CTSP – CONFIDENTIALITY AND PRIVACY POLICY

Policy Statement

The College of Trichological Science and Practice CIC (CTSP) is committed to the delivery of quality assured education and training in the field of trichology and related sectors. Under data protection law, individuals have a right to be informed about how CTSP uses any personal data that it holds about them. CTSP comply with this right by providing policies, procedures and 'privacy notices' (sometimes called 'fair processing notices') to inform individuals (data subjects) where we are processing their personal data and to meet the requirements of the General Data Protection Regulations (GDPR) which came into effect on 25 May 2018 and supersedes the Data Protection Act 1998.

CTSP Confidentiality and Privacy Policy states that:

CTSP will provide learners with the guidance and information they need to sign the ongoing confidentiality agreement with CTSP and will outline the principles of Data Protection as set out by General Data Protection Regulation (EU) 2016/679 ('GDPR') (May 25th, 2018).

Definition of Confidential Information and Personal Data

For the purposes of this policy, Confidential Information is:

- information, in whatever form obtained or maintained (including written, oral, visual and electronic), relating to any learner or, in anyway, pertaining to the business undertakings and operation of CTSP
- analyses, compilations, studies and other documents or materials which contain or otherwise reflect or are derived/generated from any information described above.

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.

The GDPR 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 considered to 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 GDPR 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.

The GDPR 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.

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:

a. the data subject has given consent to the processing of his or her 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 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 controller;
f. The 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, in particular where the data subject is a child.
g. 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:
h. 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);
i. 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 or 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);
j. The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject if physically or legally incapable of giving consent;
k. The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing s 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;
l. The processing relates to personal data which is clearly made public by the data subject;
m. The processing is necessary for the conduct of legal claims or whenever courts are acting in the judicial capacity;
n. The processing is necessary for the 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;

o. The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medicine 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;

p. 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

q. 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 specific measures to safeguard the fundamental rights and the interests of the data subject.

Specified, Explicit and Legitimate Purposes

CTSP collects and processes certain personal data. 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.

CTSP only collects, processes and holds personal data for the specific purposes set out in 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 CTSP uses their personal data.

Adequate, Relevant and Limited Data Processing

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

Accuracy of Data and Keeping Data Up to Date

CTSP 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.

The accuracy of personal 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.

Data Retention

CTSP 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. For details of CTSP's approach to data retention, including retention periods for specific personal data types held by CTSP, please refer to our **Data Retention Policy and Procedures**.

Secure Processing

CTSP 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.

Accountability and Record-Keeping

CTSP 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 CTSP, and any applicable third-party data processors;
b. The purposes for which CTSP collects, holds and processes personal data;
c. Details of the categories of personal data collected, held, and processed by CTSP; and the categories of data subject to which that personal data relates;
d. Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
e. Details of how long personal data will be retained by CTSP (please refer to our Data Retention Policy and Procedures.); and
f. Detailed descriptions of all technical and organisational measures taken by CTSP to ensure the security of personal data.

Data Protection Impact Assessments

CTSP 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 CTSP's Management Team 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. How personal data is to be used;
d. The parties (internal and/or external) who are to be consulted;
e. The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
f. The risks posed to individual data subjects;
g. Risks posed to both within and to CTSP; and
h. Proposed measures to minimise and handle identified risks.

Keeping Data Subjects Informed

Where personal data is collected directly from data subjects, 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 purposes:

a. If the personal data is used to communicate with the data subject, when the first communication is made; or
b. If the personal data is to be transferred to another party, before that transfer is made; or
c. As soon as reasonably possible and in any event not more than one month after the personal data is obtained.
d. The following information shall be provided:
e. Details of CTSP including, but not limited to, the identity of its Management Team;
f. The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;
g. Where applicable, the legitimate interests upon which CTSP is justifying its collection and processing of the personal data;
h. Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
i. Where the personal data is to be transferred to one or more third parties, details of those parties;
j. 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;
k. Details of data retention;

l. Details of the data subject's rights under the GDPR;
m. Details of the data subject's right to withdraw their consent to CTSP's processing of their personal data at any time;
n. Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the GDPR);
o. 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;
p. 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.

Data Subject Access Request Form
A data subject may make a subject access request ("SARs") at any time to find out more about the personal data which CTSP holds about them, what it is doing with that personal data, and why.

Data subjects wishing to make a SAR may do so in writing, using CTSP's Subject Access Request Form, or other written communication. SARs should be addressed to CTSP's Management Team.

CTSP 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). CTSP does not charge a fee for the handling of normal SARs.

CTSP 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 CTSP to rectify any of their personal data that is inaccurate or incomplete.

CTSP shall rectify the personal data in question and inform the data subject of that rectification, within one month of the data subject informing CTSP of the issue. The period can be extended by up to two months in the case of complex requests, and in such cases 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 CTSP erases the personal data it holds about them in the following circumstances:
a. It is no longer necessary for CTSP 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 CTSP holding and processing their personal data;

c. The data subject objects to CTSP holding and processing their personal data (and there is no overriding legitimate interest to allow CTSP to continue doing so);
d. The personal data has been processed unlawfully;
e. The personal data needs to be erased in order for CTSP to comply with a particular legal obligation.

Unless CTSP 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).

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).

Restriction of Personal Data Processing

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

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).

Objections to Personal Data Processing

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

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

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

Where a data subject objects to CTSP 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'. CTSP 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

In the event that CTSP 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 GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from CTSP.

The right described as above does not apply in the following circumstances:

a. The decision is necessary for the entry into, or performance of, a contract between CTSP and the data subject;
b. The decision is authorised by law; or
c. The data subject has given their explicit consent.

Profiling

CTSP may use personal data for profiling purposes. When personal data is used for profiling purposes, the following shall apply:

a. Clear information explaining the profiling shall be provided to data subjects, including its significance and the likely consequences;
b. Appropriate mathematical or statistical procedures will be used;
c. Technical and organisational 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.

Personal Data Collected, Held and Processed

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

a. Basic details such as name, date of birth and contact details (address, phone numbers and email address), for the purpose of identifying each learner, for future correspondence we may send out (e.g. newsletters, event updates and special offers);
b. Details of contact we have had with you, when you have attended a training and queries you have made;
c. Details of training you have attended, for the purpose of providing further support and advise;
d. Learners experience feedback, for the purpose of carrying out statistics and improving our education provision;
e. Information about complaints and incidents, for the purpose of investigating and improving our procedures;
f. Notes and records about any treatment you carried out during your training, for the purpose of providing you with post-course support;
g. Information from customer surveys, competitions and marketing activities, for the purpose of improving the services provided, contacting you with the latest offers and events we are having;
h. Other information we received from other sources including, GMC, insurance companies who have obtained your permission to share information about you, for the purpose of allowing you to carry out treatments.

Security – Transferring Personal Data and Communications

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

a. All emails containing personal data must be encrypted
b. All emails containing personal data must be marked “confidential”;
c. 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, and electronic copies should be deleted securely.
d. Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
e. Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
f. 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;
g. Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Royal Mail and ask for proof of sending;
h. All personal data to be transferred physically, whether in hardcopy corm or on removable electronic media shall be transferred in a suitable container marker “confidential”.

Data Security – Storage

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

a. All electronic copies of personal data should be stored securely using passwords and data encryption;
b. 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;
c. All personal data stored electronically should be backed up at the end of each working day, with backups stored in secure drive (or drop box) and on a weekly basis stored on a secure medium. All backups should be encrypted which are compressed in a zip file and are password protected.
d. No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to CTSP or otherwise without the formal written approval of the Management Team 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.
e. 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 CTSP 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 CTSP 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 or personal data, please refer to CTSP's Data Retention Policy and Procedures.

Data Security – Use of Personal Data

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

a. No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of CTSP requires access to any personal data that they do not already have access to, such access should be formally requested from Management Team.
b. No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of CTSP or not, without the authorisation of Management Team;
c. 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;
d. 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;
e. Where personal data held by CTSP is used for marketing purposes, it shall be the responsibility of the Management Team 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 and the Email Preference Service. Such details should be checked at least every six months.

Data Security – IT Security

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

a. 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 CTSP is designed to require such passwords;
b. Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of CTSP, 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;

c. All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. CTSP'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
d. No software may be installed on any Company-owned computer or device without the prior approval of the Management Team.

Organisational Measures

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

a. All employees, agents, contractors, or other parties working on behalf of CTSP shall be made fully aware of both their individual responsibilities and CTSP's responsibilities under the GDPR 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 CTSP 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 CTSP;
c. All employees, agents, contractors, or other parties working on behalf of CTSP handling personal data will be appropriately trained to do so;
d. All employees, agents, contractors, or other parties working on behalf of CTSP handling personal data will be appropriately supervised;
e. All employees, agents, contractors, or other parties working on behalf of CTSP 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;
f. Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;
g. The performance of those employees, agents, contractors, or other parties working on behalf of CTSP handling personal data shall be regularly evaluated and reviewed;
h. All employees, agents, contractors, or other parties working on behalf of CTSP handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;
i. All agents, contractors, or other parties working on behalf of CTSP 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 CTSP arising out of this Policy and the GDPR; and
j. Where any agent, contractor or other party working on behalf of CTSP handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless CTSP against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

Transferring Personal Data to a Country Outside the UK

CTSP may be required from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the UK. The transfer of personal data to a country outside of the UK shall take place only if one or more of the following applies:

a. 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;
b. 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;

c. The transfer is made with the informed consent of the relevant data subject (s);
d. The transfer is necessary for the performance of a contract between the data subject and CTSP (or for pre-contractual steps taken at the request of the data subject);
e. The transfer is necessary for important public interest reasons;
f. The transfer is necessary for the conduct of legal claims;
g. 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
h. 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 CTSP Management Team. 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 Management Team 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 as above) to the rights and freedoms of data subjects, the Management Team 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:

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

Review arrangements

CTSP will review this policy annually and revise it as and when necessary in response to changes in practice, actions from the regulatory authorities or external agencies or changes in legislation.

If you would like to express any views on this policy, please contact our Quality Assurance manager via email to admin@ctsp.ac.uk.

Related Documents

Subject Access Request Form
Confidentiality and Privacy Policy
Data Retention Policy