Confidentiality Policy

Date approved by the Connected Together CIC Board	Ratified by CIC Board 28/06/2022
Author/Responsible Person	Michelle Wright
Next revision due	June 2025
Staff/volunteer training delivered	Included in staff induction and Volunteer Handbook
Date sent to staff	06/07/2022
	This policy covers Connected Together CIC and *all* its contracts and managed organisations, for example Healthwatch North Northamptonshire and West Northamptonshire (HWNW) and Healthwatch Rutland (HWR).
Checked for rebranding	Michelle Wright – 19/04/2022
Signed off by CEO	Kate Holt – 26/04/2022
Checked By	Catherine Maryon (CTCIC Director) – 11/05/2022

Connected Together
First for Community Engagement

Confidentiality Policy

During their employment, in the case of directors, board members, staff, or in their capacity of volunteers, persons will most certainly have access to or have sight of documents and other information that is of a confidential nature.

At all times information gained during their employment should and must be dealt by staff and volunteers in a sensitive and confidential manner.

The information may be:

- Confidential to the organisation of CTCIC, and which if disclosed could have a detrimental effect on CTCIC,
- Confidential to individual members of CTCIC or persons with whom CTCIC staff and volunteers come into contact
- Other information to which CTCIC has access or which comes to the knowledge of CTCIC staff and volunteers

Irrespective of which of the three classifications the information applies to, the way that it is handled and dealt with is the same:

Under no circumstance should information to which staff and volunteers have access to or become aware of, because of their CTCIC activities, be disclosed to persons outside the organisation, without properly authority to do so. This authority should normally be granted by either the Chair or CEO of the organisation.

1. Exceptions to disclosure.

There are, of course, exceptions when information outlined above, may and should be disclosed to persons outside CTCIC:

- To safeguard the health and welfare of any person, irrespective of whom that person may be. In this instance the safeguarding policy would be referred to
- To prevent or detect a criminal offence
- To minimise loss or damage to the reputation of CTCIC
- To minimise or prevent the loss of CTCIC property or finances
- In accordance with the CTCIC Whistleblowing policy

Where there is a legal duty on the organisation to disclose information to a statutory authority, the person to whom the confidentiality is owed should normally be in informed that disclosure has been or will be made. There are exceptions to this, when the informing of the forementioned person will amount to a criminal offence. Therefore, guidance should always be sought if there is any doubt as to the correct course of action.

2. Safeguarding information

It is the responsibility of all CTCIC directors, board members, staff, and volunteers to ensure that they handle any information they receive during them
Staff and volunteers have the use of a range of information storage systems and devices. They should always ensure that the information is kept safe and secure. Please see the Data Protection and IT Acceptable Use policies. This requirement covers all information kept by any staff member or volunteer, wherever it is stored, including but not limited to paper files, on computers (desktop and portable), mobile phones and cloud and backup systems.

All documents relating to the work of CTCIC should always be kept secure. Once the purpose for which the document has been prepared has ceased, paper copies should either be correctly and securely filed in the CTCIC office, on a password protected computer drive, or shredded, in compliance with the use of data and information act and General Data Protection Regulations (GDPR).

3. Data Protection Act

Any information held by CTCIC, and its contracted organisations should not be disclosed to a person or organisation outside of CTCIC, without the proper authority of the Chair or CEO of CTCIC. Any unauthorised disclosure may make the staff member or volunteer, as well as CTCIC, liable to prosecution, etc., under the Data Protection Act.

Please see Item 1 ‘Exceptions to disclosure’ above.

4. Access to information

Information is confidential to the organisation and should only be passed to an external organisation with the permission of the source of that information.

Sensitive information will only be made available to the person named on the file.

4.1 Personal Files

Staff and volunteers of CTCIC and its contracted organisations have the right to see their personnel files by giving reasonable notice to CTCIC CEO.

4.2 Copying files and other information

When copying documents, ensure that the contents of the document being copied cannot be seen by another person. Any misfed, misprinted or copies not required should be shredded.

4.3 Information from outside CTCIC

When information is received from organisations outside CTCIC and is deemed confidential, CTCIC undertakes to respect that confidentiality.

4.4 Storing information

General non-confidential information will be stored in filing cabinets or desk drawers, with open access to CTCIC staff. Information of a personal nature regarding staff and volunteers will be kept by the CEO or a nominated person and will be always kept secure.

In the case of an emergency, such as requiring details of Emergency Contact for a person, access can be granted by a senior manager other than the CEO.

5. Signed Confidentiality Agreements

Staff and volunteers will be required to sign confidentiality agreements and relevant Codes of Conduct.

6. Breaches of Confidentiality

Any member of staff or volunteer accessing unauthorised files or breaching confidentiality may be deemed to have committed an act of gross misconduct and may be subject to disciplinary action and ultimately dismissal.

Internal Associated Documents

- GDPR Policy-010
- Whistleblowing Policy-055