Data Protection Policy (GDPR)

Version No:	1
Current Status	Final
Date approved by the Connected Together CIC Board	14 December 2018
Author/Responsible Person	Jo Spenceley
Next revision due	December 2020
Staff/volunteer training delivered	Included in staff and volunteer induction and referred to as part of everyday practice
This policy covers Connected Together CIC (CTCIC) and all its organisations and contracts, for example Healthwatch Northamptonshire and Healthwatch Rutland	

1. Introduction

This policy supports the legal requirements of the General Data Protection Regulation, and the Data Protection Act 2018 (the UK's interpretation of GDPR), which places certain obligations on CTCIC, its staff and those who process data on our behalf. Whilst CTCIC expects its employees and staff to comply with this policy and the requirements of relevant legislation, it does not confer contractual rights or form part of any contract of employment and may be amended by CTCIC or replaced at any time following appropriate consultation and negotiation with recognised trade unions and others.

Breach of this policy may be addressed via CTCIC's disciplinary and code of conduct policies.

This policy will be reviewed by the CTCIC board in conjunction with the Data Protection Officer on a 3 year basis. It may however be amended in advance of such date in response to changes in future legislation and/or case law.

2. Ownership

The board of CTCIC owns and manages this policy on behalf of CTCIC.

3. Organisational Scope

This GDPR policy is a corporate policy and applies to all employees, volunteers, and workers, as applicable, of CTCIC, including any managed contracts and wholly owned subsidiaries, unless an alternative policy exists, subject to any qualifying conditions. This policy may form part of any agreements with organisations processing personal data on behalf of CTCIC as if they worked directly for CTCIC.

4. Definitions

This section includes all necessary definitions of terms used in the policy which are not in every day usage or where there is a need to be precise.

Personal data
Personal information data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data. We are legally obliged to report breaches that are likely to result in a risk to the rights and freedoms of individuals to the ICO and individuals will have to be notified directly by CTCIC.

Data Subject
Data subject means “an individual who is the subject of personal data”. A data subject must be a living individual.

Information Commissioner’s Office (ICO)
The UK’s independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO enforce the law in regard to information compliance legislation.

Consent
Consent means offering people genuine choice and control over how you use their data. Consent must be freely and explicitly given to be valid under GDPR.

Processing of Personal Data
Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –
(a) organisation, adaptation or alteration of the information or data,
(b) retrieval, consultation or use of the information or data,
(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
(d) alignment, combination, blocking, erasure or destruction of the information or data.

Retention schedule
A retention schedule is a list of records for which pre-determined destruction dates have been established. In the case of CTCIC, the retention schedule is combined with the information asset register into a single document. This is used as the basis for how long CTCIC should be keeping all data including personal information.

Retention period
The periods of time, varying from a few months to permanency, during which a record has to be

maintained by CTCIC. This is usually determined by statute, legal, regulatory or business compliance, or where these do not apply, by a best assessment of risks involved in destruction against the costs of retention.

CTCIC community
For the purposes of this Policy this includes staff, volunteers, contractors, and others with a direct impact on or responsibility to CTCIC.

Records Disposal
Disposal is an important part of good data protection and records management. Properly done, it ensures that CTCIC retains records for only as long as they are needed and then, when they are no longer needed, destroys them in an appropriate manner or disposes of them in some other way, e.g. by transfer to an archives service.

5. Policy Statement

5.1 CTCIC is strongly committed to complying with the legal requirements of all legislation enacted with the purpose of protecting the personal data and privacy of individuals.

5.2 This Policy and associated procedure sets out the minimum requirements for data processing by CTCIC so as to protect the rights of data subjects.

5.3 CTCIC as an institution, and individual members of the CTCIC community are expected to abide by the laws in force in this area. All CTCIC staff and contractors, as well as volunteers processing data on behalf of CTCIC, are responsible for any breaches of such legislation and any such breaches may result in fines or in extreme cases custodial sentences.

5.4 All processing of personal data under the GDPR needs to have a legal basis, and CTCIC must be able to demonstrate, to the ICO or to the individual, this basis using logged documentation.

5.5 It is important that we determine the legal basis for processing as under the GDPR this has an influence on an individual's rights. For example, if we rely on consent they will generally have stronger rights such as having data deleted.

5.6 Processing Conditions:

- Consent of the data subject.
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract.
- Processing is necessary for compliance with a legal obligation.
- Processing is necessary to protect the vital interests of a data subject or another person.
- 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.

5.7 The GDPR introduces a duty on CTCIC to report most data breaches to the Information Commissioner's Office, and often to the individuals affected. A notifiable breach has to be reported to the ICO within 72 hours of CTCIC becoming aware of it as well as, when appropriate, notification to the data subject within the same tight timescale.

5.8 Fines have increased and the maximum fines can be up to 20 million Euros or 4% Global Turnover for a breach, depending on the severity, scale or impact of the breach. For example the loss of hundreds of minor pieces of personal information might incur a smaller fine than a case where CTCIC loses the sensitive personal health information of one individual.

5.9 Failure to report a breach can also result in fines for CTCIC and potentially for the individual who has committed the breach. CTCIC requires all incidents and breaches to be reported so we can assess and reduce the risks and where possible prevent incidents from becoming serious breaches. Failure to report a breach may result in disciplinary action. Multiple breaches on a regular basis by the same individual will result in additional training being provided. Continuing breaches of personal data by one individual may result in disciplinary action being taken by CTCIC.

6. Key Principles

6.1 CTCIC needs to keep and process certain information about its employees, volunteers, contractors and others to allow it to comply with legal obligations, and to operate in an effective and efficient manner.

6.2 To comply with the existing Data Protection Act requirements and the General Data Protection Regulation, personal information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, CTCIC staff, volunteers and contractors must comply with the Principles and protections set out in the Data Protection Act 1998, Data Protection Act 2018 (GDPR) and reiterated in this policy.

6.3 CTCIC must only retain personal data in line with the guidance set out in CTCIC Retention Schedule. This document provides advice as to retention periods suitable for types of records prior to any disposal decisions being made.

6.4 Unauthorised recording of conversations is prohibited. Anyone in breach of this may be subject to disciplinary action.

7. Procedure

Data Held and Processed by CTCIC

7.1 CTCIC will use and otherwise process records of personal information relating to data subjects relevant to the effective functions and operation of its role as an employer and as the contract holder for Healthwatch Northamptonshire and Healthwatch Rutland, which provide some statutory services.

7.2 Where required, CTCIC will obtain freely given consent for all types of personal data processing except that specifically exempted by the Regulation.

7.3 The use of the information and retention of the personal data will be specifically defined.

7.4 All staff, volunteers and other data subjects about whom personal information is held have the following rights:

- The right to be informed.
- The right of access.

- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

7.5 This adds to the existing rights previously in place for data subjects which include a person's right to know:

- what information CTCIC holds and processes about them
- why the information is held and processed
- details of whom the information might be shared with
- know how to gain access to such information
- know that it is up to date
- know what CTCIC is doing to comply with its obligations under the 1998 Data Protection Act or other relevant legislation

8. Responsibilities of Staff in Relation to their own Data

All staff are responsible for:

- Checking that any personal data that they provide to CTCIC is accurate and up to date (they will be asked by CTCIC to check this periodically).
- Informing CTCIC of any changes or errors in the information held.

9. Responsibilities of Volunteers in Relation to their own Data

Volunteers will, at the time of joining, be required to agree to the use of personal data for CTCIC administrative purposes, which will be clearly specified. This will notify volunteers of the uses we are making of their personal data and will form a contract between CTCIC and the volunteer.

Volunteers must assist CTCIC in ensuring the accuracy of the personal data as provided to CTCIC and that the information is up to date. Any changes of address, etc. are to be notified to the relevant staff lead. They will be asked to check the accuracy of the information at induction. Changes made by the volunteer to the accuracy of the data CTCIC holds on them will not alter the basis of the Agreement between CTCIC and them.

10. Basic responsibilities on staff for Data Security of Third Party Personal data

CTCIC has a legal requirement to ensure that data is held securely and this includes the provision that access and disclosure of personal data should be restricted to those who have a legitimate, authorised purpose.

Staff, volunteers and contractors have a responsibility for using and otherwise processing personal data in compliance with this Policy and more specifically operating under the terms of the relevant Data Protection legislation.

Therefore, all staff, volunteers and contractors are responsible for ensuring that:

- Personal information is not disclosed by them either orally or in writing, to any unauthorised third party.
- They do not access any personal data which is not necessary for carrying out their work.
- Personal data in paper format is kept in a secure place when not being processed.
- Personal data on computer should not be accessed or viewed by unauthorised staff or students and as such workstations should be locked or password protected when not in use.
- No personal information should be removed from CTCIC buildings unless it is via a secured electronic means.
- Staff processing personal data for research purposes (for example, use of questionnaires) should include a Data Protection Notice informing the data subject of details such as why the data is being collected and how long it will be retained for.

A Data Protection Impact Assessment (DPIA) will be completed for all new projects and pieces of work by the project leader with the support of the DPO and approved by the CEO. This will ensure that data protection is considered at the planning stage, including awareness of what personal data is being collected, and planning appropriate privacy protections and mitigation any potential data protection risks.

11. Responsibilities on Volunteers for Data Security of Third Party Personal data

Volunteers may need to process personal information for project or research purposes such as surveys, etc. Such documents should include a Data Protection Notice informing the data subject of details such as why the data is being collected and how long it will be retained for. If volunteers are processing personal data then they must obtain appropriate approval from the relevant authority and any such collection of personal data should need the approval of the research lead.

12. Right of Access to Information

All data subjects have the right to access any personal data that is being kept by CTCIC about them either on computer or in certain other files. Any volunteer or service user who wishes to exercise this right should make a written request to the volunteer lead or to CTCIC Data Protection Officer. Staff should make a written request to the CEO or to CTCIC Data Protection Officer. Any requests relating to Healthwatch contracts can also be made to the independent Healthwatch Data Protection Officers (details at http://www.connectedtogether.co.uk/privacy/). CTCIC cannot charge any fee or disbursement for such a service, unless a request is manifestly unfounded or excessive, in which case a “reasonable fee” for the administrative costs of complying with the request may be charged. CTCIC must make all efforts to provide the personal data in a format defined by the requester.

All requesters will be asked to include proof of identity and no response will be sent until such proofs have been provided. CTCIC will ensure that requests for information are responded to within the statutory month period unless additional information has been requested by us to help identify the requested data. In such cases, the reason for delay will be explained in writing by the Data Protection Officer to the person making the request.
Third party information will normally be redacted in lines with the rights of such third parties.

13. Publication of CTCIC Information

Information that is already in the public domain, and accepted by the data subject as being so, is less likely to be covered by the legislation, for example, externally circulated publications and web pages. However, the GDPR does provide, in certain circumstances, for a data subject to have the right of erasure of personal data. This is a complex area and any member of staff receiving such a request should contact CTCIC Data Protection Officer. Any individual who believes that they have good reasons to have their information excluded from any such publications or released data, should inform the CEO, who will coordinate with the Data Protection Officer.

14. Associated Documents

External associated documents

- The General Data Protection Regulation 2018
- Data Protection Act 1998
- Privacy and Electronic Communications Regulation
- Information Commissioner's Office Overview of the General Data Protection Regulation (GDPR)
- Information Commissioner's Office Privacy Notices, Transparency and Control – a code of practice on communicating privacy information to individuals
- Information Commissioner's guide to data protection
- Information Commissioner's Office Guide to Privacy and Electronic Communications Regulation
- Freedom of Information Act 2000

Internal associated documents

- Confidentiality Policy
- Retention Policy
- GDPR Action Plan
- Privacy Statement

15. Equality Analysis

There is no equality impact within this policy