Information Governance – Policy – Data Protection

Version No:	1
Date approved by CIC Board	18 April 2016
Author/Responsible Person	Jo Spenceley
Last revised	
Next revision due	April 2018
Staff/volunteer training delivered	
Please note that it is the responsibility of the individual Connected Together CIC/Healthwatch Northamptonshire staff, board member or volunteer to ensure that they are reading the most current version of this policy. This policy covers Connected Together and all its organisations/contracts.	

Introduction

Connected Together CIC, and all contracts it holds, including Healthwatch Northamptonshire (from here in referred to as CTCIC) needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees/volunteers and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

Everyone has rights with regard to how their personal information is handled. In its work CTCIC will collect, store and process personal information and we recognise the need to treat it in an appropriate and lawful manner. The information is subject to safeguards specified in the Data Protection Act 1998 which imposes restrictions on how we may use that information.

Purpose

This data protection policy ensures CTCIC:

- Complies with data protection law and follow good practice
- Protects the rights of employees/volunteers, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Policy scope

This policy applies to:

- All employees and volunteers of CTCIC
- All contractors, suppliers and other people working on behalf of CTCIC

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- …plus any other information relating to individuals

Data protection risks

This policy helps to protect CTCIC from some very real data security risks, including:

- **Breaches of confidentiality,** for instance, information being given out inappropriately
- **Failing to offer choice,** for instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage,** for instance, the company could suffer if hackers successfully gained access to sensitive data.

The Data Protection Act 1998 (The Act)

The Act gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly.

The Act states that anyone who processes personal information must comply with eight principles, which make sure that personal information is:

a) Fairly and lawfully processed
b) Processed for limited purposes
c) Adequate, relevant and not excessive for the purpose
d) Accurate and up to date
e) Not kept for longer than is necessary for the purpose
f) Processed in line with the rights of data subjects
g) Secure
h) Not transferred to other countries without adequate protection

The Act also provides individuals with important rights, including the right to find out what personal information is held on computer and certain paper records.

Definitions

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems. This includes photographic images and video footage.

Data subjects are all living individuals about whom we hold and process personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Personal data means 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 from a questionnaire).

Data controllers are the organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act.

Data Protection Officer is the name given to the person in an organisation who is the central point of contact for all data compliance issues.

Data processors include any person who processes personal data on behalf of a data controller. Responsibility for compliance with the Data Protection Act remains with the Data Controller. There should be a written contract with the data processor who must have appropriate security.

Processing is any activity that involves use of the 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.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about any offence committed or alleged to have been committed by that person. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

Policy Statement

CTCIC will:

- Comply with both the Data Protection Act and good practice
- Respect individuals' rights
- Be open and honest with individuals whose data is held
- Provide training and support for those who handle personal data, so that they can act confidently and consistently

CTCIC recognises that its first priority under the Act is to avoid causing harm to individuals. Information about staff, volunteers and clients will be used fairly, securely and not disclosed to any person unlawfully.

CTCIC aims to ensure that individuals are aware that their data is being processed, and that they understand how the data is being used and how to exercise their rights.

CTCIC will also ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, CTCIC will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

Responsibilities

Healthwatch Northamptonshire CIC Board:

CTCIC is the Data Controller and is registered under the Data Protection Act. All processing of personal data will be undertaken in accordance with the data protection principles. The CTCIC Board recognises its overall responsibility for ensuring that CTCIC complies with its legal obligations.

Data Protection Officer:

The Healthwatch Northamptonshire Data Protection Officer is Jo Spenceley, who is responsible for ensuring compliance with the Act and with this Policy. The Data Protection Officer has the following responsibilities:

- Briefing the Trustees on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising staff and volunteers on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Handling subject access requests
- Ensuring contracts with Data Processors have appropriate data protection clauses

Indigo IT Services is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Performing regular checks and scans to ensure security hardware and software is functioning properly
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services

Employees and Volunteers:

Each member of staff and volunteers with CTCIC who handles personal data will comply with our procedures for handling personal data to ensure that good Data Protection practice is established and followed.

Breaches of this policy will be handled under our disciplinary procedures.

Confidentiality

Because confidentiality applies to a much wider range of information than Data Protection, CTCIC has a separate Confidentiality Policy which should be read in conjunction with this Policy.

Board members, staff and volunteers are required to sign a short statement indicating that they have been made aware of their confidentiality responsibilities. (See Confidentiality Policy and Statement.)

Operating Principles

Processing of Data

Where required, data subjects can be told that CTCIC is the Data Controller, who the Data Protection Officer is, the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

Processing for Limited Purposes

Personal data may only be processed for the specific purposes notified to the data subject by CTCIC when the data was first collected. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

Adequate, Relevant and Non-Excessive Processing

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

Consent

Consent will normally not be sought for most processing of information about staff.

Information about volunteers will be made public according to their role, and consent will be sought for (a) the means of contact they prefer to be made public, and (b) any publication of information which is not essential for their role.

Information about service users/clients will only be made public with their consent (this includes photographs). ‘Sensitive’ data about clients will be held only with the knowledge and consent of the individual.

CTCIC acknowledges that, once given, consent can be withdrawn, but not retrospectively.

Accurate Data

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and CTCIC will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data will be corrected or destroyed.

CTCIC will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

- Data on any individual will be held in as few places as necessary, and all staff and volunteers will be discouraged from establishing unnecessary additional data sets
- Effective procedures are in place so that all relevant systems are updated when information about any individual changes
- Staff and volunteers will be given guidance on accuracy in record keeping

Timely Processing

Personal data should not be kept longer than is necessary for the purpose and will be destroyed or erased from our systems when it is no longer required.

Data Security

CTCIC will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

Any recorded personal data on clients, volunteers and staff will be:

- Kept in locked desks and cabinets
- Protected by the use of passwords if kept on computer
- Destroyed confidentially if it is no longer needed

CTCIC currently hold information on a range of spreadsheets and will be moving to having a single database holding basic information about all clients and volunteers. Access to information on the database and spreadsheets is controlled by a password and only those needing access are given the password.

Data Subject's Rights

Data must be processed in line with data subjects' rights. Data subjects have a right to:

- Request access to any data held about them by CTCIC and ask why it is held and who it has been shared with
- Prevent the processing of their data for direct-marketing purposes
- Ask to have inaccurate data amended and be informed how to keep it up to date
- Prevent processing that is likely to cause damage or distress to themselves or anyone else
- Be informed how the company is meeting its data protection obligations.

Dealing with subject access requests

All clients and customers have the right to request access to all information stored about them.

Subject access requests must be in writing. All staff and volunteers are required to pass on anything which might be a subject access request to the Data Protection Officer without delay.

Individuals can be charged up to £10 per subject access request. The data controller will aim to provide the relevant data within 14 days and must provide it within 40 days.

Where the individual making a subject access request is not personally known to the Data Protection Officer their identity will be verified in writing before handing over any information.

Policy Review

The policy will be kept under review in response to changes in relevant legislation, contractual arrangements, good practice or in response to an identified failing in its effectiveness.

healthwatch Northamptonshire

Equality Impact Assessment Form

Screening determines whether the policy has any relevance for equality, i.e. is there any impact on one or more of the protected characteristics as defined by the Equality Act 2010. These are:

- Age
- Disability
- Gender Reassignment
- Marriage and Civil Partnership
- Pregnancy and Maternity
- Race
- Religion or belief Including lack of belief)
- Sex
- Sexual Orientation

1. Name of policy/procedure being assessed:	CTCIC – Information Governance Policy – Data Protection
2. Is this a new or existing policy/procedure?	New
3. What is the function of the policy/procedure?	To guide board members, staff and volunteers on the procedures CTCIC has in place in respect of data control
4. What is it trying to achieve and why?	To provide guidance on best practice in the control of data
5. Who is intended to benefit and how?	Employees, volunteers, wider public
6. Is there any potential for differential impact (negative or positive) on any of the protected characteristics?	No
7. Is there any possibility of discriminating unlawfully, directly or indirectly, against people from any protected characteristic?	No
8. Could there be an effect on relations between certain groups?	No
9. Does the policy explicitly involve or focus on a particular equalities group i.e. because they have particular needs?	No
Signature: **Name:** **Position:**	**Date:**

healthwatch Northamptonshire

Data protection guidelines for employees and volunteers

General:

- The only people able to access data covered by this policy should be those who **need it for their work**
- Data **should not be shared informally**. When access to confidential information is required, employees/volunteers can request it from their line managers
- **CTCIC will provide training** to all employees/volunteers to help them understand their responsibilities when handling data
- Employees/volunteers should keep all data secure, by taking sensible precautions and following the guidelines below
- In particular, **strong passwords must be used** and they should never be shared
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of
- Employees/volunteers **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection

Data storage:

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the data controller.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a **locked drawer or filing cabinet**
- Employees/volunteers should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer
- **Data printouts should be shredded** and disposed of securely when no longer required

- When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts
- Data should be **protected by strong passwords** that are changed regularly and never shared between employees/volunteers
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**
- Servers containing personal data should be **sited in a secure location**, away from general office space
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with standard backup procedures
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones
- **All servers and computers containing data should be protected by approved security software and a firewall**

Data use:

When personal data is accessed and used it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees/volunteer should ensure **the screens of their computers are always locked** when left unattended
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure
- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts
- Personal data should **never be transferred outside of the European Economic Area**
- **Employees/volunteers should not save copies of personal data to their own computers. Always access and update the central copy of any data**

Data accuracy:

The law requires CTCIC to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort CTCIC should put into ensuring its accuracy.

It is the responsibility of all employees/volunteers who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Employees/volunteers should not create any unnecessary additional data sets
- Employees/volunteers should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call
- CTCIC will make it **easy for data subjects to update the information CTCIC** holds about them. For instance, via the company website
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database

It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months