Refund Policy for Distance Learning Courses

Refund Policy for Distance Learning Courses

Goods relating to purchases through World Pay by Credit / Debit Card or Cheque/Cash

Standard 14 days cancellation policy after making the payment for the course. Cancellation must be made in writing by letter or via email. The Customer must also return the Materials as soon as possible and at the Customer's own cost and risk. When doing so the Customer should state his / her name, address, student registration number and the reason for cancellation.

You the consumer are liable for all costs incurred in returning the goods.

Please return your goods to NLP Centre of Excellence ltd

A refund will be issued by cheque following the above protocol;

Please return your goods to NLP Centre of Excellence ltd

Recommends that the Customer gets a free proof of postage certificate from the Post Office or sends any parcel by Recorded Delivery.

Please return your goods to NLP Centre of Excellence ltd

Jubilee Rd, Middleton, Manchester M24 2LX

Regrets that it cannot be responsible for items which never reach NLP Centre of Excellence ltd ltd or those that are damaged in transit

Where a course has been purchased with a recognised third party provider Please return your goods to NLP Centre of Excellence ltd
LTD are not liable or responsible to issue any refunds and the policy of the organisation purchased from is to be adhered to

Refund Policy for classroom Courses

Cancellation

Standard 14 days cancellation policy after making the payment for the course. Cancellation must be made in writing by letter or via email. The Customer must also return the Materials as soon as possible and at the Customer's own cost and risk. When doing so the Customer should state his / her name, address, student registration number and the reason for cancellation

You the consumer are liable for all costs incurred in returning the goods.

Please return your goods to NLP Centre of Excellence ltd

A refund will be issued by cheque following the above protocol;

Please return your goods to NLP Centre of Excellence ltd

Recommends that the Customer gets a free proof of postage certificate from the Post Office or sends any parcel by Recorded Delivery.

Please return your goods to NLP Centre of Excellence ltd

Jubilee Rd, Middleton, Manchester M24 2LX

Regrets that it cannot be responsible for items which never reach NLP Centre of Excellence ltd ltd or those that are damaged in transit

Where a course has been purchased with a recognised third party provider Please return your goods to NLP Centre of Excellence ltd
LTD are not liable or responsible to issue any refunds and the policy of the organisation purchased from is to be adhered to

If, for any reason, you have to cancel an agreed booking after your 14 day cooling off period, this must be notified to us in writing, and the cancellation fees will apply as set out below:

Cancellations must be received in writing via email to i info@online-trainingcourses.com and must contain the full booking details including delegate and organisation name and contact details. Your cancellation will be confirmed in writing to the fee payer along with an invoice for any outstanding fees due.

Cancelling a course

The following charges will apply if you wish to cancel a course after 14 day cooling period:

For the period of 1 month prior to the course start date, no refund will be given on cancellations.

For the period of 1 month to 2 months prior to the course start date, a 50% refund is obtainable on cancellations.

Cancellations prior to 2 months in advance of the course start date, an 85% refund is obtainable.

Where at least 3 months' notice is given and a valid reason is given we offer a 100% refund less deposit.

Were applicable Examination fees will only be refunded if they have not already been paid to the relevant Examining Board..

Refunds will be paid by the same way they were paid, except for cash payments which will be refunded by cheque, within 28 days of authorisation of refund.

Once you have begun training we are strictly unable to offer any refund. Where multi module courses are booked the cooling off period for all of the modules / parts of the course begins on the first day of booking the first course or module. Where multi course parts and modules are booked the cancellation period begins on the first day of booking for the first course for all courses.

NLP Centre of Excellence reserves the right to cancel or reschedule seminars at any time. If NLP Centre of Excellence cancels or reschedules the seminar due to weather or unforeseen circumstances beyond the control of NLP Centre of Excellence, you are entitled to a full refund, but NLP Centre of Excellence is not responsible for travel arrangements, travel fees, or any expenses incurred by you as a result of such cancellation. If NLP Centre of Excellence cancels a seminar in which you are enrolled, you will be contacted at the email address you provided when registering, so please be sure to provide a valid email address.

This Policy sets out the obligations of NLP CENTRE OF EXCELLENCE LIMITED

Jubilee Rd, Middleton, Manchester M24 2LX

Company number 06424287

regarding data protection and the rights of The information will be used to help us process your learning and education registration, and other related purposes such as third party certificate awarding body registration process. And update learners on events and tutorials. NLP CENTRE OF EXCELLENCE LIMITEDrespects the right to privacy of its students and is committed to safeguarding the personal information of each student.in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR 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, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets the Company'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 the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company 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.

The Data Protection Principles

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

Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

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.

Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

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.

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 GDPR in order to safeguard the rights and freedoms of the data subject.

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.

The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

The right to be informed (Part 12).

The right of access (Part 13);

The right to rectification (Part 14);

The right to erasure (also known as the ‘right to be forgotten’) (Part 15);

The right to restrict processing (Part 16);

The right to data portability (Part 17);

The right to object (Part 18); and

Rights with respect to automated decision-making and profiling (Parts 19 and 20).

Lawful, Fair, and Transparent Data Processing

The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:

The data subject has given consent to the processing of their personal data for one or more specific purposes;

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 with them;

The processing is necessary for compliance with a legal obligation to which the data controller is subject;

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

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

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.

[If the personal data in question is “special category data” (also known as “sensitive personal data”) (for example, data concerning the data subject’s race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:

The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);

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 EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);

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;

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;

The processing relates to personal data which is clearly made public by the data subject;

The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;

The processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State 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;

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 EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;

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 EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

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 GDPR based on EU or EU Member State 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.]

Specified, Explicit, and Legitimate Purposes

The Company collects and processes the personal data set out in Part 21 of this Policy. This includes:

Personal data collected directly from data subjects[.] OR [; and]

[Personal data obtained from third parties.]

The Company only collects, processes, and holds personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the GDPR).

Data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

Adequate, Relevant, and Limited Data Processing

The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in Part 21, below.

Accuracy of Data and Keeping Data Up-to-Date

The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 14, below.

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.

Data Retention

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

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

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

Secure Processing

The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall

be taken are provided in Parts 22 to 27 of this Policy.

Accountability and Record-Keeping

The Company's Data Protection Officer Jimmy Petruzzi contact info@online-trainingcourses.com

The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other data protection-related policies, and with the GDPR and other applicable data protection legislation.

The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

The name and details of the Company, its Data Protection Officer, and any applicable third-party data processors;

The purposes for which the Company collects, holds, and processes personal data;

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;

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

Details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Policy); and

Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

Data Protection Impact Assessments

The Company 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 and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR].

Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

The type(s) of personal data that will be collected, held, and processed;

The purpose(s) for which personal data is to be used;

The Company's objectives;

How personal data is to be used;

The parties (internal and/or external) who are to be consulted;

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

Risks posed to data subjects;

Risks posed both within and to the Company; and

Proposed measures to minimise and handle identified risks.

Keeping Data Subjects Informed

The Company shall provide the information set out in Part 12.2 to every data subject:

Where personal data is collected directly from data subjects, those data subjects will be

informed of its purpose at the time of collection; and

Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

if the personal data is used to communicate with the data subject, when the first communication is made; or

if the personal data is to be transferred to another party, before that transfer is made; or

as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

The following information shall be provided:

Details of the Company including, but not limited to, the identity of its Data Protection Officer;

The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing;

Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;

Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

Where the personal data is to be transferred to one or more third parties, details of those parties;

Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the “EEA”), details of that transfer, including but not limited to the safeguards in place (see Part 28 of this Policy for further details);

Details of data retention;

Details of the data subject’s rights under the GDPR;

Details of the data subject’s right to withdraw their consent to the Company’s processing of their personal data at any time;

Details of the data subject’s right to complain to the Information Commissioner’s Office (the “supervisory authority” under the GDPR);

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

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.

Data Subject Access

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

Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to the Company’s Data Protection Officer at jimmypetruzzi@nlp-trainingcourses.com.

Responses to SARs shall 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.

All SARs received shall be handled by the Company’s Data Protection Officer.

The Company does not charge a fee for the handling of normal SARs. The Company 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.

Rectification of Personal Data

Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company 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.

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.

Erasure of Personal Data

Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

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

The data subject wishes to withdraw their consent to the Company holding and processing their personal data;

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

The personal data has been processed unlawfully;

The personal data needs to be erased in order for the Company to comply with a particular legal obligations

[The personal data is being held and processed for the purpose of providing information society services to a child.

Unless the Company 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.

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).

Restriction of Personal Data Processing

Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company 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.

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).

[Data Portability

The Company processes personal data using automated means The above information will be used to help us process education registration, and other related purposes such as third party certificate awarding body registration process. Respecting the right to privacy of its students and is committed to safeguarding the personal information of each student. .

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

To facilitate the right of data portability, the Company shall make available all applicable personal data to data subjects in the following format[s]:

Stored on device locked away safe

Back up and stored on devices locked away in safe

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

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.]

Objections to Personal Data Processing

Data subjects have the right to object to the Company processing their personal data based on legitimate interests, direct marketing (including profiling), [and processing for scientific and/or historical research and statistics purposes].

Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company'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.

Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.

[Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the GDPR, "demonstrate grounds relating to his or her particular situation". The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.]

[Automated Decision-Making

The Company uses personal data in automated decision-making processes. certificate registrations and updated of developments and events.

Where such decisions have a legal (or similarly significant effect) on data subjects, those data subjects have the right to challenge to such decisions under the GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Company.

The right described in Part 19.2 does not apply in the following circumstances:

The decision is necessary for the entry into, or performance of, a contract between the Company and the data subject;

The decision is authorised by law; or

The data subject has given their explicit consent.]

[Profiling

The Company uses personal data for profiling purpose candidate registration and updates.

When personal data is used for profiling purposes, the following shall apply:

Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling;

Appropriate mathematical or statistical procedures shall be used;

Technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and

All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 to 26 of this Policy for more details on data security).]

Personal Data Collected, Held, and Processed

The following personal data is collected, held, and processed by the Company (for details of data retention, please refer to the Company's Data Retention Policy):

Data Ref.	Type of Data	Purpose of Data
1	Registrations	third party certificate awarding body registration process.
2	Email addresses	Keep learners updated of events and tutorial

Data Security – Transferring Personal Data and Communications

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

All emails containing personal data must be encrypted All medium and high risk personal data or sensitive business information must be encrypted if it leaves the centre environment. The following key principles underpin the centre policy on the storage, transmission and use of personal data and sensitive business information outside the centre. All staff must comply with these principles when using mobile devices and portable storage media or otherwise removing information outside the centre. Avoid using personal data wherever possible.

Use the centres secure shared drives to store and access personal data and sensitive business information, ensuring that only those who need to use this information have access to it.

Use remote access facilities to access personal data and sensitive business information on the central server instead of transporting it on mobile devices or using third party hosting services.

If there is no option but to use mobile devices or email for high and medium risk personal data or sensitive business information, buy encrypted memory sticks, use encryption software, or encrypt the whole hard disk.

Do not use personal equipment (such as home PCs or personal USB sticks) or third party hosting services (such as Google Mail) for high or medium risk personal data or sensitive business information.

Avoid sending high or medium risk personal data or sensitive business information by email. If you must use email to send this sort of data outside the centre, encrypt it. If you are sending unencrypted high or medium risk personal data or sensitive business information to another University email account, indicate in the email title that the email contains sensitive information so that the recipient can exercise caution when opening it.

Do not use high or medium risk personal data or sensitive business information in public places.

When accessing your email remotely, exercise caution to ensure that you do not download unencrypted high or medium risk personal data or sensitive business information sensitive data to an insecure device.

Consider the physical security of high or medium risk personal data or sensitive business information, for example use locked filing cabinets/cupboards for storage.

Implement the centres retention and disposal policies so that you do not keep personal data and sensitive business information that you do not need. If there are no suitable retention and disposal policies in place for your area, arrange to put some in place

If the use of personal data is unavoidable, consider partially or fully anonymising the information to obscure the identity of the individuals concerned.

All emails containing personal data must be marked “confidential”;

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

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

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

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;

Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient

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”.

Data Security – Storage

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

All electronic copies of personal data should be stored securely using passwords and data encryption through software;

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;

All personal data stored electronically should be backed up daily with backups stored All backups should be encrypted using software

No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise [without the formal written approval of Jimmy Petruzzi jimmypetruzzi@nlp-trainingcourses.com 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]; and

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, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

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 the Company's Data Retention Policy.

Data Security – Use of Personal Data

The Company shall ensure that the following measures are taken with respect to the use of personal data:

No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from jimmy petruzzi jimmypetruzzi@nlp-trainingcourses.com

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 jimmy petruzzi jimmypetruzzi@nlp-trainingcourses.com

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

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; and

Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of jimmy petruzzi info@online-trainingcourses.com 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.

Data Security – IT Security

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

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

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

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

No software may be installed on any Company-owned computer or device without the prior approval of the jimmy petruzzi info@online-trainingcourses.com

Organisational Measures

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

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

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

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

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

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

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

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

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

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

All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the GDPR; and

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

Transferring Personal Data to a Country Outside the EEA

The Company may from time to time transfer (‘transfer’ includes making available remotely) personal data to countries outside of the EEA.

The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;

The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner’s Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

The transfer is made with the informed consent of the relevant data subject(s);

The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);

The transfer is necessary for important public interest reasons;

The transfer is necessary for the conduct of legal claims;

The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

Data Breach Notification

All personal data breaches must be reported immediately to the Company's Data Protection Officer.

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 it.

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 29.2) 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.

Data breach notifications shall include the following information:

The categories and approximate number of data subjects concerned;

The categories and approximate number of personal data records concerned;

The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);

The likely consequences of the breach;

Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Implementation of Policy

This Policy shall be deemed effective as of 20th of May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

The current legal requirements for website cookies and similar technologies stem from the Privacy and Electronic Communications (EC Directive) Regulations 2003 and, as of 25 May 2018, from the European General Data Protection Regulation 2016 (“GDPR”).

Privacy online is of great importance, all the more so in light of the GDPR which represents the single greatest step forward in privacy legislation since the Data Protection Act of 1998; a piece of legislation which was crafted before the advent (or at least the rise) of many forms of data collection and usage that are commonplace today, particularly online.

This website, www.nlp-trainingcourses.com ("Our Site") uses Cookies and similar technologies in order to distinguish you from other users. By using Cookies, We are able to provide you with a better experience and to improve Our Site by better understanding how you use it. Please read this Cookie Policy carefully and ensure that you understand it. Your acceptance of Our Cookie Policy is deemed to occur if you continue using Our Site. If you do not agree to Our Cookie Policy, please stop using Our Site immediately.

All Cookies used by and on Our Site are used in accordance with current Cookie Law. We may use some or all of the following types of Cookie:

Strictly Necessary Cookies

A Cookie falls into this category if it is essential to the operation of Our Site, supporting functions such as logging in, your shopping basket, and payment transactions.

Analytics Cookies

It is important for Us to understand how you use Our Site, for example, how efficiently you are able to navigate around it, and what features you use. Analytics Cookies enable us to gather this information, helping Us to improve Our Site and your experience of it.

Functionality Cookies

Functionality Cookies enable Us to provide additional functions to you on Our Site such as personalisation and remembering your saved preferences. Some functionality Cookies may also be strictly necessary Cookies, but not all necessarily fall into that category.

Targeting Cookies

It is important for Us to know when and how often you visit Our Site, and which parts of it you have used (including which pages you have visited and which links you have visited). As with analytics Cookies, this information helps us to better understand you and, in turn, to make Our Site and advertising more relevant to your interests.

Third Party Cookies

Third party Cookies are not placed by Us; instead, they are placed by third parties that provide services to Us and/or to you. Third party Cookies may be used by advertising services to serve up tailored advertising to you on Our Site, or by third parties providing analytics services to Us

(these Cookies will work in the same way as analytics Cookies described above).

Persistent Cookies

Any of the above types of Cookie may be a persistent Cookie. Persistent Cookies are those which remain on your computer or device for a predetermined period and are activated each time you visit Our Site.

Session Cookies

Any of the above types of Cookie may be a session Cookie. Session Cookies are temporary and only remain on your computer or device from the point at which you visit Our Site until you close your browser. Session Cookies are deleted when you close your browser.

Cookies on Our Site are not permanent and will expire.

For more details of the personal data that We collect and use, the measures we have in place to protect personal data, your legal rights, and our legal obligations, please refer to our Privacy Policy