READING ASSOCIATION
FOR THE BLIND
WALFORD HALL
CAREY STREET
READING RG1 7JS

RAB (Reading Association for the Blind) Confidentiality Policy

General principles

Reading Association for the Blind (RAB) recognises that colleagues (employees, volunteers, and trustees) gain information about individuals and organisations during the course of their work or activities. In most cases such information will not be stated as confidential and colleagues may have to exercise common sense and discretion in identifying whether information is expected to be confidential. This policy aims to give guidance but if in doubt, seek advice from your line manager.

This policy should be read in conjunction with the RAB Data Protection Policy

- Colleagues are able to share information with their line manager in order to discuss issues and seek advice.
- Colleagues will avoid exchanging personal information or comments about individuals with whom they have a professional relationship.
- Be aware that not everyone is comfortable discussing their private life and may find personal questions intrusive.
- Colleagues will avoid talking about private or confidential information regarding the organisation and associated individuals in social settings.
- Colleagues will not disclose to anyone, other than their line manager, any information considered sensitive, personal, financial or private without the knowledge or consent of the individual, or an officer, in the case of an organisation.
- There may be circumstances where colleagues would want to discuss difficult situations with each other to gain a wider perspective on how to approach a problem. The organisation's consent must be sought before discussing the situation, unless the colleague is convinced beyond doubt that the organisation would not object to this. Whenever possible, discussions of sensitive issues should take place with names or identifying information remaining confidential.
- Where there is a legal duty on RAB to disclose information, the person to whom the confidentiality is owed will be informed that disclosure has or will be made.

Why information is held

- Most information held by RAB relates to individuals, their support needs, and the history of support they have received from RAB. RAB also holds information on other organisations, including contact details of individuals within them.
- Information is kept to enable RAB colleagues to understand the history and activities of individuals or organisations in order to deliver the most appropriate services.
- Information that is used when reporting to funders is fully anonymised to ensure confidentiality.
- Demographic information is kept for the purposes of monitoring our equal opportunities policy and also for reporting back to funders.

Access to information

- Information is confidential to RAB as an organisation and may be passed to colleagues, line managers or trustees to ensure the best quality service for users.
- Where information is sensitive, e.g. containing personal details, it will be confidential to the employee dealing with the case and their line manager.
- Colleagues will not withhold information from their line manager unless it is purely personal.
- Users may have sight of RAB records held in their name or that of their organisation. The request must be in writing to the Chief Executive Officer (CEO) giving 14 days' notice and be signed by the individual, or in the case of an organisation's records, by the Chair or CEO. Sensitive information as outlined above will only be made available to the person or organisation named on the file.
- Employees may have sight of their personnel records by giving 14 days' notice in writing to the CEO.
- When photocopying or working on confidential documents, colleagues must ensure people passing do not see them. This also applies to information on computer screens.
- Organisations must be able to prove that any information they hold on an individual is necessary to the running of the organisation. RAB colleagues are therefore expected to only record essential information and, as per our safeguarding policy, when recording or discussing sensitive matters written records must be restricted to the facts and not record the reporter's opinions.

Storing information

Information on service users, employees, volunteers, and other individuals working within RAB will be stored on the Password protected Charity Log CRM and BrightPay payroll portal. Information on payments to individuals is also stored on RAB's password protected online banking system. Any confidential information stored on Office 365 will be restricted to those requiring access. Paper record-keeping is kept to a minimum. Staff communicate on the Teams system and have a WhatsApp Chat. The primary channel for communication about service users cases is Charity Log but in certain circumstances operational necessity requires service users to be referred to on Teams or WhatsApp. Service users must be referred to by Charity Log ID number, not name, on Teams and WhatsApp.

Charity Log permissions are set so that users can only access operationally essential information.

Staff records are restricted to the line manager of the member of staff, and the CEO where they are not the line manager. Historic personell records (created before RAB started using Charity Log and not yet due for deletion) are on the CEO's password-protected One Drive. Historic paper personell records (created before RAB switched to digital record-keeping and not yet due for deletion) are kept in sealed envelopes in a locked office.

Duty to disclose information

There is a legal duty to disclose some information including:

- Safeguarding Concerns (see the RAB Safeguarding Policy) – these will be reported to the Local Authority
- Where colleagues believe an illegal act has taken place - this will be reported to the police.
- The subject of the disclosure has a right to be informed. If it is not deemed advisable to inform them (e.g. if this would pose a risk to the person making the disclosure) then this must form part of the report to the appropriate authorities.

Data Protection Act

Information about individuals, whether on computer or on paper, falls within the scope of the Data Protection Act and must comply with the data protection principles.

These are that personal data must be:

- Obtained and processed fairly and lawfully.
- Held only for specified purposes.
- Adequate, relevant and not excessive.
- Accurate and up to date.
- Not kept longer than necessary.
- Processed in accordance with the Act.
- Kept secure and protected.
- Not transferred out of Europe.

The RAB Data Protection Policy contains more information on how RAB complies with the Data Protection Act.

Breach of confidentiality

Colleagues who are dissatisfied with the conduct or actions of other colleagues or RAB should raise this with their line manager using the grievance procedure, if necessary, and not discuss their dissatisfaction outside RAB

Colleagues accessing unauthorised files or breaching confidentially may face disciplinary action.

Whistle blowing

All colleagues hold the right to inform either their manager or one of the trustees if they believe that RAB is being brought into disrepute by the actions of another colleague or trustee.

Reviewed July 2022
Review due July 2024