INSERT LOGO

DATA PROTECTION POLICY

Classification: **Public**

This document may be shared with interested parties outside of [Company Name]

Version	Approved By	Owner	Date Last Updated	Review Frequency	Next Review	Comments

Contents

Purpose of This Document

This policy outlines how the [Company Name] will;

- Protect, process and store any personal data it handles on behalf of employees, signatories or customers.

- Comply with Data Protection legislation, including, but not limited to, the UK's Data Protection Act and the UK and EU General Data Protection Regulations and use these as a benchmark of personal data protection guidance for data globally.

Definitions & Scope

Personal data is defined as any information relating to an identified or identifiable natural living person and may include;

- names of individuals
- postal addresses
- email addresses
- telephone numbers
- photos
- any other information relating to individuals

DPA or GDPR does not cover anonymised data if the data cannot be reverse-engineered to identify the subject.

Some information is highly sensitive and should be afforded greater protection, including;

- Race or ethnic origin
- Political opinions;
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric ID data
- Health data
- Sexual life or sexual orientation
- Criminal data (convictions and offences)

Within the policy, the term "Responsible Person" means the person within the organisation who owns the business process and processes the data.

Data Protection Principles

Personal Data must be;

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer

periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR to safeguard the rights and freedoms of individuals; and

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures."

General Provisions

a. This policy applies to all personal data the [Company Name] processes, including staff, consultants, signatories, and others.
b. The data owners within the [Company Name] shall be responsible for ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.
d. The [Company Name] shall register with the Information Commissioner's Office as an organisation that processes personal data.
e. The [Company Name] shall check annually on identifying and appointing a Data Protection Officer.

Lawful, Fair & Transparent Processing

a. To ensure its data processing is lawful, fair and transparent, the [Company Name] shall maintain a Register of Systems processing personal data.
b. The Register of Systems shall be reviewed at least annually.
c. Individuals have the right to access their data, and any requests to the [Company Name] shall be handled promptly.

Lawful Purpose

a. All data processed by the [Company Name] must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).
b. The [Company Name] shall record the lawful basis, if necessary.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available, and systems should be in place to ensure such revocation is reflected accurately in the [Company Name] 's systems.

Data Minimisation

a. The [Company Name] shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

a. The [Company Name] shall take reasonable steps to ensure accurate personal data.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

Archiving & Removal

a. To ensure that personal data is kept for no longer than necessary, the [Company Name] shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
b. The archiving policy shall consider what data should/must be retained, for how long, and why.

Security

a. The [Company Name] shall ensure that personal data is stored securely using modern, up-to-date software.
b. Access to personal data shall be limited to personnel who need access, and appropriate security should be in place to avoid unauthorised information sharing.
c. When personal data is deleted, this should be done safely so that the data is irrecoverable.
d. Appropriate backup and disaster recovery solutions shall be in place.

Breaches of Personal Data

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the [Company Name] shall promptly;

1. Report the breach to the IT Helpdesk team as quickly as possible so that they may support controlling the data breach.
2. Report the breach to their line manager, who will assist with the impact assessment and oversight.
3. Report the breach to the Director of People Operations (or Chief People & Culture Officer if they are unavailable) in the [Company Name] People Team for any breaches of staff data.
4. Assess the risk to people's rights and freedoms and, if appropriate, report this breach to the ICO (more information on the ICO website). Do not report the breach to the ICO without a Line Manager's approval and assessment.