PRIVACY POLICY FOR CUSTOMERS

CIC appreciates the trust you place in us when sharing your personal data. The security of that data is very important to us. This privacy policy explains how we collect, use and look after your personal data.

We will explain what rights you have with regards to your personal data and how you can exercise those rights.

WHO WE ARE

CNLR is a limited company and trades under the name of CiC. We provide employee assistance programmes to organisations which includes services to be utilised by employees, such as 24/7 Advice Line and counselling support. We offer international services such as global trauma support and peer and professional support programmes and critical incident support. We also offer mediation, training and coaching sessions.

COLLECTION OF PERSONAL DATA

Definitions:

For the purposes of this policy CiC is the Data Controller and:

- A customer is the legal entity we contract with;
- A client includes the employee, partner of an employee or family member of an employee belonging to the customer we contract with;
- An affiliate is a contractor who delivers our counselling and support services on our behalf;
- Third party professional services are a third party that we share your data with in order to deliver critical services to you e.g. GPs and other medical professionals or legal advisors;
- Third party processors are a third party service provider who undertake data processing activities on our behalf e.g. IT support services.

We collect personal data from you for one or more of the following purposes:

- To provide you with information that you have requested or which we think may be relevant to a subject in which you have demonstrated an interest;
- To initiate and complete commercial transactions with you, or the entity that you represent, for the purchase of products and/or services;
- To fulfil a contract that we have entered into with you or with the entity that you represent;
- To ensure the security and safe operation of our websites and underlying business infrastructure, and
- To manage any communication between you and us.

Table 1 below provides more detail about the data that we collect for each of these purposes and the lawful basis for doing so.

LAWFUL BASIS FOR PROCESSING OF PERSONAL DATA

The table below describes the various forms of personal data we collect and the lawful basis for processing this data. We have processes in place to ensure that only those people in our organisation who need to access your data can do so. A number of data elements are collected for multiple purposes, as the table below shows. Some data may be shared with third parties and, where this happens, this is also identified below.

When we process on the lawful basis of legitimate interest, we apply the following test to determine whether it is appropriate:

The purpose test – is there a legitimate interest behind the processing?

Necessity test – is the processing necessary for that purpose?

Balancing test – is the legitimate interest overridden, or not, by the individual's interests, rights or freedoms?

TABLE 1

Data processed	Purpose for processing	Lawful basis	Data is shared with
Customers and potential customers: Company name Address Contact First Name Contact Last Name Contact Emails Telephone numbers	To provide and manage the services the customer has requested or to enable us to communicate with them regarding the services they are interested in. We store this data in our CRM database. We also store this data in our accounts system for accounting purposes.	**Legitimate interest:** where it is in our legitimate interests to manage our customer relationship and provide a high level of service, to protect our business interests and the interests of our customers. To carry out our contractual agreement or take steps to enter into a contract with the customer. Where the law requires it.	Internally and may be shared with affiliate counsellors.
Customers: Contact First Name Contact Last Name Contact Email	To send the customer monthly help sheets and promotion of Well-online. We store this data in spreadsheets, our database and Mailchimp.	**Legitimate interest:** where it is in our legitimate interests to manage our customer relationship and provide a high level of service To carry out our contractual obligation to send the customer help sheets.	Internally and Mailchimp

Customers, potential customers: Company name Address Contact First Name Contact Last Name Contact Email Telephone numbers	To handle enquiries and complaints. We may store this data in our CRM, or email system.	**Legitimate interest:** where it is in our legitimate interests to manage our customer relationship and provide a high level of service, to respond to enquiries and to ensure complaints are investigated promptly and satisfactorily.	Internally and may be shared with affiliate counsellors if necessary.
Customer, potential customer: Company name Address Contact First Name Contact Last Name Contact Email Telephone numbers	To communicate with the customer/potential customer by email, phone, post or other digital methods. For example: • to manage customer and supplier relationships • for the purpose of meeting contractual or regulatory requirements • to keep the customer informed of changes or updates to their services • to respond to an enquiry through our contact us form on our website	**Legitimate interest:** where it is in our legitimate interests to do so, to manage our customer relationship and provide a high level of service, to protect our business interests and the interests of our clients. Where the law requires it.	Internally and may be shared with affiliate counsellors or other third party service providers.

	We keep records of communication in our CRM, or email system.		
Customers: Company name Address Contact First Name Contact Last Name Position Contact Email Telephone numbers	To contact the customer with marketing information and offers relating to the products and services offered by us that we think may be of interest. We store this data in our CRM, and email system. This data may also be processed through Mailchimp.	**Legitimate interest:** where the customer has purchased our services or requested information about our goods and services. Where the customer has opted-in to receiving marketing information. In relation to direct digital marketing - under the Privacy and Electronic Communications Regulations, if the organisation is a limited company, we may send marketing communications without their consent. However, they can still opt out of receiving marketing emails from us at any time by clicking on the unsubscribe link.	Internally and with third party service providers e.g. Mailchimp
Customers: Company name, Address, Contact First Name Contact Last Name Contact email address, Telephone number	To process financial transactions for products and services and to ensure any transaction issues can be dealt with. The majority of this data is generic company accounts and contains no personal identifying Information. To meet	**Legitimate interest:** where it is in our legitimate interest to ensure our business is run with due diligence. **Legal obligation:** to fulfil our statutory obligations.	Internally and with professional advisors e.g. accountants

Bank account details	accounting and taxation requirements.		
Customers: Company name, Address, Contact First Name Contact Last Name Contact email address, Telephone number Bank account details	To recover any debts owed to us and enforce other obligations we are entitled to under contract and to protect ourselves against harm to our rights and property interests. We keep records of communication in our CRM database, filing system and accounts system.	**Legitimate interest:** where it is in our legitimate interest to ensure our business is run with due diligence and we are capable of recovering the debts owed to us.	Internally and professional advisors e.g. solicitors
Customers: Company Name, Directors names Physical address, Email address, telephone number, Bank account details (for credit accounts).	To undertake checks for the purposes of detecting and preventing fraud, and money laundering, to verify the customer's identity and credit worthiness before providing services to them.	**Legitimate interest:** where it is in our legitimate interest to detect and prevent fraud, money laundering and other crimes and to verify your identify in order to protect our business. **Legal obligation:** Where the law requires it.	Internally and third party service providers e.g. credit checks companies

SPECIAL CATEGORY DATA

Special category data is defined under GDPR 2016 Article 9 as personal data revealing ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Health data is collected as part of case notes and is necessary in order to provide the service. The basis for processing health data is legitimate interest as you, the client, makes an informed decision to self-refer to the service requested and would have a reasonable expectation that case notes must be maintained in order to provide the support and services. On this basis all case notes are held for 7 years in line with ……

We only collect special category data that falls within the equality and diversity data listed in Table 1 for the purposes recorded. We only collect equality and diversity data with the individual's consent.

THIRD PARTIES SERVICE PROVIDERS WHO WE MAY SHARE YOUR DATA WITH OR WHO COULD POTENTIALLY HAVE ACCESS (AS DEFINED IN TABLE 1)

- **Government and law enforcement agencies:** We may be required by law to share your data with other organisations, such as government or law enforcement agencies:
    - to satisfy any applicable law, regulation, legal process, or governmental request;
    - to detect, prevent, or otherwise address fraud, security, or technical issues;
    - protect our rights, property or safety, our users and the public.

    This may include exchanging information with other companies and organisations for fraud protection and spam/malware prevention if required by law.

- Professional advisors including lawyers, bankers, auditors and insurers.

    Third parties to whom we sell, transfer, or merge parts of our business or our assets.

If we do share data with third parties, we always do so securely, and we won't share more than we need to.

- Service providers who provide IT and system hosting services that could be defined as 'data processors' under GDPR. Generally, these service providers do not have access to data but as they host or manage the servers on which the data resides there is potential, in exceptional circumstances, where the data could be accessed e.g. during disaster recovery. All such service providers are thoroughly vetted and have stringent access controls in place.

Our service providers: we have listed in Table 2 service providers who are providing services that makes them 'processors' as defined by GDPR 2016. We will always ensure they follow similarly high standards to CiC and are bound by contractual confidentiality, data protection and information security requirements.

TABLE 2

Service provider	Purpose of processing	Link to Privacy Policy
Mailchimp	Provides marketing mail portal	https://mailchimp.com/legal/privacy/?_ga=2.2884912.1025376997.1527161488-2091482877.1526982076
Connect Assist	Out of hours call centre	https://www.connectassist.co.uk/privacy-policy/
Workbooks CRM	Cloud based CRM	https://www.workbooks.com/sites/default/files/_assets/pdf/legal/privacy-notice.pdf
ACM Solutions	Manages the hosted virtual server for CiCiS. Coders for CiCis clinical database.	Awaiting new website.
Our IT Department	Provides IT services. Manages IT infrastructure	https://www.ouritdept.co.uk/wp-content/uploads/2018/05/OurITDept-Privacy-Policy.pdf
Law Express	Provides legal advice	https://lawexpress.co.uk/privacy-policy

KTEG (Everyday Matters)	Personal Concierge Service	
True Bearing/ Bread & Butter Advice	Financial Guidance	https://www.truebearing.co.uk/data-security-policy/
PayPlan	Provides debt advice and solutions	https://www.payplan.com/legal/privacy-policy/

YOUR RIGHTS

The GDPR aims to give you more control of your data. It provides new and strengthened rights.

Right to access – you can ask us whether we're processing your personal data, including where and for what purpose. You can also request an electronic copy of your personal data free of charge. If you require further copies of the data there may be a charge where permitted by the legislation.

Right to restrict processing – in certain circumstances, you can ask us to restrict our use of your personal data.

Right to rectification – you can ask us to correct inaccurate personal data we hold about you.

Right to erasure (right to be forgotten) – in certain circumstances, you can ask us to erase your personal data.

Right to data portability – you can ask us to provide you with a copy of your personal data in a commonly used electronic format so that you can transfer it to other businesses.

Right to object to automated decision-making – in certain circumstances, you can ask us not to make automated decisions about you based on your personal data that produce significant legal effects.

Right to object to automated decision-making – in certain circumstances, you can ask us not to make automated decisions about you based on your personal data that produce significant legal effects.

Right to lodge a complaint – you can lodge a complaint with the supervisory authority ICO but we ask that you allow us to see if we can resolve the problem first (See complaints and queries section).

This means you can at any time:

- inform us of a correction to your personal data;
- withdraw any permission you have previously given to allow us to use your information in certa;
- object to any automated decision-making;
- ask us to stop or start sending you marketing messages;
- ask us to send you (or someone you nominate) a copy of the information we hold about you;
- ask us to stop using your information in certain circumstances.

DATA SUBJECT ACCESS REQUEST (DSAR)

You have the right to request a copy of the personal data we hold about you and to have any inaccuracies corrected. We will require you to prove your identity with 2 pieces of approved identification. We will use reasonable efforts consistent with our legal duty to supply, correct or delete personal information about you on our files.

We will need two copies of forms of identification, which can be: passport, driving licence, birth certificate, utility bill (from last 3 months), current vehicle registration document or a bank statement (from last 3 months).

If you can advise of the specific information that you require, we can process your request more quickly. We will respond to your request within one month of you providing information that confirms your identity.

We will then give you a description of your data, why we have it, who it could be disclosed to and it will be in a format that you can access easily.

If you wish to make a DSAR request please contact us using the contact details at the end of this notice and we will provide you with the necessary request documents.

RETENTION OF YOUR DATA

We will keep your data for as long as we have a relationship with you. Once our relationship has come to an end we will only retain your personal data for a period of time that is calculated depending on the type of personal data and the purposes for which we hold that data. We maintain a Retention of Records Schedule to communicate our record retention requirements to all relevant staff and ensure data is not retained for longer than necessary.

We only retain information that enables us to:

- maintain business records to comply with our contractual obligations
- comply with record retention requirements under the law
- defend or bring any existing or potential legal claims
- maintain records of anyone who does not want to receive marketing from us
- deal with any future complaints regarding services we have delivered
- if required to by law enforcement agencies

HOW WE PROTECT YOUR PERSONAL DATA

We are committed to protecting your information. CiC are certified to the ISO 27001 Information Security Standard. We take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of your personal data and against accidental loss or destruction of, or damage to, your personal data.

The measures we use are designed to provide a level of security appropriate to the risk of processing your personal information. However, please bear in mind that IT infrastructure and the internet cannot be guaranteed to be 100% secure. We have security measures in place and restrict access to databases only to those who need access appropriate to their job role.

All personal information and details provided as part of an enquiry, support or service request, or financial details are stored on a secure server. We do not store credit card numbers or related identifying information on any of our servers.

Digital data and hard copy data is securely disposed of when no longer required. This is conducted in line with our information security Disposal of Data Policy and procedure.

CHANGES TO THIS PRIVACY POLICY

We keep our privacy policy under regular review. This privacy policy was last updated on 25th May 2018.

QUERIES OR COMPLAINTS

We try to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously. Please get in touch if you think we are using or collecting your data in an inappropriate way.

You can call us on 020 7938 0992 and ask to be referred to the DPO or Client Services Manager;
or you can email dpo@cic-eap.co.uk or you can write to us at the address listed at the beginning of this document.

You can also contact or make a complaint directly to the supervisory body for the UK. This is the Information Commissioners Office (ICO)
You can visit their website at: https://ico.org.uk/
Or contact them on: 0303 123 1113

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	Guy Outram	25/05/2018
2	Added clarification on the types of special category data that may be collected. Separated definitions of third parties into professional services and service providers and updated the data shared with column.	Guy Outram	26/06/2018
3	Added references to emergency services	Guy Outram	28/06/2018
4	Added additional service providers to Table 2	Guy Outram	24/08/2018
5	Amended terminology to Customers i.e organisation and Client i.e. staff member/employee receiving the service.	Guy Outram	22/02/2019
6	Retitled Privacy Policy for Customers.	Guy Outram	19/06/2019