



Triple C
(Liverpool)

Christ Church Community Centre
Sedgemoor Road
Liverpool
L11 3BR
0151 226 2992
info@triplecliverpool.org

CONFIDENTIALITY POLICY

<u>Policy Adopted</u>	<u>August 2009</u>
<u>Last Reviewed</u>	<u>March 2024</u>
<u>Next Review Due</u>	<u>March 2027</u>

<u>Date</u>	<u>Reviewed by</u>	<u>Approved by</u>	<u>Date Accepted by Trustees</u>
Month YYYY		Policy Review Group	May 2021
February 2024	SC/SJ/HE/KW	Policy Review Team	March 2024

CONFIDENTIALITY POLICY

1. Introduction

Triple C (Liverpool), hereafter referred to as Triple C, recognises the great importance of confidentiality in the professional practice of its staff and administrative procedures. Triple C understands confidentiality to mean that information clearly intended for one purpose should not be used for another, without the permission of the person supplying that information.

2. UK GDPR

Triple C is committed to ensuring the Charity follows good practice in matters covered by GDPR. Triple C is registered with the Information Commissioners Office and further details about GDPR are available on their website. <https://ico.org.uk/for-organisations/>

The UK GDPR set out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

These principles should lie at the heart of Triple C's approach to processing and handling personal data.

These underlie our approach to confidentiality.

3. Confidentiality

- 2.1 Information must not be divulged to another agency or person without the consent of the informant. All requests for information from an outside organisation must be passed to the Operations Manager of Triple C before any action is taken. The only exception is where there is clear evidence of misconduct, serious danger to the staff member or to other persons in the community. *Such information should then only be divulged after discussion with a Trustee.*
- 2.2 Any disclosure of such confidential information must remain limited to the strict needs of the situation at the time, and the staff member should not assume authority to reveal matters, which are not relevant to that situation.
- 2.3 Staff members must ensure that documentation relating to service users, is only kept for legitimate purposes (GDPR compliant) and is kept in a secure place at all times.
- 2.3 Contact details for service users should be safely stored and only shared for legitimate purposes and with appropriate consent.
- 2.3 All reasonable steps must be taken to ensure documentation which includes personal information (beyond names) should not be left in places where they may be seen by those without a legitimate reason to see them, for example staff and volunteers leading activities.
- 2.4 Confidential interviews must not be held in places where they can be overheard. No one should be asked to give personal information in, for example, a hall, over a counter, or in a place such as a passage or stairs where it may be overheard by others.

4. Third parties

- 3.1 It is not only service users who have the right to confidentiality. Third parties, e.g. other agencies, must not be quoted without their permission, or discussed with service users without the agreement of the third party. Discussion about service users must not take place in a public place and must be conducted at all times in a manner conducive to creating an atmosphere of trust.
- 3.2 Information must not be given to a third party over the telephone without the sanction of the original informant or service user.
- 3.3 If personal information is to be transmitted to a third party, e.g. to another agency or an internal committee of Triple C then the information to be transmitted must be clearly agreed between the

staff member and the subject of the transmission. In certain circumstances, it may be advisable for the subject to be given details in writing of the information to be submitted and signify his/her agreement by signing and returning the document.

- 3.4 The recording of this information is another aspect of confidentiality, and all information of this kind should be stored appropriately.
- 3.5 Care should be taken to ensure that when records are destroyed this is done effectively (e.g. through shredding, deleting from computers or appropriate recycling methods that maintain confidentiality).

5. Breach of confidentiality.

If an individual is found to have breached this policy, depending on the severity of a breach, the individual could be subject to disciplinary proceedings.