[Company]

DATA PROTECTION POLICY

GDPR and Data Protection Act 2018 Requirements

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	[DATE]		Document first created

2 Document Contents Page

4 Data Protection Policy

4.1 Purpose

The purpose of this policy is the company legal and regulatory requirements under the GDPR and the Data Protection Act 2018 and the rights of data subjects.

4.2 Scope

All employees and third-party users.

Personal Data as defined by GDPR.

4.3 Principle

Personal data is classified and treated as classification level Confidential, and all associated policies, controls and processes apply.

4.4 Data Protection Policy Statement

The company is classed as a Data Controller/Data Processor based on the context of the processes under the current UK Data Protection Act 2018. This policy confirms our commitment to protect the privacy of the personal information of our customers, clients, employees, and other interested parties. We have engaged in a programme of Information Security Management which is aligned to the international standard ISO27001 to ensure that the processes of personal information is conducted using best practice processes.

5 Legal Basis for Processing

Article 6 of the GDPR provides the legal basis under which Personal Data can be processed. Our legal basis for processing is documented in our **Record of Processing Activities**.

6 Data protection principles

The company is committed to processing data in accordance with its responsibilities under the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

Article 5 of the GDPR requires that personal data shall be:

6.1 Lawfulness, Fairness and Transparency

- processed lawfully, fairly and in a transparent manner in relation to individuals

We have reviewed and documented the data that we control and or process and determined the legal basis for processing. We provide privacy notices and inform data subjects of their rights as well as what processing takes place, by whom, for how long and why.

6.2 Purpose Limitation

- 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 incompatible with the initial purposes

We ensure we only process data for the purposes it has been collected and communicated and not for other reasons without the agreement and knowledge of the Data Subject(s).

6.3 Data Minimisation

- adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed

We ensure that data collected is not excessive and is appropriate to the purpose for which it was collected. We conduct Data Privacy Impact Assessments as part of our project lifecycle.

6.4 Accuracy

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay

  We ensure that data is reviewed and assessed for accuracy on a periodic basis and have implemented processes for the rectification and erasure of data without undue delay.

6.5 Storage Period Limitation

- 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 in order to safeguard the rights and freedoms of individuals

  We have implemented a data retention policy and data retention schedule in line with legal, regulatory and company needs.

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against

accidental loss, destruction, or damage, using appropriate technical or organisational measures.

We have implemented an information security management system in line with ISO 27001 the International Standard for Information Security. We have a culture of information security and assess security controls and requirements throughout the project life cycle.

7 Personal Information Classification and Handling

Personal data classification and handling is in line with the Information Classification and Handling Policy.

8 Personal Information Retention

Personal data is retained and destroyed in line with the Information Classification and Handling Policy, Asset Management Policy, and the Data Retention Schedule.

9 Personal Information Transfer / Transmit

Personal data is transferred in line with the Information Transfer Policy and employees ensure the appropriate level of security in line with the policy and company processes.

10 Personal Information Storage

Personal Information storage is in line with the Information Classification and Handling Policy, Physical and Environmental Security Policy, Cryptographic Control and Encryption Policy, Backup Policy, and the Data Retention Schedule.

11 Breach

In the event of a breach of the principles of the Data Protection Act 2018 employees inform their line manager, and /or a member of the Management Review Team and/or Senior Management and invoke the Incident Management Process.

Breaches are assessed and where appropriate and required the Data Subjects and / or the Information Commissioners Office are informed without undue delay.

12 The Rights of Data Subjects

12.1 The right to be informed

Individuals have the right to be informed about how we use their Personal Data.

This includes:

- The name and contact details of our organisation.
- The name and contact details of our representative (if applicable).
- The contact details of our data protection officer (if applicable).
- The purposes of the processing.

- The lawful basis for the processing.

12.2 The right of access

- Individuals have the right to access their personal data.
- This is commonly referred to as subject access.
- Individuals can make a subject access request verbally or in writing.
- We have one month to respond to a request.
- We cannot charge a fee to deal with a request in most circumstances.

12.3 The right to rectification

- The GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete.
- An individual can make a request for rectification verbally or in writing.
- We have one calendar month to respond to a request.
- In certain circumstances we can refuse a request for rectification.

12.4 The right to erasure (the right to be forgotten)

- The GDPR introduces a right for individuals to have personal data erased.
- The right to erasure is also known as ‘the right to be forgotten’.
- Individuals can make a request for erasure verbally or in writing.
- We have one month to respond to a request.
- The right is not absolute and only applies in certain circumstances.

- This right is not the only way in which the GDPR places an obligation on us to consider whether to delete personal data.

12.5 The right to restrict processing

- Individuals have the right to request the restriction or suppression of their personal data.
- This is not an absolute right and only applies in certain circumstances.
- When processing is restricted, we are permitted to store the personal data, but not use it.
- An individual can make a request for restriction verbally or in writing.
- We have one calendar month to respond to a request.

12.6 The right to data Portability

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- Doing this enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits.
- The right only applies to information an individual has provided to a controller.

12.7 The right to object

- The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.
- Individuals have an absolute right to stop their data being used for direct marketing.
- In other cases where the right to object applies, we may be able to continue processing if we can show that we have a compelling reason for doing so.
- We must tell individuals about their right to object.
- An individual can make an objection verbally or in writing.

12.8 Rights in relation to automated decision making and profiling

Individuals have the right not to be subject to a decision when:

- It is based on automated processing, and
- It produces a legal effect or a similarly significant effect on them.

13 Definitions

To ensure the company understands its obligations to the protection of Personal Information, the following definitions apply and are based on current understanding of these terms within UK and European law, and specifically in Article 4 of GDPR.

13.1 Personal Data

Any information relating to an identified or identifiable natural person ("Data Subject") who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

13.2 Sensitive Personal Data

Personal Data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Sensitive Personal Data includes Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

13.3 Data Controller

The natural or legal person, public authority, agency, or any other body, which alone or jointly with others, determines the purposes and means of the processing of Personal Data.

13.4 Data Processor

A natural or legal person, public authority, agency, or any other body which processes Personal Data on behalf of a Data Controller.

13.5 Processing

An operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of the data.

13.6 Anonymization

Irreversibly de-identifying Personal Data such that the person cannot be identified by using reasonable time, cost, and technology either by the controller or by any other person to identify that individual. The Personal Data processing principles do not apply to anonymized data as it is no longer Personal Data.

14 Policy Compliance

14.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

14.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

14.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

14.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.