Data Handling Policy

1. Introduction

This Policy is a supporting document to the Data Protection Policy of Hidden Figures Planning Ltd, a company registered in England under number 14839627 whose registered office is at Beck Mill, Skye Road, Clayton, Bradford BD14 8QY ("the Company") regarding data protection and the rights of clients and business connections.

This Policy sets out rules and guidance for all employees, agents, contractors, or other parties working on behalf of the Company regarding the handling of personal data.

2. Definitions

"consent"	means the consent of the data subject which must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they (by a statement or by a clear affirmative action) signify their agreement to the processing of personal data relating to them;
"Data Protection Legislation"	means all applicable legislation in force from time to time in the United Kingdom applicable to data protection and privacy including, but not limited to, the UK GDPR, the Data Protection Act 2018 (and regulations made thereunder), and the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation;
"data subject"	means a living, identified, or identifiable individual about whom the Company holds personal data;
"personal data"	means any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, 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 data subject. Unless otherwise stated, references in this Policy to "personal data" shall also include special category personal data;
"personal data breach"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or

	access to, personal data transmitted, stored, or otherwise processed;
"processing"	means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"special category personal data"	means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, biometric, or genetic data.

3. Data Protection Officer & Scope of Policy

3.1 The Company's Data Protection Officer is Helen Little, The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

3.2 All are responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of the Company comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.

3.3 Any questions relating to this Policy, the Company's collection, processing, or holding of personal data, or to the Data Protection Legislation should be referred to the Data Protection Officer.

4. Data Protection

4.1 The Company collects and processes the personal data received via contact forms or emails from clients and business relations.

4.2 The Company only collects, processes, and holds personal data for the specific purposes set out in our Data Protection Policy (or for other purposes expressly permitted by the Data Protection Legislation).

4.3 The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed).

4.4 Employees, agents, contractors, or other parties working on behalf of the Company may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy and the Company's Data Protection Policy. Excessive personal data must not be collected.

4.5 Employees, agents, contractors, or other parties working on behalf of the Company may process personal data only when the performance of their job duties requires it. Personal data held by the Company cannot be processed for any unrelated reasons.

4.6 The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject.

4.7 If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

4.8 The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

4.9 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

4.10 For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Policy.

4.11 For more details about the Company's approach to Data Protection and the obligations which apply to the Company and to all employees, agents, contractors, or other parties working on behalf of the Company, please refer to the Company's Data Protection Policy which includes sections on:

a) The data protection principles;

b) The rights of data subjects;

c) Consent;

d) The accuracy of personal data and keeping personal data up-to-date;

e) Personal data retention;

f) Accountability and record-keeping;

g) Data protection impact assessments;

h) Privacy by design;

i) Keeping data subjects informed about their personal data and our use of it;

j) Data subject access requests;

k) Rectification of personal data;

l) Erasure of personal data;

m) Restricting personal data processing;

n) **[**Personal data portability;**]**

o) Objections to personal data processing;

p) **[**Automated personal data processing, decision-making, and profiling;**]**

q) **[**Marketing;**]**

r) Details of the personal data collected, held, and processed by the Company;

s) Data security;

t) Organisational security;

u) Transferring personal data to countries located outside of the UK; and

v) Handling data breaches;

5. Data Security

5.1 The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are set out below in Part 6.

5.2 Data security must be maintained at all times by protecting the confidentiality, integrity, and availability of all personal data as follows:

a) only those with a genuine need to access and use personal data and who are authorised to do so may access and use it;

b) personal data must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed; and

c) authorised users must always be able to access the personal data as required for the authorised purpose or purposes.

6. Data Handling

6.1 All personal data must be handled in accordance with the requirements of the Data Protection Legislation, the Company's Data Protection Policy, and other related policies.

6.2 It is preferable that personal data be submitted via our secure online forms, but should email be used, it must be encrypted or sent at the individual's risk.

6.3 All emails containing personal data must be marked "confidential".

6.4 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.

6.5 Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable.

6.6 Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted permanently.

6.7 Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data.

6.8 Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Royal Mail registered delivery service.

6.9 All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential".

6.10 All electronic copies of personal data should be stored securely on a secure server using passwords and data encryption.

6.11 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar.

6.12 All personal data stored electronically should be backed up daily with backups stored onsite **and** offsite.

6.13 When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Company's Data Retention Policy.

6.14 No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company.

6.15 No personal data should be transferred to any computer or device personally belonging to an employee, agent, contractor, or other party working on behalf of the Company and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Data Protection Legislation (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

6.16 No personal data may be shared informally and if an employee, agent, contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from the Director.

6.17 No personal data may be shared with or transferred to any employee, agent, contractor, or other party, whether such parties are working on behalf of the Company or not, without the authorisation of the individual and only then if the sharing or transfer is secure, lawful, and fair. Personal data shared with third parties must be covered by a suitable written agreement to ensure compliance with the Data Protection Legislation.

6.18 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, contractors, or other parties at any time.

6.19 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.

6.20 Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Director to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

6.21 All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by the Company is designed to require such passwords.

6.22 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords.

6.23 Under no circumstances should any passwords relating to Company systems and/or personal data be saved on any computer or device. This includes saving passwords in internet browsers and in third-party password manager applications.

6.24 Under no circumstances should any computer or device used for accessing or handling personal data be used without the correct security functions enabled including, as appropriate, passwords, PIN codes, biometric security (e.g. fingerprint), and any additional security software provided by the Company.

6.25 All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Company's IT service provider shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible**,** unless there are valid technical reasons not to do so**.**

6.26 No software may be installed on any Company-owned computer or device without the prior approval of the Director.

6.27 If any computer or device used to access or store personal data, whether personal or Company-owned, is lost or stolen, the loss or theft must be reported to the Director as soon as possible, and all assistance required provided with any investigation.

6.28 All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the Data Protection Legislation and under all applicable Company policies, including (but not limited to) this Policy and the Data Protection Policy.

6.29 Only employees, agents, contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company.

6.30 All sharing of personal data shall comply with the information provided to the relevant data subjects and, if required, the consent of such data subjects shall be obtained prior to the sharing of their personal data.

6.31 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so.

6.32 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised.

6.33 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise.

6.34 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed.

6.35 All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy.

6.36 The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed.

6.37 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Data Protection Legislation and this Policy by contract.

6.38 All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same

conditions as those relevant employees of the Company arising out of this Policy and the Data Protection Legislation.

6.39 Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

7. Accountability and Record-Keeping

7.1 The Data Protection Officer is responsible for administering this Policy and for developing and implementing all applicable related policies, procedures, and/or guidelines.

7.2 The Company shall follow a privacy by design approach at all times when collecting, holding, and processing personal data. Data Protection Impact Assessments shall be conducted if any processing presents a significant risk to the rights and freedoms of data subjects.

7.3 All employees, agents, contractors, or other parties working on behalf of the Company shall be given appropriate training in data protection and privacy, addressing the relevant aspects of the Data Protection Legislation, this Policy, the Company's Data Protection Policy, and all other applicable Company policies.

7.4 The Company's data protection compliance shall be regularly reviewed and evaluated by means of Data Protection Audits.

7.5 The Company shall keep written internal records of all personal data collection, holding, and processing.

8. Implementation of Policy

This Policy shall be deemed effective as of 07.06.2023 No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: Helen Little

Position: Director

Date: 07.06.2023

Due for Review by: 06.06.2024

Signature: