



Royal Association for Deaf people

Confidentiality policy

Version number	Date	Author	Purpose
001	October 2019	Joint CEO	Policy review
002	February 2023	Joint CEO	Policy review

Executive summary

[Click here for BSL](#)

RAD is committed to the confidentiality of information about the organisation and the people who use our services. Colleagues may have access to confidential information during the normal course of their duties. No information regarding a client shall be given directly or indirectly to any third party outside of RAD without the client's permission, unless there is an immediate risk of harm or where a crime has been committed, or a threat to commit a crime is declared (refer to Safeguarding Policies and Procedures).

Unauthorised disclosure of personal information, or details of RAD as an organisation, will be dealt with under RAD's Disciplinary Procedure.

Full policy

Policy Statement

RAD is committed to the confidentiality of information about the organisation and the individuals who use our services. We recognise that all clients should be able to access services and ask for advice in confidence. Where there are concerns about an individual or situation, colleagues must disclose these concerns to their line manager or a member of the executive team within RAD. Disclosure within the organisation is not a breach of confidentiality.

There are exceptions to our commitment to keeping information confidential, these are as follows:

- Where there is a safeguarding concern in relation to a child, young person or vulnerable adult. This could be where:
 - An individual has been abused / harmed by someone else
 - A person plans to or has harmed / abused another person
 - A client tells you they plan to self-harm
- When there are concerns about financial irregularities, such as money laundering or embezzlement
- When a crime (or the intention to commit a crime) against a person or property has been disclosed
- Where information related to terrorism or suspected terrorism is disclosed

Author: Joint Chief Executives
Date of review: February 2023

If it is safe to do so, the client will be told that the information is going to be shared. See further details regarding what actions to take below.

Unauthorised disclosure of personal information, or details of RAD as an organisation, will be dealt with under RAD's Disciplinary Procedure. Deliberate unauthorised access to confidential information is a serious matter and will also be dealt with under RAD's Disciplinary Procedure.

Every colleague receives induction in which confidentiality is explained and they are required to sign a Code of Confidentiality or Confidentiality Agreement at the commencement of their employment or period of voluntary work. For paid staff this is contained within the Contract of Employment.

The policy in practice

Colleagues may have access to confidential information in the normal course of their duties. No information regarding a client shall be given directly or indirectly to any third party outside of RAD without the client's permission, unless there is an immediate risk of harm, or where a crime has been committed, or a threat to commit a crime is declared (refer to Safeguarding Policy and Procedures).

As a service-delivery organisation within the Deaf Community we recognise and accept that the community is small, and that confidentiality concerns might arise linked to the venue of a service, or a relationship with an appointed support worker/service colleague. All efforts will be made to ensure that colleagues are able to adjust support in order to ensure that a client feels comfortable.

Statistical recording

The statistical recording of service data enables us to monitor and quality ensure our services. It also helps us to identify any policy issues that may arise from our services; and as such, we are committed to ensuring that our statistical recording and reporting is as effective as possible.

All statistical records given to third parties, such as to funders (to support applications and monitor services) will be produced in anonymous form so that individuals cannot be recognised.

Client files

All client files and related documents must be stored in locked filing drawers/cabinets and files must be secured at the end of each working day. This includes notebooks, copies of correspondence, case notes and any other sources of information.

Consent to sharing information

Where support is commissioned by a local authority, or other body/individual, the nature of information that will be shared and or disclosed will be determined at the beginning of the contracted work, by both the clients and the commissioner.

Where RAD agrees to act on behalf of a client, it is the responsibility of the support worker or service delivery colleague to ensure that all clients sign a consent form. This form should be placed on the client's file. Service delivery colleagues are responsible for checking and maintaining accurate contact information for active clients/cases.

All details of express consent must be recorded on the client's file.

Breaches of Confidentiality

There are occasions when confidentiality must be breached. Colleagues with concerns about safeguarding issues in relation to a child, young person or adult should refer to the policy for the Safeguarding of Children or the Adult Safeguarding Policy, both of which provide step-by-step guidance on the procedures that need to be followed.

Should concerns relate to terrorism or a crime, including disclosure of information relating to the harm of a child or adult or against a RAD colleague or property, this must be reported immediately in line with the Safeguarding Policy and Procedures. In the event of any uncertainty, or to avoid delay – contact the CEO.

Procedures

- All records, paper and computerised, are subject to GDPR and must not be disclosed to an unauthorised person
- Security passwords must not be disclosed to unauthorised persons
- Unauthorised access to RAD's computers is not allowed
- Paper records of clients, colleagues, or any other confidential information, must be stored in an area that is secure from unauthorised access out of office hours and does not allow access by unauthorised persons. It is recommended that lockable metal filing cabinets or other secure means be used to store files to prevent unauthorised access
- All alterations or additions made to client files or personal records should be dated and signed
- Confidential matters should not be discussed in public places
- Every colleague is prohibited from discussing confidential client (client) related issues with family and friends – this includes withholding the client's name but still disclosing information that could identify them
- Any colleague involved in a recruitment selection procedure should declare any relationship or specific contact between themselves and the candidate
- Every colleague has a duty of confidentiality that applies throughout their employment or period of voluntary work including notice periods. This continues beyond employment. This is covered in the Contract of Employment
- A clear desk policy should be adopted in all times. Confidential information should not be left on desks or in filing trays or on public view, i.e., 'post it' notes on walls, desks or computers. This applies whether offices are locked or there are colleagues on the premises
- If, by the requirements of their employment, colleagues take confidential files out of a RAD office, the following protocols must be followed:
 - The files must be carried and stored discreetly and securely
 - Colleagues must have the consent of their line manager prior to removing client files from a RAD office

Author: Joint Chief Executives
Date of review: February 2023

- Files should never be left on car seats or in a car overnight
- Any files removed from a RAD office must be recorded, dated and signed in a suitable book and signed in again when returned

Strictest confidentiality is required when carrying out a home visit to a client on behalf of RAD. Details of the client's home, personal circumstances or family should not be disclosed or commented on unless directly relating to the situation in hand and then only with the client's permission. Two exceptional areas of disclosure would be in the case of:

- The risk of significant harm or death
- The abuse of a child or vulnerable adult
- Interviews or discussion with clients of RAD should be carried out in a manner that ensures that privacy and dignity are maintained
- In the event of an emergency, and to avoid harm to clients and prevent serious infringement of the law, colleagues are encouraged to share and disclose information with their line manager
- Where clients of RAD have difficulty maintaining their own privacy and dignity, colleagues are responsible for providing sympathetic help and support

/