

GDPR Data Protection Policy



ALLAN PEACOCK
STREET LIGHTING

Introduction

At Allan Peacock (Street Lighting) Ltd, we take the privacy and security of personal information seriously.

We may collect, record, and use personal data about people with whom we work — whether on paper, electronically, or by other means.

We are committed to handling this information lawfully, fairly, and transparently, in line with the General Data Protection Regulation (GDPR).

This policy outlines how we process personal data and applies to all job applicants, employees, former employees, customers, suppliers, and contractors.

Definitions

- **Personal Data:** Information that identifies an individual, either directly or indirectly (e.g., name, ID number, location, online identifier).
- **Special Categories of Data:** Information relating to health, race, religion, political opinions, sex life, sexual orientation, trade union membership, and biometric data.
- **Criminal Offence Data:** Information related to criminal convictions or offences.
- **Data Processing:** Any action performed on personal data, including collection, storage, retrieval, use, disclosure, erasure, or destruction.

Data Protection Principles

We fully comply with GDPR by ensuring that personal data:

- Is processed fairly, lawfully, and transparently.
- Is collected for specific, explicit, and legitimate purposes.
- Is adequate, relevant, and limited to what is necessary.
- Is accurate and kept up to date.
- Is kept no longer than necessary.
- Is processed securely to prevent unauthorised access, loss, or damage.

Types of Data Held

We hold various categories of personal data, including:

- Personal details (name, address, phone numbers)
- Recruitment information (CVs, references, employment history)
- Pay administration details (NI numbers, bank details, tax codes)
- Health or medical information
- Employment information (job title, salary, contracts, disciplinary records, training)

Data is stored securely in personnel files and computer systems such as payroll and timesheet systems.

Employee Rights

Individuals have the following rights regarding their personal data:

- To be informed about how their data is used.
- To access their data (via a Subject Access Request).
- To have inaccurate data corrected.
- To have data erased where applicable.
- To restrict or object to data processing.
- To request data portability.
- To object to automated decision-making or profiling.

Responsibilities

All employees who process data are trained to do so responsibly.

We have appointed Directors to oversee data protection compliance and regularly audit our systems.

Lawful Basis for Processing

We ensure that a lawful basis exists for every data processing activity.

Where no other basis applies, we seek explicit and informed consent.

Access to Data

Employees can request access to their personal data at any time.

We respond to Subject Access Requests within one month, free of charge (unless the request is excessive).

Data Disclosures

We may need to disclose personal data:

- For employee benefits operated by third parties
- To support disabled employees
- For health and safety obligations
- For statutory reporting (e.g., tax, sick pay)
- To assist law enforcement or regulatory authorities

Such disclosures are made only when strictly necessary.

Data Security

- Personal information is kept in locked storage.

- Access to data is restricted to authorised personnel only.
- Password protection is enforced on all IT systems.
- Use of laptops, USB sticks, or portable devices is restricted and must be encrypted.

Third-Party Processing

Where third parties process data on our behalf, we ensure that robust agreements are in place to protect personal data.

International Data Transfers

We do not transfer personal data outside of the European Economic Area (EEA).

Data Breaches

All data breaches are recorded in our Data Breach Register.

Where required, breaches will be reported to the Information Commissioner's Office (ICO) within 72 hours and affected individuals will be informed.

Training

All employees receive training on data protection during induction and ongoing refresher sessions.

Training covers confidentiality, data security, breach identification, and the consequences of non-compliance.

Record-Keeping

We maintain records of all data processing activities, including purposes and retention periods.