Name of Policy: Data Protection Policy Category of Policy: **Status:** Draft **Approved by:** Trustees **Date:** 10 October 2020 **Review date:** 10 October 2021	CAMBRIDGESHIRE CONSULTANCY IN COUNSELLING *Registered Charity 1181861*

Data Protection Policy

1. POLICY STATEMENT

1.1 During the course of our activities, Cambridgeshire Consultancy in Counselling ('the Charity') as the data controller will process personal information and we recognise the need to treat it in an appropriate and lawful manner.

1.2 This policy sets out how the Charity and its staff handle the personal data of our customers, suppliers, business contacts, employees, workers and other individuals that the Charity has a relationship with. In processing personal data, the Charity will comply with the General Data Protection Regulation and the Data Protection Act 2018 (together the 'Data Protection Legislation').

2. STATUS OF THE POLICY

2.1 This policy must be complied with by all staff working for the Charity (including, employees (whether permanent, fixed term or temporary), self-employed personnel, volunteers and agency workers).

2.2 This policy is non-contractual, and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action up to and including dismissal.

2.3 Any questions or concerns about the operation of this policy should be referred in the first instance to Judie Jones at director@ccc-counselling.org.uk.

3. DEFINITIONS

3.1 **Consent:** agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the processing of personal data relating to them.

3.2 **Data Subject:** for the purpose of this policy include all living, identified or identifiable individuals about whom we hold personal data. A data subject need not be a UK national or resident.

3.3 **Explicit Consent:** consent which requires a very clear and specific statement.

3.4 **Personal Data:** data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

3.5 **Processing or Process**: any activity that involves use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.6 **Special Category Data:** information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and personal data relating to criminal offences and convictions.

4. THE DATA PROTECTION PRINCIPLES

4.1 All staff processing personal data must comply with the data protection principles. These provide that personal data must be:

(a) Processed lawfully, fairly and in a transparent manner;
(b) Collected only for specified, explicit and legitimate purposes;
(c) Adequate, relevant and limited to what is necessary in relation to the proposes for which it is processed;
(d) Accurate and where necessary kept up to date;
(e) Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed;
(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage;
(g) Not transferred to another country without appropriate safeguards being in place; and
(h) Made available to data subjects and allow data subjects to exercise certain rights in relation to their data.

4.2 *We will demonstrate compliance with the data protection principles.*

5. LAWFULNESS, FAIRNESS AND TRANSPARENCY

5.1 **Lawfulness and fairness:** For personal data to be processed lawfully, certain conditions have to be met.

In most circumstances, the Charity will rely upon the following conditions for processing personal data:

(a) the data subject has consented to the processing;
(b) the processing is necessary for our legitimate interests;
(c) the processing is necessary for the performance of a contract; and/or
(d) the processing is conducted to meet our legal obligations.

Further information on the processing of personal data is set out in our Privacy Notices available from director@ccc-counselling.org.uk.

5.2 **Consent:** A data subject consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing.

Usually we will be relying on another legal basis (and not require explicit consent) to process most types of special category data.

Where consent is given, you will be able to easily withdraw your consent at any time. Consent may need to be refreshed if we intend to process personal data for a different and incompatible purpose which was not disclosed when you first consented.

5.3 **Transparency:** Whenever we collect personal data directly from data subjects, including for HR or employment purposes, we will provide the data subject with specific information including:

(a) that we are the data controller; and
(b) how and why we will process that personal data.

This is provided through a Privacy Notices available from director@ccc-counselling.org.uk.

When personal data is collected indirectly (for example, from a third party or publicly available source), we will provide the data subject with all the information required by the Data Protection Legislation as soon as possible after collecting/receiving the data.

6. PROCESSING FOR LIMITED PURPOSES

6.1 Personal data may only be processed for the specified, explicit and legitimate purposes. This means that personal data must not be collected for one purposes and used for another unless we have informed the data subject of the new purpose(s).

6.2 Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. You may only process personal data that you require for your job duties.

6.3 We process personal data to enable us to:

(a) Provide marketing, advertising and public relation services to our clients;
(b) Maintain our accounts and record;
(c) Promote our services;
(d) Undertake research; and
(e) Support and manage employees.

6.4 We will ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised.

7. ACCURATE DATA

We will ensure that personal data we hold is accurate and where necessary, kept up to date. We will take steps to ensure the accuracy of the data held at regular intervals and take reasonable steps to destroy or amend inaccurate or out of date data.

8. TIMELY PROCESSING

8.1 We will not keep personal data in an identifiable form for longer than is necessary for the purposes for which the data was gathered. We will take all reasonable steps to ensure that data is destroyed or erased from our systems when it is no longer required, unless a law requires such data to be kept for a minimum time. This includes requiring third parties to delete such data where applicable.

8.2 To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of data subjects' personal data, the purposes for which we process their personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

8.3 In some circumstances we may anonymise personal data (so that it can no longer be associated with the data subject) for research or statistical purposes in which case we may use this information indefinitely without further notice to the data subject.

9. DATA SECURITY

9.1 We will ensure that appropriate security measures appropriate to the size, scope and available resources of our business are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

9.2 We will regularly evaluate the effectiveness of the safeguards put in place. Personal data may only be transferred to a third-party data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures. We will exercise particular care in protecting special category personal data.

9.3 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it.
(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
(c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

9.4 **Security procedures include:**

(a) **Entry controls.** Any stranger seen in entry-controlled areas should be reported.

(b) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(c) **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required by giving them to the IT Department.

(d) **Equipment.** Staff should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

(e) **Password Protection/Encryption.** Personal data held on computers must be stored confidentially by means of password protection and encryption. Each employee has a password to access the system and these passwords are not held anywhere.

(f) **System protection.** Antivirus software is installed on computers and the server and this is updated automatically when a new version is available.

10. DISCLOSURE OF PERSONAL INFORMATION INCLUDING THE TRANSFER OF PERSONAL DATA TO A COUNTRY OUTSIDE THE EUROPEAN ECONOMIC AREA ("EEA")

10.1 We may also disclose personal data we hold to third parties:

(a) In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.

(b) If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

(c) If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; to protect our rights, property, or safety of our employees, customers, or others; or to comply with a request of a regulator. This includes exchanging information with other companies and organisations for the purposes of fraud protection and debt collection.

(d) To undertake surveys and research.

10.2 We may only share the personal data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the personal data complies with the privacy notice provided to the data subject and, if required, the data subject's consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer restrictions; and

(e) a fully executed written contract that contains Data Protection Legislation approved third party clauses has been obtained (where appropriate and necessary).

10.3 We may transfer any personal data we hold to a country outside the EEA, provided that one of the following conditions applies:

(a) The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.

(b) The data subject has given his explicit consent.

(c) The transfer is necessary for one of the reasons set out in the Data Protection Legislation, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.

(d) Appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism.

(e) The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

11. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

11.1 Data subjects have rights when it comes to how we handle their personal data. These include rights to:

(a) withdraw consent to processing;

(b) receive certain information about our processing activities;

(c) request access to their personal data that we hold;

(d) prevent our use of their personal data for direct marketing purposes;

(e) ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict processing in specific circumstances;

(g) challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which personal data is transferred outside of the EEA;

(i) object to decisions based solely on automated processing, including profiling;

(j) prevent processing that is likely to cause damage or distress to the data subject or anyone else;

(k) be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to the supervisory authority; and

(m) in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

Some of these rights are not automatic.

11.2 You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing personal data without proper authorisation).

11.3 If a data subject wishes to exercise a right, you must immediately forward the request you receive to Judie Jones at director@ccc-counselling.org.uk.

12. REPORTING A PERSONAL DATA BREACH

12.1 The Charity has put in place procedures to deal with any suspected personal data breach (i.e. the loss, or unauthorised access, disclosure or acquisition, of personal data), and will notify the data subject or any applicable regulator where it is legally required to do so.

12.2 If a member of staff knows or suspects that a personal data breach has occurred or may occur, they should not attempt to investigate the matter themselves. They should immediately contact Judie Jones on director@ccc-counselling.org.uk and preserve all evidence relating to the potential personal data breach.

13. ACCOUNTABILITY, TRAINING AND RECORD-KEEPING

13.1 The Charity has adequate resources and controls in place to ensure and to document data protection compliance including:

(a) implementing Privacy by Design when processing personal data and completing privacy impact assessments where processing presents a high risk to rights and freedoms of data subjects;

(b) integrating data protection into internal documents including this policy, related policies and privacy notices;

(c) regularly training relevant staff on the Data Protection Legislation, this policy, related policies and data protection matters including, for example, data subject's rights, consent, legal basis, privacy impact assessments and personal data breaches; and

(d) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

13.2 We will keep and maintain accurate corporate records reflecting our processing including records of data subjects' consents and procedures for obtaining consents.

14. AUTOMATED PROCESSING AND AUTOMATED DECISION-MAKING

Automated Decision-Making is where a decision is made based on the automatic processing of personal data which significantly affects an individual. The Charity does not take any decisions using automated means. However, it will notify you in writing if this position changes.

15. MONITORING AND REVIEW OF THE POLICY

We reserve the right to change this policy at any time without notice to you. This policy is reviewed annually by the Trustees to ensure it is achieving its stated objectives.