1. Introduction

This Policy sets out the obligations of Learn to Trade Limited (referred to as "LTT" or "the Company") regarding data protection and the rights of current, past and prospective staff, suppliers, clients, customers, and others with whom it has business or with whom it communicates ("data subjects") in respect of their personal data in accordance with UK data protection law which includes but may not be limited to the UK General Data Protection Regulation ("UK GDPR"), the Privacy and Electronic Communications Regulation (PECR) and the data Protection Act 2018 (DPA) (hereafter referred to as UK data protection law). Other legislation may be applicable according to the jurisdiction in which an individual for whom we may process personal data may reside.

UK data protection law defines "personal data" as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, name, email address, telephone number, postal address, IP address etc, and credit card numbers.

This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by LTT, its employees, agents, contractors, or other parties working on behalf of the Company.

LTT is committed to ensuring that it treats personal information lawfully 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. The Data Protection Principles

This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be:

a) processed lawfully, fairly, and in a transparent manner in relation to the data subject;

b) collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

d) 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 they are processed, is erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data 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 Regulation in order to safeguard the rights and freedoms of the data subject;

f) 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.

g) Demonstrably accounted for with accurate records of all processing activities, please refer to section 9 of this policy.

3. Lawful, Fair, and Transparent Data Processing

The Regulation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Regulation states that 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 his or her personal data for one or more specific purposes;

b) processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into a contract;

c) processing is necessary for compliance with a legal obligation to which the controller is subject;

d) processing is necessary to protect the vital interests of the data subject or of another natural person;

e) 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 controller;

f) processing is necessary for the purposes of the legitimate interests pursued by the 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, where the data subject is a child.

g) LTT will initially process the personal data of potential and actual customers using their consent (a). Once a prospective customer becomes an actual customer the lawful basis will be contractual obligation (b). For the avoidance of doubt, this condition provides for the sharing of the data with other companies details of which are included in the terms of the contract.

4. Processed for Specified, Explicit and Legitimate Purposes

To conduct its normal business, LTT collects and uses certain types of personal information about living individuals. This personal data will be processed according to the legal basis of consent, contractual relationships with data subjects, compliance with regulated activities in which LTT is engaged and for the purposes of legitimate interests pursued by LTT , for example processing data to help improve the Company's products and services.

In particular:-

4.1 LTT collects and processes the personal data set out in Appendix C of this Policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates with us) and data received from third parties.

4.2 LTT only processes personal data for the specific purposes set out in Appendix A of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

5. Adequate, Relevant and Limited Data Processing

LTT will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 4, above.

6. Accuracy of Data and Keeping Data Up to Date

LTT shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

7. Timely Processing

LTT shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay. LTT's data retention policy is located at Appendix E.

8. Secure Processing

LTT shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 22 and 23 of this Policy.

9. Accountability

9.1 LTT, as Data Controller provides a structure that acknowledges the responsibilities and accountability for data protection. This is detailed in Appendix B.

9.2 LTT keeps internal records of all personal data collection, holding, and processing, which incorporate the following information:

a) LTT's name and details, responsible person(s) for data protection (see Appendix B), and any applicable third-party data processors (see Appendix D);

b) The purposes for which LTT processes personal data (see Appendix A);

c) Details of the categories of personal data collected, held, and processed by the Company; and the categories of data subject to which that personal data relates; (See Appendix C)

d) Details (and categories) of any third parties that will receive personal data from LTT; (See Appendix C)

e) Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

f) Details of how long personal data will be retained by LTT (see Appendix E); and

g) Detailed descriptions of all technical and organisational measures taken by LTT to ensure the security of personal data (refer to the IT Security Policy).

10. Privacy Impact Assessments (DPIAs)

LTT shall carry out Privacy Impact Assessments when and as required under the Regulation. The provision of a Privacy Impact Assessment shall be overseen by LTT's Compliance Team and shall address the following areas of importance:

10.1 The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;

10.2 Details of the legitimate interests being pursued by LTT;

10.3 An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

10.4 An assessment of the risks posed to individual data subjects; and

10.5 Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

11. The Rights of Data Subjects

The Regulation sets out the following rights applicable to data subjects:

a) The right to be informed;

b) The right of access;

c) The right to rectification;

d) The right to erasure (also known as the 'right to be forgotten');

e) The right to restrict processing;

f) The right to data portability;

g) The right to object;

h) Rights with respect to automated decision-making and profiling.

Attached at Appendix F is the process for a data subject to follow to exercise one of it's rights in respect of 11 a) – h).

12. Keeping Data Subjects Informed

12.1 LTT shall ensure that the following information is provided - by reference to this Data Protection Policy - to every data subject when personal data is collected:

a) Details of LTT including, but not limited to, the identity of any appointed Data Protection Officer;

b) The purpose(s) for which the personal data is being collected and will be processed (as detailed in Appendix A of this Policy) and the legal basis justifying that collection and processing;

c) Where applicable, the legitimate interests upon which LTT 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 European Economic Area (the "EEA") or any other country which the UK or the EU do not consider adequate, details of that transfer, including but not limited to the safeguards in place (see Part 21 of this Policy for further details concerning such third country data transfers);

g) Details of the length of time the personal data will be held by LTT (or, where there is no predetermined period, details of how that length of time will be determined);

h) Details of the data subject's rights under the Regulation;

i) Details of the data subject's right to withdraw their consent to LTT'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 (the 'supervisory authority' under the Regulation);

k) 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;

l) Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

12.2 The information set out above in Part 12.1 shall be provided to the data subject at the following applicable time:

12.2.1 Where the personal data is obtained from the data subject directly, at the time of collection;

12.2.2 Where the personal data is not obtained from the data subject directly (i.e. from another party):

a) If the personal data is used to communicate with the data subject, at the time of the first communication; or

b) If the personal data is to be disclosed to another party, before the personal data is disclosed; or

c) In any event, not more than one month after the time at which LTT obtains the personal data.

13. Data Subject Access

13.1 A data subject may make a subject access request (“SAR”) at any time to find out more about the personal data which LTT holds about them. LTT is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

13.2 All subject access requests received must be forwarded to the name of your Data Protection officer.

13.3 LTT will not charge a fee for the handling of normal SARs. LTT 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.

13.4 All SARs will be handled in accordance with the guidance of the ICO.

14. Rectification of Personal Data

14.1 If a data subject informs LTT that personal data held by LTT is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject’s notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

14.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

15. Erasure of Personal Data

15.1 Data subjects may request that LTT erases the personal data it holds about them in the following circumstances:

a) It is no longer necessary for LTT to hold that personal data with respect to the purpose for which it was originally collected or processed;

b) The data subject wishes to withdraw their consent to LTT holding and processing their personal data;

c) The data subject objects to LTT holding and processing their personal data (and there is no overriding legitimate interest to allow LTT to continue doing so) (see Part 18 of this Policy for further details concerning data subjects' rights to object);

d) The personal data has been processed unlawfully;

e) The personal data needs to be erased for LTT to comply with a legal obligation

15.2 Unless LTT 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 (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

15.3 In the event that any personal data that is to be erased in response to a data subject 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).

16. Restriction of Personal Data Processing

16.1 Data subjects may request that LTT ceases processing the personal data it holds about them. If a data subject makes such a request, LTT shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

16.2 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).

17. Data Portability

17.1 LTT processes personal data using automated means to ensure compliance with environmental legislation.

17.2 Where data subjects have given their consent to LTT to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between LTT and the data subject, data subjects have the legal right under the Regulation to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers, e.g. other organisations).

17.3 To facilitate the right of data portability, LTT shall make available all applicable personal data to data subjects in one of the following formats:

a) CSV files;
b) PDF files
c) Other multimedia, electronic (soft) or hard copy files.

17.4 Where technically feasible, if requested by a data subject, personal data shall be sent directly to another data controller.

17.5 All requests for copies of personal data shall be complied with within one month of the data subject's request (this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

18. Objections to Personal Data Processing

18.1 Data subjects have the right to object to LTT processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling), and processing for historical research and statistics purposes.

18.2 Where a data subject objects to LTT processing their personal data based on its legitimate interests, LTT shall cease such processing forthwith, unless it can be demonstrated that LTT's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

18.3 Where a data subject objects to LTT processing their personal data for direct marketing purposes, LTT shall cease such processing forthwith.

18.4 Where a data subject objects to LTT processing their personal data for historical research and statistics purposes, the data subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. LTT is not required comply if the research is necessary for the performance of a task carried out reasons of public interest.

19. Automated Decision-Making

19.1 In the event that LTT uses personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge to such decisions under the Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from LTT.

20. Profiling

Where LTT uses personal data for profiling purposes, the following shall apply:

a) Clear information explaining the profiling will be provided, including its significance and the likely consequences;

b) Appropriate mathematical or statistical procedures will be used;

c) Technical and organizational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented; and

d) All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 and 23 of this Policy for more details on data security).

21. International Transfer of Data

21.1 LTT may transfer personal data to countries who are not signatory to the GDPR for the following reasons:

a) To provide the data subject by telephone and e-mail with details of LTT's events, products and services which is facilitated by Empower U Inc (EU inc) a Company registered in the Philippines.

b) LTT has entered into an agreement with EU Inc to ensure EU Inc upholds LTT's data protection and data privacy policies.

c) LTT's Compliance Team will regularly hold training with EU Inc to ensure the compliance with the relevant legislation:

21.2 Where data is shared with or is accessible from a third country, LTT will adhere to its obligation regarding the UK data transfer regime. This includes but may not be limited to undertaking a transfer risk assessment. LTT will ensure that a UK safeguard is in force in such circumstances. These include using the UK addendum in combination with the EU standard contractual clauses (SCCs) or the UK international data transfer agreement (IDTA).

21.3 The Philippines legislation, the Data privacy Act of 2012(Republic Act No. 10173 requires a suitable data sharing agreement between group companies for the purpose of inter-group transfers. Such an agreement should include details relating to: –

a) purposes of the data sharing and the appropriate lawful basis
b) objectives that the data sharing is meant to achieve
c) identify all controllers that are a party to the data sharing agreement, and for each party, the agreement should specify:
d) the types of personal data it will share
e) whether the personal data processing will be outsourced, and if so, the types of processing the processor will be allowed to perform
f) the method to be used for processing; and
g) the designated data protection officer ('DPO')
h) term and duration of the data sharing arrangement
i) operational details of the data sharing, including the procedure the parties intend to observe in implementing the arrangement
j) description of the reasonable and appropriate organisational, physical and technical security measures that the parties intend to adopt
k) process for data breach management
l) mechanisms that allow the data subjects to exercise their rights relative to their personal data, including:
m) identity of the party or parties responsible for addressing information requests, complaints by the data subject, and/or any investigation by the NPC; and
n) procedure by which a data subject can access or obtain a copy of the data sharing agreement; and

o) rules for retention of the shared data, and the method that will be adopted for the secure return, destruction, or disposal of the shared data and the timeline.

21.4 Where the recipient is authorised to disclose the shared data or grant public access to the same, the data sharing agreement must clearly establish this, including the justification for allowing such public access, the parties to whom access is granted, the types of personal data made accessible, and the frequency and volume of such access. Furthermore, if the disclosure or further access is facilitated by an online platform, the program, middleware, and encryption method that will be used should also be identified in the data sharing agreement. The controllers' respective DPOs must sign as witnesses to the data sharing agreement. Furthermore, NPC Circular 20-03 also requires controllers to establish and maintain a record of its data sharing arrangements, including, among other things, contact details of all parties and their respective DPOs, legal bases for the data sharing arrangements, and, where applicable, proof of consent obtained from data subjects.

22. Data Protection Measures

LTT shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

a) All emails containing personal data must be encrypted;

b) Where 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. Hardcopies should be shredded.

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

d) Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

e) 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;

f) 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;

g) Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Royal Mail or an equivalent postal service;

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

i) 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;

j) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of the DPO.

k) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, volunteers, agents, sub-contractors or other parties at any time;

l) 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;

m) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to LTT or otherwise without formal written approval 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.

n) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, volunteers, contractors, or other parties working on behalf of LTT where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to LTT that all suitable technical and organisational measures have been taken);

o) All personal data stored electronically should be encrypted and backed up weekly with back-ups stored offsite.

p) All electronic copies of personal data should be stored securely using passwords and data encryption;

q) 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;

r) Under no circumstances should any passwords be written down or shared between any employees, volunteers, agents, contractors, or other parties working on
behalf of LTT, 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;

s) Where personal data held by LTT is used for marketing purposes, it shall be the responsibility of the Head of Marketing, to ensure that no data

subjects have added their details to any marketing preference databases including, but not limited to, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service, and the Fax Preference Service. Such details should be checked at least annually.

23. Organisational Measures

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

a) All employees, volunteers, agents, contractors, or other parties working on behalf of LTT shall be made fully aware of both their individual responsibilities and LTT's responsibilities under the Regulation and under this Policy, and shall be provided with a copy of this Policy;

b) Only employees, agents, sub-contractors, or other parties working on behalf of LTT 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 LTT;

c) All employees, volunteers, agents, contractors, or other parties working on behalf of LTT handling personal data will be appropriately trained to do so;

d) All employees, volunteers, agents, contractors, or other parties working on behalf of LTT handling personal data will be appropriately supervised;

e) Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;

f) The performance of those employees, volunteers, agents, contractors, or other parties working on behalf of LTT handling personal data shall be regularly evaluated and reviewed;

g) All employees, volunteers, agents, contractors, or other parties working on behalf of LTT handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract;

h) All agents, contractors, or other parties working on behalf of LTT 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 LTT arising out of this Policy and the Regulation;

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

24. **Data Breach Notification**

24.1 All personal data breaches must be reported immediately to LTT by e-mail to data@learntotrade.co.uk.

24.2 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), the 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 the breach.

24.3 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 24.2) to the rights and freedoms of data subjects, the data protection officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

24.4 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 LTT'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 LTT to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

25. General Training

LTT is responsible for ensuring that all of its employees, volunteers, associates, interns and contractors are aware of their personal responsibilities in relation to personal data, ensuring that it is properly protected at all times and is processed only in line with LTT's procedures.

To this end, LTT shall ensure that all of its employees are given appropriate and relevant training.

26. Implementation of Policy

This Policy was updated on 10th January 2023 and is reviewed annually.

APPENDIX A

1. LTT is a financial trading education company founded in 2003, which provides educational products and services to the public. LTT provides education in foreign exchange trading and also stocks, indices and commodities.. As LTT;

   a) Markets and offers to the general public free promotional events that provide information on education products and services. LTT's marketing activities collect data by way of implied consent to which all data subjects are asked to agree to and have the option to change their preferences at any time;

APPENDIX B – LTT data protection responsibilities

LTT will maintain a team with management oversight and responsibility for operational processes and maintenance of data protection policies and activities. The team will be made up of:-

Chief Executive Officer, with oversight of application of the regulation.

Head of Digital Marketing with responsibility for oversight of marketing activities with regard to compliance with the Regulation.

IT Manager with responsibility for Data compliance for all LTT systems, data stores and maintaining secure systems and processes through IT security policies

APPENDIX C - PERSONAL DATA

The following data may be collected, held and processed by LTT:

TYPE OF DATA	LAWFUL REASON FOR PROCESSING	PROSPECTIVE CUSTOMER	CUSTOMER	STAFF
FIRST NAME	CONSENT OR CONTRACTUAL	Y	Y	Y
LAST NAME	CONSENT OR CONTRACTUAL	Y	Y	Y
E-MAIL ADRESS	CONSENT OR CONTRACTUAL	Y	Y	Y
TELEPHONE NUMBER	CONSENT OR CONTRACTUAL	Y	Y	Y
MOBILE NUMBER	CONSENT OR CONTRACTUAL	Y	Y	Y
IP ADDRESS	CONSENT	Y	Y	Y
DATE OF BIRTH	CONSENT OR LEGAL OBLIGATION	N	Y	Y
POSTAL ADDRESS	CONSENT OR CONTRACTUAL	N	Y	Y
GENDER	CONSENT	N	Y	Y
EDUCATION LEVEL	CONSENT	N	N	Y

EMPLOYMENT STATUS	COMPLIANCE WITH LEGAL OBLIGATION	N	N	Y
ANNUAL INCOME	COMPLIANCE WITH LEGAL OBLIGATON	N	N	Y
CREDIT /DEBIT CARD	CONTRACTUAL	N	Y	N
BANK ACCOUNT DETAILS	CONTRACTUAL	N	Y	Y
NATIONAL INSURANCE NUMBER	COMPLIANCE WITH LEGAL OBLIGATION	N	N	Y
TAX CODES* this information may be shared with relevant tax authority.	COMPLIANCE WITH LEGAL OBLIGATION	N	N	Y
NATIONALITY	COMPLIANCE WITH LEGAL OBLIGATION	N	N	Y
NEXT OF KIN* this information may be shared in compliance with a legal obligation	COMPLIANCE WITH LEGAL OBLIGATION	N	N	Y
MEDICAL RECORDS	CONSENT / CONTRACTUAL	N	N	Y
PASSPORT NUMBER	COMPLIANCE WITH LEGAL OGBLIGATION	N	N	Y

DATA LTT SHARES WITH SMART CHARTS

DATA TYPE	LAWFUL REASON FOR PROCESSING	PROSPECTIVE CUSTOMER
NAME	CONTRACTUAL / LEGITIMATE INEREST	Y
EMAIL ADDRESS	CONTRACTUAL / LEGITIMATE INTEREST	Y
TELEPHONE	CONTRACTUAL / LEGITIMATE INTEREST	Y
ADDRESS	CONTRACTUAL / LEGITIMIATE INTEREST	Y

DATA LTT SHARES WITH CAPITAL INDEX

DATA TYPE	LAWFUL REASON FOR PROCESSING	PROSPECTIVE CUSTOMER	CUSTOMER
NAME	CONSENT CONTRACTUAL	N	Y
E-MAIL ADDRESS	CONSENT CONTRACTUAL	N	Y
TELEPHONE NUMBER	CONSENT CONTRACTUAL	N	Y

APPENDIX D - List of 3rd party data processors of LTT

a) Auditors
b) Aircall – integration with Pipedrive – name and phone number combined - based
c) External IT Providers
d) Payroll processors
e) HR advisory
f) Got to Webinar – all webinars
g) Legal advisers
h) Salesforce
i) Ringcentral
j) Kapow – manual upload – only phone numbers (salesforce)
k) Force 24
l) Calendly
m) Webinar Fuel
n) Click funnels
o) Integromat
p) Payment providers including but not limited to Chargebee and Stripe
q) Power BI
r) Pipedrive
s) Typeform (from waitlist)
t) Trengo
u) Go to webinar
v) Facebook forms
w) Brevo (previously Send in Blue)
x) Scoreapp (from DNA test on website)
y) Twillio
z) Zapier
aa) Zoom
bb) Supermetrics
cc) All other software, platforms and external consultants in the future

APPENDIX E- Retention Table

Category	Retention	DATA TYPE RETAINED	Unsubscribe Option	FREQUENCY OF PURGE
Advanced Digital Programme Customer	7 years from date of invoice	Documents required for audit e.g. invoices, receipts, payments history	**N**	**1 YEAR**
	6 years from date of enrolment on to programme	Salesforce customer information		
	6 years	Outlook 365 Default policy for e-mails		
	6 Months	Call Recordings		**Automatic deletion after 6 months**

Digital Programme Customer	7 years from date of invoice 6 years from date of enrolment on to programme 6 years 6 Months	Documents required for audit e.g. invoices, receipts, payments history Salesforce customer information Outlook 365 Default policy for e-mails Call recordings	**N**	**1 YEAR** **Automatic Deletion After 6 months**
STAFF	6 Years after employment ends or As long as necessary to fulfil the purposes we collected	Documents required for legal, accounting and reporting obligations or in respect to disputes. Data for fulfilling contractual obligations or necessary in	**N**	**1 YEAR**

	for, as required to satisfy any legal, accounting or reporting obligations or as necessary to resolve disputes.	course of employment		