

## FUTURE STRATEGY

Terms and Conditions for Supply of Services (the “**Conditions**”)

**THE CLIENT’S ATTENTION IS PARTICULARLY DRAWN TO THE PROVISIONS OF CLAUSE 8 (LIMITATION OF LIABILITY).**

### 1. Interpretation

The following definitions and rules of interpretation apply in these Conditions.

#### 1.1. Definitions:

**Business Day:** a day other than a Saturday, Sunday or public holiday in England, when banks in London are open for business.

**Charges:** the charges payable by the Client for the supply of the Services in accordance with clause 5.

**Client:** the person or firm who purchases Services from Future Strategy.

**Client Default:** has the meaning set out in clause 4.2.

**Commencement Date:** has the meaning given in clause 2.2.

**Conditions:** these terms and conditions as amended from time to time in accordance with clause 11.5.

**Future Strategy:** Future Strategy Limited a company incorporated and registered in England with company number 07768919 whose registered office address is The Old Carriage Works, Moresk Road, Truro, Cornwall, TR1 1DG.

**Contract:** the contract between Future Strategy and the Client for the supply of Services in accordance with these Conditions.

**Control:** has the meaning given in section 1124 of the Corporation Tax Act 2010, and the expression **change of control** shall be construed accordingly.

**Order:** the Client's order for Services set out in the Proposal & Agreement.

**Proposal & Agreement:** provided to the Client by Future Strategy detailing the Services to be provided by Future Strategy.

**Services:** the services supplied by Future Strategy to the Client as set out in the Agreement Documents.

**Agreement Documents:** the description and/or specification of the Services provided in the Proposal & Agreement.

**Consultant Materials:** has the meaning set out in **clause 4.1(f)**.

#### 1.2. Interpretation:

- (a) A reference to legislation or a legislative provision:
  - (i) is a reference to it as it is in force as at the date of this Contract; and
  - (ii) shall include all subordinate legislation made as at the date of this Contract under that legislation or legislative provision.
- (b) Any words following the terms **including, include, in particular, for example** or any similar expression, shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms.
- (c) A reference to **writing** or **written** includes email but not fax.

## **2. Basis of contract**

- 2.1. The Order constitutes an offer by the Client to purchase Services in accordance with these Conditions.
- 2.2. The Order shall only be deemed to be accepted when the Client returns a signed Proposal & Agreement to Future Strategy. However, no material work or actions will be carried out by Future Strategy until the Charges are paid by the Client to Future Strategy in accordance with clause 5 (**Commencement Date**).
- 2.3. Any samples, drawings, descriptive matter or advertising issued by Future Strategy, and any descriptions or illustrations contained in Future Strategy's catalogues or brochures, are issued or published for the sole purpose of giving an approximate idea of the Services described in them. They shall not form part of the Contract or have any contractual force.
- 2.4. These Conditions apply to the Contract to the exclusion of any other terms that the Client seeks to impose or incorporate, or which are implied by law, trade custom, practice or course of dealing.
- 2.5. Any Proposal & Agreement given by Future Strategy shall not constitute an offer, and is only valid for a period of 14 Business Days from its date of issue unless otherwise agreed by Future Strategy.

## **3. Supply of Services**

- 3.1. Future Strategy shall supply the Services to the Client in accordance with the Agreement Documents in all material respects.
- 3.2. Future Strategy shall use reasonable endeavours to perform the Services specified in the Order, but any dates given by Future Strategy shall be estimates only as it is limited by third party performance. Future Strategy aim to supply the Services in a time scale of

three to nine months but time shall not be of the essence for performance of the Services.

- 3.3. Future Strategy reserves the right to amend the Agreement Documents if necessary to comply with any applicable law or regulatory requirement, or if the amendment will not materially affect the nature or quality of the Services, and Future Strategy shall notify the Client in any such event.
- 3.4. Future Strategy warrants to the Client that the Services will be provided using reasonable care and skill.

#### 4. **Client's obligations**

- 4.1. The Client shall:
  - (a) ensure that the terms of the Order (including all associated documents) and any information it provides in the Order or otherwise to Future Strategy are complete and accurate;
  - (b) be responsible for providing up-to-date, relevant and accurate information and materials as Future Strategy may reasonably require in order to supply the Services, and ensure that such information is complete and accurate in all material respects;
  - (c) be responsible at all times throughout the Contract and upon termination of it, for any action, penalty or other consequence arising as a result of Future Strategy using such information;
  - (d) co-operate with Future Strategy in all matters relating to the Services;
  - (e) obtain and maintain all necessary licences, permissions and consents which may be required for the Services before the date on which the Services are to start;
  - (f) keep all documents and other property of Future Strategy (**Consultant Materials**) at the Client's premises, and not dispose of or use the Consultant Materials other than in accordance with Future Strategy's written instructions or authorisation;
  - (g) maintain accurate company book keeping and records in accordance with statutory requirements;
  - (h) notify Future Strategy of any changes to the Client business; and
  - (i) comply with any additional obligations as set out in the Order.
- 4.2. If Future Strategy's performance of any of its obligations under the Contract is prevented or delayed by any act or omission by the Client or failure by the Client to perform any relevant obligation (**Client Default**):

- (a) without limiting or affecting any other right or remedy available to it, Future Strategy shall have the right to suspend performance of the Services until the Client remedies the Client Default, and to rely on the Client Default to relieve it from the performance of any of its obligations in each case to the extent the Client Default prevents or delays Future Strategy's performance of any of its obligations;
- (b) Future Strategy shall not be liable for any costs or losses sustained or incurred by the Client arising directly or indirectly from Future Strategy's failure or delay to perform any of its obligations as set out in this clause 4.2; and
- (c) the Client shall reimburse Future Strategy on written demand for any costs or losses sustained or incurred by Future Strategy arising directly or indirectly from the Client Default.

## **5. Charges and payment**

- 5.1. The Charges for the Services shall be as set out in the Order (and all associated documents, or as amended in accordance with clause 5.3.
- 5.2. The Client shall pay the Charges on submission of the Order unless otherwise agreed by Future Strategy in full and in cleared funds to a bank account nominated in writing by Future Strategy.
- 5.3. Future Strategy shall be entitled to assess the Charges for the Services throughout the duration of the Contract and, if required, may request additional Charges (**Additional Charges**) to reflect additional work required to perform the Services which results from the Client's failure to provide accurate or complete information or materials prior to the Contract commencing or throughout the Contract.
- 5.4. Future Strategy shall inform the Client of any Additional Charges and shall provide the Client with an invoice. The Client shall settle such invoice in full and cleared funds within 14 days of the date of the invoice.
- 5.5. Time for payment shall be of the essence of the Contract.
- 5.6. All amounts due under the Contract shall be paid in full without any set-off, counterclaim, deduction or withholding (other than any deduction or withholding of tax as required by law).

## **6. Our Guarantee**

The Client may terminate the Contract within 14 days of acceptance in accordance with clause 9.5 (subject to clause 10.2).

## **7. Data protection**

The parties shall comply with their data protection obligations as set out in Schedule 1.

## **8. Limitation of liability**

- 8.1. Future Strategy's Services may include changing the registered office address of the Clients' limited company for correspondence purposes. Future Strategy does not accept or hold itself responsible or in any way acting as or representing the Client to any third party.
- 8.2. Future Strategy holds no responsibility for the accuracy of the information provided by the Client and which is subsequently used in the preparation or filing of any documentation, including, but not limited to any statement, report or audit on the Client's behalf.
- 8.3. As part of the Services, Future Strategy shall notify H M Revenue and Customs and the Client's creditors of the Client's intention to cease trading. Future Strategy shall rely upon and use the information provided by the Client to notify such parties. Future Strategy is not responsible for the accuracy of such information and is reliant on the information provided by the Client.
- 8.4. Future Strategy has obtained insurance cover in respect of its own legal liability for individual claim. The limits and exclusions in this clause reflect the insurance cover Future Strategy has been able to arrange and the Client is responsible for making its own arrangements for the insurance of any excess loss.
- 8.5. References to liability in this clause 8 include every kind of liability arising under or in connection with the Contract including liability in contract, tort (including negligence), misrepresentation, restitution or otherwise.
- 8.6. Neither party may benefit from the limitations and exclusions set out in this clause in respect of any liability arising from its deliberate default.
- 8.7. Nothing in this clause shall limit the Client's payment obligations under the Contract.
- 8.8. Nothing in the Contract limits any liability which cannot legally be limited, including but not limited to liability for:
  - (a) death or personal injury caused by negligence;

- (b) fraud or fraudulent misrepresentation; and
  - (c) breach of the terms implied by section 2 of the Supply of Goods and Services Act 1982 (title and quiet possession).
- 8.9. Subject to clause 8.6 (No limitation in respect of deliberate default), and clause 8.5 (Liabilities which cannot legally be limited), Future Strategy's total liability to the Client:
  - (a) for loss arising from Future Strategy's failure to comply with its data processing obligations under clause 7 shall not exceed £150,000 and
  - (b) for all other loss or damage shall not exceed £150,000.
- 8.10. Subject to clause 8.6 (No limitation in respect of deliberate default), clause 8.7 (No limitation of Client's payment obligations) and clause 8.8 (Liabilities which cannot legally be limited), this clause 8.10 sets out the types of loss that are wholly excluded:
  - (a) loss of profits.
  - (b) loss of sales or business.
  - (c) loss of agreements or contracts.
  - (d) loss of anticipated savings.
  - (e) loss of use or corruption of software, data or information.
  - (f) loss of or damage to goodwill; and
  - (g) indirect or consequential loss.
- 8.11. Future Strategy has given commitments as to compliance of the Services with relevant specifications in clause 3. In view of these commitments, the terms implied by sections 3, 4 and 5 of the Supply of Goods and Services Act 1982 are, to the fullest extent permitted by law, excluded from the Contract.
- 8.12. Unless the Client notifies Future Strategy that it intends to make a claim in respect of an event within the notice period, Future Strategy shall have no liability for that event. The notice period for an event shall start on the day on which the Client became, or ought reasonably to have become, aware of the event having occurred and shall expire three months from that date. The notice must be in writing and must identify the event and the grounds for the claim in reasonable detail.
- 8.13. This clause shall survive termination of the Contract.

## **9. Termination**

- 9.1. Without affecting any other right or remedy available to it, either party may terminate the Contract by giving the other party one months' written notice.

- 9.2. Without affecting any other right or remedy available to it, either party may terminate the Contract with immediate effect by giving written notice to the other party if:
- (a) the other party commits a material breach of any term of the Contract and (if such a breach is remediable) fails to remedy that breach within 10 Business Days of that party being notified in writing to do so; or
  - (b) the other party's financial position deteriorates to such an extent that in the terminating party's opinion the other party's capability to adequately fulfil its obligations under the Contract has been placed in jeopardy.
- 9.3. Without affecting any other right or remedy available to it, Future Strategy may terminate the Contract with immediate effect by giving written notice to the Client if but not limited to:
- (a) the Client fails to pay any amount due under the Contract on the due date for payment; or
  - (b) the Client making company filings without discussing the implication first and obtaining authority to do so from Future Strategy; or
  - (c) the Client changing the company name; or
  - (d) the Client changing directors or resigning as a director; or
  - (e) the Client starting a new limited company before your company has been fully dissolved; or
  - (f) the Client commencing trade within the company; or
  - (g) the Client failing to respond to any contact by Future Strategy within a reasonable timeframe; or
  - (h) the Client has committed fraud; or
  - (i) there is a change of control of the Client.
- 9.4. Without affecting any other right or remedy available to it, Future Strategy may suspend the supply of Services under the Contract or any other contract between the Client and Future Strategy if the Client fails to pay any amount due under the Contract on the due date for payment.
- 9.5. The Client may terminate the Contract within 14 days of acceptance (subject to clause 10.2).

## **10. Consequences of termination**

- 10.1. On termination or expiry of the Contract (except in accordance with clause 9.5):
- (a) the Client shall immediately pay to Future Strategy all Charges due under the Contract;

- (b) the Client shall immediately pay to Future Strategy any further charges reasonably required by Future Strategy for work that will still need to be supplied but for which no invoice has been submitted, Future Strategy shall submit an invoice, which shall be payable by the Client immediately on receipt; and
  - (c) the Client shall return or destroy as appropriate all of the Consultant Materials and any Deliverables which have not been fully paid for. If the Client fails to do so, then Future Strategy may enter the Client's premises and take possession of them. Until they have been returned, the Client shall be solely responsible for their safe keeping and will not use them for any purpose not connected with the Contract.
- 10.2. If the Client terminates the contract in accordance with clause 9.5, Future Strategy will provide a refund of the Charges paid by the Client minus any costs already incurred by Future Strategy.
- 10.3. Termination or expiry of the Contract shall not affect any rights, remedies, obligations or liabilities of the parties that have accrued up to the date of termination, including the right to claim damages in respect of any breach of the Contract which existed at or before the date of termination or expiry.
- 10.4. Any provision of the Contract that expressly or by implication is intended to come into or continue in force on or after termination or expiry of the Contract shall remain in full force and effect.

## **11. General**

- 11.1. **Force majeure.** Neither party shall be in breach of the Contract nor liable for delay in performing, or failure to perform, any of its obligations under the Contract if such delay or failure result from events, circumstances or causes beyond its reasonable control.
- 11.2. For the avoidance of doubt pandemics and epidemics shall constitute a force majeure event.
- 11.3. **Assignment and other dealings.**
- (a) Future Strategy may at any time assign, mortgage, charge, subcontract, delegate, declare a trust over or deal in any other manner with any or all of its rights and obligations under the Contract.
  - (b) The Client shall not assign, transfer, mortgage, charge, subcontract, delegate, declare a trust over or deal in any other manner with any of its rights and obligations under the Contract.



#### **11.4. Confidentiality.**

- (a) Each party undertakes that it shall not at any time during the Contract, and for a period of two years after termination or expiry of the Contract, disclose to any person any confidential information concerning the business, affairs, Clients, clients or Consultants of the other party, except as permitted by clause 11.3(b).
- (b) Each party may disclose the other party's confidential information:
  - (i) to its employees, officers, representatives, contractors, subcontractors or advisers who need to know such information for the purposes of carrying out the party's obligations under the Contract. Each party shall ensure that its employees, officers, representatives, contractors, subcontractors or advisers to whom it discloses the other party's confidential information comply with this clause; and
  - (ii) as may be required by law, a court of competent jurisdiction or any governmental or regulatory authority.
- (c) Unless agreed otherwise in these Conditions neither party shall use the other party's confidential information for any purpose other than to perform its obligations under the Contract.

#### **11.5. Entire agreement.**

- (a) The Contract constitutes the entire agreement between the parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter.
- (b) Each party acknowledges that in entering into the Contract it does not rely on, and shall have no remedies in respect of any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in the Contract. Each party agrees that it shall have no claim for innocent or negligent misrepresentation or negligent misstatement based on any statement in the Contract.
- (c) Nothing in this clause shall limit or exclude any liability for fraud.

**11.6. Variation.** Except as set out in these Conditions, no variation of the Contract shall be effective unless it is in writing by both parties (or their authorised representatives).

**11.7. Waiver.** A waiver of any right or remedy under the Contract or by law is only effective if given in writing and shall not be deemed a waiver of any subsequent right or remedy. A failure or delay by a party to exercise any right or remedy provided under the Contract or by law shall not constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict any further exercise of that or any other right or remedy. No single or

partial exercise of any right or remedy provided under the Contract or by law shall prevent or restrict the further exercise of that or any other right or remedy.

**11.8. Severance.** If any provision or part-provision of the Contract is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of this agreement. If any provision or part-provision of this Contract deleted under this clause the parties shall negotiate in good faith to agree a replacement provision that, to the greatest extent possible, achieves the intended commercial result of the original provision.

**11.9. Notices.**

- (a) Any notice or other communication given to a party under or in connection with the Contract shall be in writing and shall be delivered by hand or by pre-paid first-class post or other next working day delivery service at its registered office; or sent by email to the address specified in the Order.
- (b) Any notice or communication shall be deemed to have been received:
  - (i) if delivered by hand, at the time the notice is left at the proper address;
  - (ii) if sent by pre-paid first-class post or other next working day delivery service, at 9.00 am on the second Business Day after posting; or
  - (iii) if sent by email at the time of transmission, or, if this time falls outside business hours in the place of receipt, when business hours resume. In this clause 11.8(b)(iii), business hours means 9.00am to 5.00pm Monday to Friday on a day that is not a public holiday in the place of receipt.
- (c) This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any other method of dispute resolution.

**11.10. Third party rights.**

Unless it expressly states otherwise, the Contract does not give rise to any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of the Contract.

**11.11. Governing law.** The Contract, and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by, and construed in accordance with the law of England and Wales.

**11.12. Jurisdiction.** Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with the Contract or its subject matter or formation.



Future Strategy Limited  
Data Protection Policy  
Created: February 2022  
Last updated: March 2022

## 1. Introduction

This Policy sets out the obligations of Future Strategy Limited, a company registered in England and Wales under number 07768919 whose registered office is at The Old Carriage Works, Moresk Road, Truro, Cornwall, TR1 1DG (“Future Strategy”) regarding data protection and the rights of staff, retail and corporate customers and business contacts (“data subjects”) in respect of their personal data under Data Protection Law.

“Data Protection Law” means all legislation and regulations in force from time to time regulating the use of personal data and the privacy of electronic communications including, but not limited to, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the “UK GDPR”), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation.

This Policy sets Future Strategy’s obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by Future Strategy, its employees, agents, contractors, or other parties working on behalf of Future Strategy.

## 2. Definitions

<b>“consent”</b>	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;
<b>“data controller”</b>	means the natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, Future Strategy is the data controller of all personal data relating to staff, retail and corporate customers and business contacts used in our business for our commercial purposes;
<b>“data processor”</b>	means a natural or legal person or organisation which processes personal data on behalf of a data controller;
<b>“data subject”</b>	means a living, identified, or identifiable natural person about whom Future Strategy holds personal data;
<b>“EEA”</b>	means the European Economic Area, consisting of all EU Member States, Iceland, Liechtenstein, and Norway;

<b>“personal data”</b>	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;
<b>“personal data breach”</b>	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;
<b>“processing”</b>	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;
<b>“pseudonymisation”</b>	means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person; and
<b>“special category personal data”</b>	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. **Scope**

1. Future Strategy is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.
2. Future Strategy’s **Data Protection Officer** is Russell Caldwell. The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.
3. Future Strategy’s **Data Protection Officer** is Russell Caldwell, is responsible for ensuring that all employees, agents, contractors, or other parties working on

behalf of Future Strategy comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.

4. Any questions relating to this Policy or to Data Protection Law should be referred to the Data Protection Officer. In particular, the Data Protection Officer should always be consulted in the following cases:
  - a) if there is any uncertainty relating to the lawful basis on which personal data is to be collected, held, and/or processed;
  - b) if consent is being relied upon in order to collect, hold, and/or process personal data;
  - c) if there is any uncertainty relating to the retention period for any particular type(s) of personal data;
  - d) if any new or amended privacy notices or similar privacy-related documentation are required;
  - e) if any assistance is required in dealing with the exercise of a data subject's rights (including, but not limited to, the handling of subject access requests);
  - f) if a personal data breach (suspected or actual) has occurred;
  - g) if there is any uncertainty relating to security measures (whether technical or organisational) required to protect personal data;
  - h) if personal data is to be shared with third parties (whether such third parties are acting as data controllers or data processors);
  - i) if personal data is to be transferred outside of the UK and there are questions relating to the legal basis on which to do so;
  - j) when any significant new processing activity is to be carried out, or significant changes are to be made to existing processing activities, which will require a Data Protection Impact Assessment;
  - k) when personal data is to be used for purposes different to those for which it was originally collected;
  - l) if any automated processing, including profiling or automated decision-making, is to be carried out; or
  - m) if any assistance is required in complying with the law applicable to direct marketing.

#### 4. **The Data Protection Principles**

This Policy aims to ensure compliance with Data Protection Law. The UK GDPR sets out the following principles with which any party handling personal data must comply. Data controllers are responsible for, and must be able to demonstrate, such compliance. All personal data must be:

1. processed lawfully, fairly, and in a transparent manner in relation to the data subject;
2. 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;

3. adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;
4. accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 UK GDPR in order to safeguard the rights and freedoms of the data subject;
6. 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.

## 5. **The Rights of Data Subjects**

The UK GDPR sets out the following key rights applicable to data subjects:

1. The right to be informed;
2. the right of access;
3. the right to rectification;
4. the right to erasure (also known as the 'right to be forgotten');
5. the right to restrict processing;
6. the right to data portability;
7. the right to object; and
8. rights with respect to automated decision-making and profiling.

## 6. **Lawful, Fair, and Transparent Data Processing**

1. Data Protection Law seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Specifically, the processing of personal data shall be lawful if at least one of the following applies:
  - a) the data subject has given consent to the processing of their personal data for one or more specific purposes;
  - b) the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;
  - c) the processing is necessary for compliance with a legal obligation to which the data controller is subject;



- d) the processing is necessary to protect the vital interests of the data subject or of another natural person;
  - e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
  - f) the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
2. If the personal data in question is special category personal data (also known as “sensitive personal data”), at least one of the following conditions must be met:
- a) the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless the law prohibits them from doing so);
  - b) the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by law or a collective agreement pursuant to law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);
  - c) the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
  - d) the data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
  - e) the processing relates to personal data which is manifestly made public by the data subject;
  - f) the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
  - g) the processing is necessary for substantial public interest reasons, on the basis of law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
  - h) the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the UK GDPR;

- i) the processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or
- j) the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the UK GDPR (as supplemented by section 19 of the Data Protection Act 2018) based on law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.]

## 7. **Consent**

If consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, the following shall apply:

1. Consent is a clear indication by the data subject that they agree to the processing of their personal data. Such a clear indication may take the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity are unlikely to amount to consent.
2. Where consent is given in a document which includes other matters, the section dealing with consent must be kept clearly separate from such other matters.
3. Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly.
4. If personal data is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal data was originally collected that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject.
5. If special category personal data is processed, Future Strategy shall normally rely on a lawful basis other than explicit consent. If explicit consent is relied upon, the data subject in question must be issued with a suitable privacy notice in order to capture their consent.
6. In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, records must be kept of all consents obtained in order to ensure that Future Strategy can demonstrate its compliance with consent requirements.

## 8. **Specified, Explicit, and Legitimate Purposes**

1. Future Strategy collects and processes the personal data set out in Part 24 of this Policy. This includes:
  - a) personal data collected directly from data subjects and;
  - b) personal data obtained from third parties.

2. Future Strategy only collects, processes, and holds personal data for the specific purposes set out in Part 24 of this Policy (or for other purposes expressly permitted by Data Protection Law).
  3. Data subjects must be kept informed at all times of the purpose or purposes for which Future Strategy uses their personal data. Please refer to Part 15 for more information on keeping data subjects informed.
9. **Adequate, Relevant, and Limited Data Processing**
1. Future Strategy 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) as under Part 8, above, and as set out in Part 24, below.
  2. Employees, agents, contractors, or other parties working on behalf of Future Strategy may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected.
  3. Employees, agents, contractors, or other parties working on behalf of Future Strategy may process personal data only when the performance of their job duties requires it. Personal data held by Future Strategy cannot be processed for any unrelated reasons.
10. **Accuracy of Data and Keeping Data Up-to-Date**
1. Future Strategy 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, as set out in Part 17, below.
  2. The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. 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.
11. **Data Retention**
1. Future Strategy 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.
  2. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.
  3. For full details of Future Strategy's approach to data retention, including retention periods for specific personal data types held by Future Strategy, please refer to our Data Retention Policy.
12. **Secure Processing**
1. Future Strategy 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 provided in Parts 25 to 30 of this Policy.

2. All technical and organisational measures taken to protect personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data.
3. 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.

### 13. **Accountability and Record-Keeping**

1. The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.
2. Future Strategy 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 (please refer to Part 14 for further information).
3. All employees, agents, contractors, or other parties working on behalf of Future Strategy shall be given appropriate training in data protection and privacy, addressing the relevant aspects of Data Protection Law, this Policy, and all other applicable Company policies.
4. Future Strategy's data protection compliance shall be regularly reviewed and evaluated.
5. Future Strategy shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:
  - a) the name and details of Future Strategy, its Data Protection Officer, and any applicable third-party data transfers (including data processors and other data controllers with whom personal data is shared);
  - b) the purposes for which Future Strategy collects, holds, and processes personal data;
  - c) Future Strategy's legal basis or bases (including, but not limited to, consent, the mechanism(s) for obtaining such consent, and records of such consent) for collecting, holding, and processing personal data;
  - d) details of the categories of personal data collected, held, and processed by Future Strategy, and the categories of data subject to which that personal data relates;
  - e) details of any transfers of personal data to non-UK countries including all mechanisms and security safeguards;

- f) details of how long personal data will be retained by Future Strategy (please refer to Future Strategy's Data Retention Policy);
- g) details of personal data storage, including location(s);
- h) detailed descriptions of all technical and organisational measures taken by Future Strategy to ensure the security of personal data.

**14. Data Protection Impact Assessments and Privacy by Design**

1. In accordance with the privacy by design principles, Future Strategy shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies where the processing involved is likely to result in a high risk to the rights and freedoms of data subjects.
2. The principles of privacy by design should be followed at all times when collecting, holding, and processing personal data. The following factors should be taken into consideration:
  - a) the nature, scope, context, and purpose or purposes of the collection, holding, and processing;
  - b) the state of the art of all relevant technical and organisational measures to be taken;
  - c) the cost of implementing such measures; and
  - d) the risks posed to data subjects and to Future Strategy, including their likelihood and severity.
3. Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:
  - a) the type(s) of personal data that will be collected, held, and processed;
  - b) the purpose(s) for which personal data is to be used;
  - c) Future Strategy's objectives;
  - d) how personal data is to be used;
  - e) the parties (internal and/or external) who are to be consulted;
  - f) the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
  - g) risks posed to data subjects;
  - h) risks posed both within and to Future Strategy; and
  - i) proposed measures to minimise and handle identified risks.

**15. Keeping Data Subjects Informed**

1. Future Strategy shall provide the information set out in Part 15.2 to every data subject:
  - a) where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

- b) where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
    - i) if the personal data is used to communicate with the data subject, when the first communication is made; or
    - ii) if the personal data is to be transferred to another party, before that transfer is made; or
    - iii) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.
2. The following information shall be provided in the form of a privacy notice:
- a) details of Future Strategy including, but not limited to, contact details, and the names and contact details of any applicable representatives and its Data Protection Officer;
  - b) the purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 24 of this Policy) and the lawful basis justifying that collection and processing;
  - c) where applicable, the legitimate interests upon which Future Strategy is justifying its collection and processing of the personal data;
  - d) where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
  - e) where the personal data is to be transferred to one or more third parties, details of those parties;
  - f) where the personal data is to be transferred to a third party that is located outside of the UK, details of that transfer, including but not limited to the safeguards in place (see Part 31 of this Policy for further details);
  - g) details of applicable data retention periods;
  - h) details of the data subject's rights under the UK GDPR;
  - i) details of the data subject's right to withdraw their consent to Future Strategy's processing of their personal data at any time;
  - j) details of the data subject's right to complain to the Information Commissioner's Office;
  - k) where the personal data is not obtained directly from the data subject, details about the source of that personal data;
  - l) where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
  - m) details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

## 16. **Data Subject Access**

- 1. Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which Future Strategy holds about them, what it is doing with that personal data, and why.

2. Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to Future Strategy's Data Protection Officer at russell@futurestrategy.co.uk.
3. Responses to SARs must normally be made within one month of receipt, however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.
4. All SARs received shall be handled by Future Strategy's Data Protection Officer and in accordance with Future Strategy's Data Subject Access Request Policy & Procedure.
5. Future Strategy does not charge a fee for the handling of normal SARs. Future Strategy reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

**17. Rectification of Personal Data**

1. Data subjects have the right to require Future Strategy to rectify any of their personal data that is inaccurate or incomplete.
2. Future Strategy shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing Future Strategy of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
3. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

**18. Erasure of Personal Data**

1. Data subjects have the right to request that Future Strategy erases the personal data it holds about them in the following circumstances:
  - a) it is no longer necessary for Future Strategy to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
  - b) the data subject wishes to withdraw their consent to Future Strategy holding and processing their personal data;
  - c) the data subject objects to Future Strategy holding and processing their personal data (and there is no overriding legitimate interest to allow Future Strategy to continue doing so) (see Part 21 of this Policy for further details concerning the right to object);
  - d) the personal data has been processed unlawfully;
  - e) the personal data needs to be erased in order for Future Strategy to comply with a particular legal obligation;
2. Unless Future Strategy has reasonable grounds to refuse to erase personal data,

all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

3. In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

#### 19. **Restriction of Personal Data Processing**

1. Data subjects may request that Future Strategy ceases processing the personal data it holds about them. If a data subject makes such a request, Future Strategy shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.
2. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

#### 20. **Data Portability**

1. Future Strategy does not process any personal data using solely automated means. At Future Strategy we do use a third-party automated programme supplied by Credit Safe to assist us in the identification process of company directors, this is used in conjunction with a human approach which ultimately makes the final decision. We also use third-party software supplied by Trello to record all customer interactions and upload all documentation to a third party storage system supplied by DropBox.
2. Where data subjects have given their consent to Future Strategy to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between Future Strategy and the data subject, data subjects have the right, under the UK GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).
3. To facilitate the right of data portability, Future Strategy shall make available all applicable personal data to data subjects in the following formats:
  - a) CSV
  - b) PDF
  - c) Microsoft Word
4. Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.
5. All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.



**21. Objections to Personal Data Processing**

1. Data subjects have the right to object to Future Strategy processing their personal data based on legitimate interests, for direct marketing (including profiling).
2. Where a data subject objects to Future Strategy processing their personal data based on its legitimate interests, Future Strategy shall cease such processing immediately, unless it can be demonstrated that Future Strategy's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.
3. Where a data subject objects to Future Strategy processing their personal data for direct marketing purposes, Future Strategy shall cease such processing promptly.

**22. Direct Marketing**

1. Future Strategy is subject to certain rules and regulations when marketing its services.
2. The prior consent of data subjects is required for electronic direct marketing including email, text messaging, and automated telephone calls subject to the following limited exception:
  - a) Future Strategy may send marketing text messages or emails to a customer provided that that customer's contact details have been obtained in the course of a sale, the marketing relates to similar services, and the customer in question has been given the opportunity to opt-out of marketing when their details were first collected and in every subsequent communication from Future Strategy.
3. The right to object to direct marketing shall be explicitly offered to data subjects in a clear and intelligible manner and must be kept separate from other information in order to preserve its clarity.
4. If a data subject objects to direct marketing, their request must be complied with promptly. A limited amount of personal data may be retained in such circumstances to the extent required to ensure that the data subject's marketing preferences continue to be complied with.

**23. Data Security - Transferring Personal Data and Communications**

Future Strategy shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

1. All emails containing personal data must be encrypted.
2. All emails containing personal data must be marked "confidential";
3. Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
4. Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
5. 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;

6. 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;
7. Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient.
8. 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";

#### **24. Data Security - Storage**

Future Strategy shall ensure that the following measures are taken with respect to the storage of personal data:

1. All electronic copies of personal data should be stored securely using passwords and data encryption;
2. 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;
3. All personal data stored electronically should be backed up with backups stored. All backups should be encrypted.
4. No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to Future Strategy or otherwise without the formal written approval of Future Strategy's Data Protection Officer – Russel Caldwell and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;
5. No personal data should be transferred to any device personally belonging to an employee, agent, contractor, or other party working on behalf of Future Strategy and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of Future Strategy where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the applicable Data Protection Law (which may include demonstrating to Future Strategy that all suitable technical and organisational measures have been taken);

#### **25. Data Security - Disposal**

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 Future Strategy's Data Retention Policy.

#### **26. Data Security - Use of Personal Data**

Future Strategy shall ensure that the following measures are taken with respect to the

use of personal data:

1. No personal data may be shared informally and if an employee, agent, contractor, or other party working on behalf of Future Strategy requires access to any personal data that they do not already have access to, such access should be formally requested from Russell Caldwell, Future Strategy's Data Protection Officer.
2. No personal data may be transferred to any employee, agent, contractor, or other party, whether such parties are working on behalf of Future Strategy or not, without the authorisation of Russell Caldwell, Future Strategy's Data Protection Officer.
3. 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;
4. 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;
5. Where personal data held by Future Strategy is used for marketing purposes, it shall be the responsibility of Russell Caldwell, Future Strategy's Data Protection Officer 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;

## **27. Data Security - IT Security**

Future Strategy shall ensure that the following measures are taken with respect to IT and information security:

1. 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 Future Strategy is designed to require such passwords;
2. Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of Future Strategy, 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;
3. All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. Future Strategy's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible after the updates are made available by the publisher or manufacturer, unless there are valid technical reasons not to do so;
4. No software may be installed on any Company-owned computer or device without the prior approval of the Russell Caldwell, Future Strategy's Data Protection Officer.

## 28. **Organisational Measures**

Future Strategy shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

1. All employees, agents, contractors, or other parties working on behalf of Future Strategy shall be made fully aware of both their individual responsibilities and Future Strategy's responsibilities under Data Protection Law and under this Policy, and shall be provided with a copy of this Policy;
2. Only employees, agents, contractors, or other parties working on behalf of Future Strategy 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 Future Strategy;
3. 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;
4. All employees, agents, contractors, or other parties working on behalf of Future Strategy handling personal data will be appropriately trained to do so;
5. All employees, agents, contractors, or other parties working on behalf of Future Strategy handling personal data will be appropriately supervised;
6. All employees, agents, contractors, or other parties working on behalf of Future Strategy 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;
7. Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
8. All personal data held by Future Strategy shall be reviewed periodically, as set out in Future Strategy's Data Retention Policy;
9. The performance of those employees, agents, contractors, or other parties working on behalf of Future Strategy handling personal data shall be regularly evaluated and reviewed;
10. All employees, agents, contractors, or other parties working on behalf of Future Strategy handling personal data will be bound to do so in accordance with the principles of Data Protection Law and this Policy by contract;
11. All agents, contractors, or other parties working on behalf of Future Strategy 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 Future Strategy arising out of this Policy and Data Protection Law;
12. Where any agent, contractor or other party working on behalf of Future Strategy handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless Future Strategy against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

## 29. **Transferring Personal Data to a Country Outside the UK**

1. Future Strategy may, from time to time, transfer ('transfer' includes making available remotely) personal data to countries outside of the UK. The UK GDPR

restricts such transfers in order to ensure that the level of protection given to data subjects is not compromised.

2. Personal data may only be transferred to a country outside the UK if one of the following applies:
  - a) The UK has issued regulations confirming that the country in question ensures an adequate level of protection (referred to as 'adequacy decisions' or 'adequacy regulations'). From 1 January 2021, transfers of personal data from the UK to EEA countries will continue to be permitted. Transitional provisions are also in place to recognise pre-existing EU adequacy decisions in the UK.
  - b) Appropriate safeguards are in place including binding corporate rules, standard contractual clauses approved for use in the UK (this includes those adopted by the European Commission prior to 1 January 2021), an approved code of conduct, or an approved certification mechanism.
  - c) The transfer is made with the informed and explicit consent of the relevant data subject(s).
  - d) The transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between the data subject and Future Strategy; public interest reasons; for the establishment, exercise, or defence of legal claims; to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent; or, in limited circumstances, for Future Strategy's legitimate interests.

### 30. **Data Breach Notification**


1. All personal data breaches must be reported immediately to Future Strategy's Data Protection Officer, Russell Caldwell.
2. If an employee, agent, contractor, or other party working on behalf of Future Strategy becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. Any and all evidence relating to the personal data breach in question should be carefully retained.
3. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g., financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), then Russell Caldwell, as Future Strategy's Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
4. In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 32.3) to the rights and freedoms of data subjects, then Russell Caldwell, Future Strategy's Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.
5. Data breach notifications shall include the following information:
  - a) The categories and approximate number of data subjects concerned;
  - b) The categories and approximate number of personal data records concerned;

- c) The name and contact details of Future Strategy’s data protection officer (or other contact point where more information can be obtained);
- d) The likely consequences of the breach;
- e) Details of the measures taken, or proposed to be taken, by Future Strategy to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

**31. Implementation of Policy**

This Policy shall be deemed effective as of 1<sup>st</sup> March 2022. 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:** Russell Caldwell  
**Position:** Director and Data Protection Officer  
**Signature:**   
**Date:** 28<sup>th</sup> March 2022  
**Due for Review by:** 28<sup>th</sup> March 2023

**HEAD OFFICE**

Suite 3, 91 Mayflower Street,  
Plymouth, Devon PL1 1SB

**WALES OFFICE**

Suite 100, 45 Salisbury Road,  
Cardiff, CF24 4AB

**SCOTLAND OFFICE**

Suite 14, 98 Woodlands Road,  
Charing Cross, Glasgow, G3 6HB

**N.IRELAND OFFICE**

Suite 20, 21 Botanic Avenue,  
Belfast, Northern Ireland, BT17 1JJ

Future Strategy Limited is Authorised & Regulated by the Financial Conduct Authority, FRN: 730047

Registered Office: The Old Carriage Works, Moresk Road, Truro, Cornwall, TR1 1DG | Company Registration Number: 07768919