Information Sharing Policy and Procedure

Date approved by the Connected Together CIC Board	24th March 2020
Author/Responsible Person	Michelle Wright
Next revision due	March 2023
Staff/volunteer training delivered	This will be included in staff induction
Date sent to staff	
	This policy covers Connected Together CIC and *all* its contracts and managed organisations, for example Healthwatch West Northamptonshire (HWW) and Healthwatch Rutland (HWR).
Checked for rebranding	Michelle Wright – 29/04/2022
Signed off by CEO	Kate Holt – 03/05/2022
Checked By	Catherine Maryon (CTCIC Director) - date
Amendments made	Amendments made by Michelle Wright removing reference to Healthwatch North Northamptonshire.18/03/2025

1. Introduction

This policy provides further detail to supplement the Connected Together CIC Data Protection Policy.

The purpose of this document is to facilitate the lawful, appropriate, and effective sharing of information between Connected Together CIC (CTCIC) and its partner organisations.

Some of the agencies that CTCIC will share information with include:

- Other local Healthwatch organisations for the purpose of identifying common themes or issues relating to the provision of health and social care, for joint working on issues which cross boundaries between multiple local Healthwatch organisations, and for the general sharing of intelligence, expertise, training, and advice

- Healthwatch England for the purpose of supporting Healthwatch England in its statutory functions

- Service providers and commissioners, to ensure information is used to shape, influence, and inform the design and delivery of health and social care services

- Regulators, e.g. the Care Quality Commission (CQC) to support the exercise of their functions, including monitoring and enforcing compliance with regulations and conditions of registration

- Safeguarding teams, to ensure that the welfare of children and vulnerable adults is protected.

Where regular flows of information are anticipated, information sharing protocol are negotiated and agreed, e.g. with large service providers and their commissioners.

These protocols provide information as to:

- the purpose for the sharing
- the circumstances that trigger the sharing of information
- the method for disclosure (how the information will transfer, who will send the information, and to whom)
- any security measures to be applied, and
- any limitations on the use of the data.

For those agencies who receive our information less regularly, e.g. smaller providers such as GPs, care homes, optician, dentists and pharmacies, we provide the same information, in the form of 'guidance notes', and there is no requirement to provide a named person. This is due to the large number of smaller providers across the county. We ask that they follow the guidance to ensure that the information provided is used appropriately and sensitively.

In most cases, it is anticipated that information sharing for the all the above purposes shall be met by sharing information that is not personal data (i.e. from which individuals cannot be identified), unless those individuals have given their consent to the sharing of their personal data or, in extraordinary circumstances, where the disclosure is lawful without consent and in the very clear public interest (for example, where necessary to protect any person from serious harm).

2. Connected Together CIC (including HWW and HWR, and any other contracts held by CTCIC) will comply with the common law duty of confidentiality

This means that all personal and sensitive information provided by patients and the public, whether held on paper, computer, visually or audio recorded, or held in the memory of the member of staff or volunteer, must not normally be disclosed without the consent of the individual.

Three circumstances making disclosure of confidential information outside of CTCIC lawful are:

- consent has been given by the individual(s) to share their information, or
- when disclosure is lawful without consent and in the very clear public interest, e.g. to protect any person from serious harm
- where there is a legal duty to do so, for example a court order.

3. Safeguarding

If CTCIC receives information or allegations regarding abuse (including, neglect, physical abuse, emotional abuse, sexual abuse or institutional abuse) or other information which suggests that the welfare of vulnerable people may be at significant risk, we will report these directly, in accordance with local safeguarding procedures.

4. Legal requirements

CTCIC and our partner organisations must comply with all relevant legal requirements relating to the processing of information (particularly personal data). The principal legislation is found and explained in the General Data Protection Regulation (GDPR) which came into effect in May 2018.

Partner organisations must also comply with the common law duty of confidentiality as detailed above.

Other legislation where relevant has also been considered, such as the Freedom of Information Act 2000.

5. Responsibilities

Where information sharing is agreed, each partner organisation is responsible for ensuring:

- Their organisational, technological and security measures meet the requirements of the protocol/guidance we provide.
- That the requirements of their protocol is appropriately and adequately communicated to their staff, and to other agents acting on their behalf, and for ensuring compliance with the protocol.
- Their own compliance with applicable legislation and common law. If they consider that any part of the protocol is incompatible with that requirement, then compliance with the law takes precedence. In such circumstances, they must notify all parties as soon as possible.

6. Personal data (including sensitive personal data)

Staff should only be given access to personal data where that access is necessary in order for them to perform their duties.

Personal data must only be shared between partner organisations where:

a) There is a lawful basis to do so (consent is one lawful basis)
b) The organisation receiving the personal data has a genuine and legitimate 'need to know' (i.e. they have a legitimate purpose for receiving the information), and
c) The disclosure is considered proportionate, with consideration of the potential impact upon the privacy of individuals.

Wherever possible, consideration should be given as to whether it is necessary or appropriate to share or use personal data. Where non-personal, anonymised or pseudonymised data can practicably be used to achieve the same purpose, then personal data must not be shared or used.

CTCIC will ensure that each partner organisation is made aware that they must ensure that any of its employees or agents accessing personal data is fully aware of their responsibilities to maintain the security and confidentiality of personal data.
CTCIC will ensure that each partner organisation is made aware of their responsibility to take reasonable steps to ensure that any of its staff accessing personal data follow the procedures and standards set in the information sharing protocols.

Consent (in relation to personal data)

Consent is the main legal basis we use for sharing personal data, i.e. CTCIC will only disclose identifiable personal data to other parties with the consent of the person who provided that information to them (unless there is a legal obligation to disclose, or – in extreme and exceptional circumstances – where failure to disclose the information is likely to result in serious harm to any person).

Therefore, CTCIC takes particular care to ensure that the data subject is fully informed as to what data it is proposed to disclose, with whom, for what purpose and how that data will be handled and used. This is outlined in an information sheet or statement for each piece of work undertaken and explained to members of the public in writing or verbally. Failure to respond to a communication will not be assumed to indicate 'implied' consent.

Although consent is normally obtained at the earliest opportunity, if some time has lapsed between asking for consent to share personal data, and the data being shared, we will check that the data subject (the person to whom the information relates) is still happy to give consent.

The data subject has the right to withdraw consent at any time. Sharing or disclosure of personal data must cease if consent is withdrawn. Withdrawal of consent must be communicated to the other parties as soon as possible. Following the withdrawal of consent, all parties must

assess whether another condition under the General Data Protection Regulation will lawfully apply to allow them to continue processing that personal data which they already hold.

Where the data subject is an adult and does not have the capacity to give informed consent, no other person may give consent on their behalf unless specifically empowered to do so by power of attorney or order of a court. In such circumstances, personal data may only be shared where another condition under the General Data Protection Regulation will lawfully apply to permit this.

7. Anonymised data

For the purposes of this section, references to anonymisation also apply to pseudonymisation (where personal identifiers have been removed, but the provider organisation is still able to identify the data subject, for example by use of a unique identifier number).

In order to protect privacy, reduce the risks relating to General Data Protection Regulations compliance, and to minimise the risk of security breaches, data being used by and shared between the partner organisations should be anonymised wherever there is not a legitimate reason and legal basis for using or sharing personal data.

Anonymised data about an individual can be shared without consent in a form where the identity of the individual cannot be recognised i.e. when:

- Reference to any data item that could lead to an individual being identified has been removed; and
- The data cannot be combined with any data sources held by any likely recipient in order to produce personal identifiable data (i.e. where nobody who is likely to receive the data could reasonably be able to identify individual(s) from that data, on its own or when combined with other information available to them or likely to become available to them)

It is the responsibility of CTCIC to ensure that any anonymisation of personal data is adequate.

Partner organisations will be informed that they must not attempt to identify individuals from anonymised information, or to combine anonymised information with other information in such a way as to make it reasonably possible to identify individuals, without the written consent of CTCIC.

8. Non-personal data

Partner organisations will be informed that they should not assume that non-personal information is not sensitive or confidential and can be freely shared. This may not be the case and, where there is any doubt as to whether such information is sensitive or confidential, the information provider should be contacted before any further sharing takes place.

9. Data quality

CTCIC shall ensure the information it provides is of sufficient quality, i.e:

- adequate,
- relevant,
- not excessive in relation to the purposes for which it is required, and
- accurate.

10. Prohibition on further use

Partner organisations will be informed that they should ensure the information provided by CTCIC is used exclusively for the specified purposes set out in the protocol and not further use the information in any manner incompatible with that purpose or purposes without the prior written consent of the CTCIC, or as provided by law.

11. Security arrangements

CTCIC will ensure the security of supplied information, personal or non-personal, and process the information accordingly, to mitigate against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

CTCIC will make it a condition of employment that employees will abide by this policy in relation to the protection and use of personal data and other confidential information. This condition will be written into employment contracts and any failure by an individual to follow the policy will be dealt with in accordance with our disciplinary procedures.

CTCIC will ensure that information sharing protocols with their partners include a condition that they abide by the rules and policies in relation to the protection and use of confidential information.
CTCIC will exercise reasonable judgement to ensure that information is transmitted in accordance with the level of security appropriate to its content. CTCIC will ensure it maintains the appropriate security measures throughout the lifecycle of the information, in particular, during storage, use, transmission and destruction.

This section is covered in more detail in our **ICT Acceptable Use Policy and Data Breach Notification Policy**.

12. Access to information requests

Freedom of Information Act 2000

CTCIC holds information in part for the purpose of performing statutory functions on behalf of West Northamptonshire County Council (WNC) and Rutland County Council (RCC), subject to the terms of the contracts held. NCC and RCC will have a legal responsibility to respond to Freedom of Information Act (FOI) 2000 requests for information held by CTCIC. CTCIC

recognises that NCC and RCC are responsible for meeting their FOI Act obligations and will respond to requests.

The General Data Protection Regulation (GDPR) Subject Access Request (SAR)

GDPR provides a right of subject access (for any person to be supplied with personal data relating to themselves held by any organisation). Hence, the information that is the subject of this policy may therefore be subject to disclosure.

Dealing with subject access requests (SAR) is covered in more detail in our SAR Policy and Procedures, but in brief:

- SARs can be made verbally or in writing
- Where the individual making a SAR is not personally known to CTCIC or its contracts, their identity will be verified before handing over any information
- Information will be sent within one month of receiving the request.

Although CTCIC appoints the Chief Executive to handle access to information requests, all staff will be trained to identify requests, which may in some instances be communicated verbally, or via email. A request does not have to include the phrase 'subject access request' or Article 15 of the GDPR, as long as it is clear that the individual is asking for their own personal data.

13. Retention periods

Information will be stored in accordance with the CTCIC **Record Keeping and Retention Policy**. Information will not be retained for longer than is necessary to fulfil the specified purpose or purposes; and will be reviewed annually.

14. Inappropriate or unauthorised access or use of personal data

CTCIC will investigate and deal with the inappropriate or unauthorised access to, or use of, personal data whether intentional or inadvertent.

In the event of personal data that has been shared under this policy becoming compromised, or suspected of becoming compromised, whether accidental or intentional, CTCIC will without delay:

- Assess the potential implications for the individual whose information has been compromised
- If the severity is likely to result in a risk to people's rights and freedoms, then the breach will be reported to the Information Commissioners Office (ICO), e.g. if it were to result in discrimination, identity theft or fraud, financial loss or damage to reputation
- Notify the individual, advise the individual of their rights, and provide appropriate support
- Take steps to investigate the cause
- If appropriate, take disciplinary action against the person(s) responsible
- Take appropriate steps to avoid a repetition
- Take appropriate steps where possible to mitigate any impact.

More information can be found in our **Data Breach Notification Policy**.

Internal associated documents

- GDPR Policy-009/QD29
- ICT Acceptable Use Policy-028/QD48
- Data Security Policy-010/QD30
- Record Keeping and Retention Policy-039/QD59
- Data Breach Notification Policy -008/QD28