

## Confidentiality Policy

Rochdale Connections Trusts' staff and volunteers handle a great deal of information, in both paper and electronic formats. Some of this is the personal data of beneficiaries, suppliers, staff, volunteers, supporters/campaigners, donors and trustees and is covered by our Data Sharing Code of Practice. Information about Rochdale Connections Trust and its work is also sensitive and confidential and could, if disclosed, have adverse implications for the Charity. The confidentiality policy and associated procedures set the framework within which personal and any other potentially sensitive information is to be collected, stored, handled and disclosed.

Most breaches of confidentiality happen through lack of thought or consideration of the possible consequences, or a lack of private or secure facilities. The best protection against breaches of confidentiality is to keep to a minimum the number of people who have access to sensitive information. Anyone worried or distressed by something they hear or read should seek guidance and support from their manager. Rochdale Connections Trust is committed to providing a confidential service to all of its users. No information given to the Organisation will be shared with any other organisation or individual without the user's expressed permission.

For the purpose of this policy, confidentiality relates to the transmission of personal, sensitive or identifiable information about individuals or organisations (confidential information), which comes into the possession of the Organisation through its work.

The Organisation holds personal data about its staff, service-users, volunteers etc which will only be used for the purposes for which it was gathered and will not be disclosed to anyone outside of the organisation without prior permission. All personal data will be dealt with sensitively and in the strictest confidence internally and externally.

### Purpose

The purpose of the Confidentiality Policy is to ensure that all staff, members, volunteers and service-users understand the Organisations requirements in relation to the disclosure of personal data and confidential information.

### Principles

- All personal paper-based and electronic data must be stored in accordance with the Data Protection Act 1998 and must be secured against unauthorised access, accidental disclosure, loss or destruction.
- All personal paper-based and electronic data must only be accessible to those individuals authorised to have access.

### Statistical Recording

The Organisation is committed to effective statistical recording of the use of its services in order to monitor usage and performance.

All statistical records given to third parties, such as to support funding applications or monitoring reports for the local authority shall be produced in anonymous form, so individuals cannot be recognised.

All documentary or other material including any downloaded data onto a laptop or PC, USB drive or any other storage device containing confidential information must be kept securely at all times when not being used by a member of staff and must be returned to the organisation at the time of termination of employment, or at any other time upon request.

Conversations relation to confidential matters affecting the organisation, employees, service-users, volunteers etc should not take place in situations where they can be overheard.

The contents of this Confidentiality Policy shall continue to apply for the termination of employment from this Organisation without limit in point of time but shall cease to apply to information ordered to be disclosed by a Court of competent jurisdiction or otherwise required to be disclosed by law.

## **Records**

All paper records are kept in locked filing cabinets. All information relating to service users will be left in locked drawers. This includes notebooks, copies of correspondence and any other sources of information.

## **Breaches of Confidentiality**

As an organisation working with highly vulnerable children, young people and adults there are occasions that may arise where individual workers are required to breach confidentiality. Confidential or sensitive information relating to an individual may be divulged where there is risk of danger to the individual, a volunteer or employee, or the public at large, or where it is against the law to withhold it. In these circumstances, information may be divulged to external agencies including the police or social services on a need to know basis. This is communicated in verbal and written format to all service-user's as part of their initial assessment following referral.

Where a worker feels confidentiality should be breached the following steps will be taken:

- The worker should raise the matter immediately with their Line Manager.
- The worker must discuss with the Line Manager the issues involved in the case and explain why they feel confidentiality should be breached and what would be achieved by breaching confidentiality. The Line Manager should take a written note of this discussion.
- The Line Manager is responsible for discussing with the worker what options are available in each set of circumstances.
- The Line Manager is responsible for making a decision on whether confidentiality should be breached. If the Line Manager decides that confidentiality is to be breached then they should take the following steps:

The Line Manager should contact the Chair in the first instance, or Vice Chair of the Board of Trustees and brief the Chair/Vice Chair on the full facts of the case, ensuring they do not breach confidentiality in doing so. The Line Manager should seek authorisation to breach confidentiality from the Chair/Vice Chair.

If the Chair/Vice Chair agrees to breach confidentiality, a full written report on the case should be made and any action agreed undertaken. The Line Manager is responsible for ensuring all activities are actioned.

If the Chair/Vice Chair does not agree to breach confidentiality then this is the final decision of Rochdale Connections Trust.

Further, employees of this Organisation will be aware of our Data Sharing Code of Practice in relation to data security and ensure strict adherence to the provisions therein at all times. Personal data about the Organisation's employees, service-users, volunteers etc is to be handled with utmost care and you must ensure that compliance with our Data Sharing Code of Practice is ensured. If you become aware of a data breach you must inform your Line Manager as a matter of urgency.

### **Legislative Framework**

The Organisation will monitor this policy to ensure it meets statutory and legal requirements including the Data Protection Act, Children's Act, Rehabilitation of Offenders Act and Prevention of Terrorism Act. Training on the policy will include these aspects.

### **Ensuring the Effectiveness of the Policy**

All members of the Board receive a copy of the Confidentiality Policy as they commence in post and this is re-issued every 12 months. Existing and new workers will be introduced to the confidentiality policy via induction and training. The policy will be reviewed annually and any amendments will be proposed and agreed by the Board of Trustees.

### **Non-adherence**

Breaches of this policy will be dealt with under the Grievance and/or Disciplinary procedures as appropriate.

### **REVIEW SCHEDULE:**

The Confidentiality Policy is formally reviewed on an annual basis.

**Date of last review:** August 2023

**Reviewed by:** Lizl Donnelly

**Job Role:** Business Support Manager

**Next Review Date:** August 2024