Introduction to Data Protection

This document contains details of Crux Conversation CIC's policy on personal privacy and data protection, including in particular our obligation to comply with the eight Data Protection Principles contained in the Data Protection Act 1998 to protect the personal privacy of all living people.

A Glossary of terms is set out at the end of the document.

a) Data Protection Supervisor

If you have any questions or need information on anything to do with data protection, please contact the Founders.

b) What is Data Protection?

In simple terms, data protection is the protection of information about living people. This information can be created and kept in many forms - for example on computer (such as emails), paper, CCTV, photographs, personal digital assistants and many others; it covers both facts and opinions about people.

c) What is the Data Protection Act?

The Data Protection Act 1998 (the "Act") imposes obligations on businesses that hold personal information, and gives rights to individuals whose data is held. The Information Commissioner oversees and enforces the Act.

The General Data Protection Regulation (the "GDPR") will come into force in the UK in May 2018, and provides additional protection to individuals.

d) What does the Act apply to?

The Act applies to "personal data". This is information relating to living people who can be identified from the information that a "data controller" has, even if an individual's name is not specifically mentioned, and is referred to throughout this policy as "Personal Information". These individuals are known as "data subjects".

The Act is intended to protect this information and the way that the information is used. It is also intended to regulate against the potential misuse of this information.

e) Who does the Act apply to?

The Act applies to anyone who processes personal information. "Processing" is a broad term referring to almost anything that can be done to information - including collecting, recording, storing, transferring, amending, destroying it or simply holding it.

f) What are the Data Protection Principles?

There are 6 Data Protection Principles under article 5 of the GDPR, which are designed to protect the personal privacy of each of us and with which we must comply under the Act. The Principles state that personal information must be:

i. processed lawfully, fairly and in a transparent manner in relation to individuals;
ii. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

iii. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
iv. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
v. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
vi. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

g) What is the CIC's legal basis for processing personal data?

Where the CIC does not have consent, it is entitled to process data under article 6(f) of the GDPR because it is in its legitimate interests. That means that the processing is necessary for the legitimate interests of the CIC unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. It is necessary for the CIC to process data to carry out the purposes and aims that it was set up to do and operate as a mediation and coaching service. It is in the legitimate interests of the CIC to obtain data from:

i. mediation and coaching clients in order to help them mediate their conflict and ultimately to benefit them;
ii. directors to contact them and to comply with legislation;
iii. volunteers in order to manage mediation and coaching cases effectively, by ensuring mediators and volunteers have the appropriate training and experience to mediate;
iv. any staff to ensure they have the appropriate experience and skills to manage cases and comply with their contracts of engagement.

h) What is the legal basis for processing special categories of personal data?

"Sensitive personal data" or "special categories of personal data" (under the GDPR) is given additional protection under the Act. This is information that relates to an individual's:

- racial or ethnic origin
- political opinions
- religious or similar beliefs
- trade union membership
- physical or mental health or condition
- sexual life
- criminal history (including convictions or commission of offences/alleged offences).

This is referred to throughout this Policy as "special categories of personal data".

The CIC must gain explicit consent for processing special categories of personal data.

Data Protection Policy Areas of good practice:

1. All personal data is potentially disclosable to the person to whom it relates. Volunteers, staff and directorsshould bear this in mind when recording expressions of opinion about people and ensure that the CIC can justify what it writes (e.g. in interview notes or in emails).

2. It is important for volunteers and staff to remind mediation clients that anything expressed in writing about another person could be seen by that person if they make a subject access request.

3. All personal data held on personal computers, phones, tablets and other devices must be deleted at the end of a case. This includes emails sent and received, case notes, handwritten notes, documents to prepare for a mediation and any other written data.

4. If data is retained by volunteers, staff or directors, for example for professional development or to comply with professional requirements, it must be anonymised so that the data subject cannot be identified from the data held. If data is held which would allow the data subject to be identified, then the holder of this data is required to comply with the data protection legislation in their own right.

5. Please keep devices or paperwork relating to cases or the work of the CIC secure, that is: a. Password protect phones and devices b. Ensure that data in transit is password protected if appropriate c. Make sure you know where your data is stored. If you cannot guarantee that data remains in the UK/EEA please inform the Founders.

6. The CIC appreciates that anyone can make a mistake. In the event of a data protection breach (e.g. a personal phone being lost or stolen with emails relating to cases on it) please let the staff or a trustee know as soon as possible. The CIC is required to notify the Information Commissioners' Office within 72 hours and there could be serious consequences for the CIC of we fail to comply.

7. In processing data for children under 13, parental consent is required to handle data. Please speak to the Founders if processing data concerning those under 18. 8. If consent to holding data is communicated to you, please notify the Founders without delay.

a) Collection, use and storage of personal data

The CIC will:

• unless it is entitled to hold data in its legitimate interests, seek your consent prior to the collection of your personal data.

• make sure that the personal information which it holds is adequate, relevant and not excessive in relation to its business purposes (i.e. no one will ask for or record excessive information that we do not need, even if it is information that is 'nice to know').
• make sure that the personal information is accurate and kept up to date, and is not kept for any longer than is necessary.

• make sure that, to the extent necessary, data subjects are given notice of the processing of their personal information including:
- details of the information to be collected
- the purpose for which it is to be collected and used, and
- any other relevant information.

• comply with the rights of people on whom we hold information (such as the right to access information about themselves or the request to erase that information).

• only process special categories of personal data with the explicit consent of the person on whom we hold the information.

b) Security of personal Information

The CIC will seek your consent prior to the collection of your personal data, and will:

• take positive steps to prevent the accidental, improper or deliberate disclosure, mis-use or loss of personal information and prevent unauthorised access to it.

• protect all data on a computer in a secure office.

• limit the disclosure of and access to personal information to those who have a business need to access the information.

c) Disclosure of personal information to others

The CIC will:

• not disclose personal information relating to individual without the individual's consent.

• ensure that where any person or organisation processes personal information on behalf of the CIC (such as a marketing agency or IT service provider) the CIC enters into a written agreement with them requiring them to:

- process the personal information only in accordance with the CIC's instructions;
- maintain adequate information security; and
- take reasonable steps to ensure staff who have access to the information are reliable.

d) Disclosure of personal information outside the EEA

The CIC will:

• make sure that personal information is not transferred to any country outside the UK unless that country has adequate levels of protection in place to protect personal data;

• make sure that the data subject(s) concerned has/have consented to the transfer of the information; or

• make sure that an agreement has been entered into with the organisation the data is being transferred to based on the EU standard model clauses.

e) Subject Access Requests

A person on whom the CIC holds information has the right to be informed of this and to have a copy of the information, subject to a few limited exceptions. He or she must make a written request (which can be by email). If his/her personal information is being processed, the individual will be provided with (subject to limited exceptions): - a copy of the data - the source of the data - the purposes for which the data is being processed - to whom it may be disclosed - an explanation of any unintelligible codes or rating systems.

Compliance with the subject access request is not required where the CIC has complied with an identical or similar request of the data subject in the 6 month period prior to the new request and the data held has not changed substantially in that period.

The response to the subject access request should be made promptly. It must be made no more than 40 days from receipt of the request.

Information about staff and volunteers

This section sets out the policy in relation to the processing of information about the CIC's staff and volunteers. As the CIC may need to hold and use certain information relating to its staff and volunteers in the course of their employment or role in the CIC, this section gives information about the personal information that the CIC may hold and how it is used or is intended to be used:

Use of Personal Information Information may be used in relation to the following:

- recruitment;
- payroll and benefits administration (including sick pay, pensions, health insurance, gym membership etc), work and career management, including performance appraisals; in the case of employees;
- disciplinary and grievance procedures (including monitoring compliance with and enforcing policies) in the case of employees;
- payment under contracts for the engagement of services;
- ensuring co-mediators are paired appropriately;
- ensuring mediators have the appropriate training and experience;
- deriving statistics to apply for funding to support the work that we do.
- assessing performance and to set targets to further the aims of the CIC.
- absence monitoring;
- training course management;
- monitoring registrations with regulatory bodies to ensure compliance, training and other requirements are met;
- administering termination of employment, references etc;
- maintaining contact details to contact you for urgent business or personal reasons when you are out of the office;
- maintaining emergency contact and beneficiary details (which involves the CIC holding information on those you nominate in this respect);
- protecting the safety and security of staff and property; and
- to ensure health and safety compliance.

The CIC may also hold other information for accounting and billing purposes, work management and business development.

Disclosure of Personal Information

- Your consent will be obtained before the CIC responds to requests for information about you from third parties such as banks, mortgage lenders, prospective landlords or employers (e.g. requests for references), insurance and health providers.

- In relation to volunteers, your curriculum vitae (CV) may also be disclosed to mediation clients (both existing and prospective) and other professional advisers in the course of the provision of mediation services.

Document retention

The CIC will only store data for as long as is necessary, after which time it will anonymise or delete that data. The CIC will keep data relating to a case or enquiry for not more than 1 year after a case has closed. The CIC will keep data from volunteers for not more than 1

year after the end of your volunteer agreement. The CIC will keep data from staff and directors for not more than 6 years after the end of your contract or resignation. The following exceptions are in relation to information that the CIC is required to keep to comply with legal requirements:

- Gift aid records: 6 years
- Financial information (bank statements and paying in slips, cash books, invoices, receipts) for HMRC: 6 years from the end of the financial year in which the transaction was made.
- Safeguarding information as long as necessary in relation to the purposes for which that information was obtained
- Unsuccessful applications for volunteering or contracts: 1 year.
- Insurance policies and claims – 3 years after lapse or settlement of claim.
- Employer's liability certificate – 40 years.
- Minutes of trustee meetings and resolutions: 10 years
- Annual accounts and annual reviews: permanently

Future Developments

The law and practice in relation to data protection is still evolving. This will be reflected, so far as necessary, by amendments to this Policy. If material changes are made, you will be notified.

Glossary General terms:

CIC refers to Crux Conversations CIC and its successors and assigns from time to time.

Employee refers to anyone who has entered into a binding contract of employment with the CIC.

Mediation or coaching client means any person taking part (or preparing to take part) in a mediation or coaching session facilitated by the CIC.

Founders means that person designated by the CIC with that title, from time to time, and currently: Sarah Guthrie and Philip Guthrie: info@crux.org.uk.

Staff refers to directors, consultants, contractors, directors, and managers, whether employed directly by the CIC, or self-employed.

Volunteer refers to anyone who is volunteering their time and skills to the CIC on a pro bono basis.

Directors refers to the directors from time to time of WMS who are at the date of this version of the handbook:

- Jen Miles
- Sarah Guthrie
- Philip Guthrie
- Joel Robertson
- Stephen Ruttle QC
- Mark Scoggins
- Selina Stone

Data Protection terms:

Data Controller is a person who either alone, or jointly with other people, gives instructions as to what should happen to personal information and how it is to be processed.

Data Subject means an individual to whom the personal information relates.

Personal Data or Personal Information means any information that relates to a living individual (not companies). It includes information by which that individual can be identified and includes facts and expressions of opinion about individuals.

Process/processing/processed means almost anything that can be done to personal information - including collecting, recording, storing, transferring, amending, using, holding and destroying the information.

Special categories of personal data (formerly known as Sensitive Personal Data or Sensitive Personal Information) means any information relating to an individual's: (a) racial or ethnic origin; (b) political opinions; (c) religious beliefs; (d) trade union membership; (e) physical or mental health conditions; (f) sexual life; (g) criminal offence (Please note that there are additional restrictions on how this type of information can be used.)

Subject Access Request means a written request by a data subject made to a data controller, who must:

- inform him whether it has processed or is processing any information concerning him;
- describe the personal information, the source of the personal information, the purpose for which it is used and any third parties who receive the personal information; and
- provide the individual with a copy of the personal information except in certain limited circumstances.

This policy is illustrative of the way in which Crux Conversations CIC aims to approach its relationship with each of its directors, staff members, volunteers and mediation clients and other third parties.

This policy is reviewed regularly, in advance of Directors meetings, unless an incident occurs, or new legislation suggests the need for an earlier review date.