Updates will be communicated to all employees.

**Reviewed / Approved By:**

Name: Kyle McGimpsey

Position: Managing Director

Signature:



Date: 18/05/2026