

Responsible Team Delegate	EMSD
Approving Officer	CEO
Date Adopted	03 March 2020

1.0 Purpose

The purpose of this policy is to ensure that management of personal information for both clients and staff meets all relevant legislative and regulatory requirements.

2.0 Scope

The *Privacy Act (2009) Qld* and *Information Privacy Act (2009)* only applies to personal information. This means information, or an opinion, that is recorded in any form (whether true or not) about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. Personal information may be of a sensitive or routine nature. Sensitive information, of which personal health information forms a part, is subject to higher privacy standards.

This policy outlines for both staff and clients how Richmond Fellowship Queensland (RFQ) will manage their personal information.

3.0 Policy

RFQ is committed to quality and ethical relationships and practices in all aspects of its work. This commitment includes protecting the privacy of personal information, in accordance with the Australian Privacy Principles (APPs) set out in the *Privacy Act (2009) Qld* and in accordance with the Information Privacy Principles (IPPS) set out in the *Information Privacy Act (2009)*.

RFQ values the privacy of every individual's personal and health information and is committed to open and transparent management of the information it holds and uses about all individuals who provide personal information to us.

4.0 Procedural Requirements

4.1 What personal information do RFQ collect and hold?

Personal information collected and held by RFQ may include name, date of birth, gender, current and previous addresses, residency status, telephone/mobile phone number, e-mail address, bank account, tax file number, driver's licence number, Centrelink information, photographs, race or ethnicity.

Health information which RFQ collect may include:

- medical information, when this is collected or used in connection with delivering services to clients, or when it is predictive of a client's ongoing health;
- personal details, which for clients may include admission and discharge dates; and
- information generated by a health service provider, such as notes and professional opinions in relation to a client's health.

4.2 How does RFQ collect personal information?

- Directly from clients, when they provide information orally or in writing;
- From third parties, such as medical practitioners, government agencies, client representatives, carer/s, and other health service providers;
- From client referrals; and
- From publicly available sources of information.

RFQ will:

- obtain client consent to collect sensitive information, such as information related to health, unless an exemption applies, e.g. the collection is required by law, court/tribunal order or is necessary to prevent or lessen a serious and imminent threat to life or health;
- only collect sensitive information necessary to support roles, functions or activities with RFQ;
- collect sensitive information directly from clients if it is reasonable and practicable to do so;
- use fair and lawful ways to collect sensitive information, and not in an intrusive manner; and
- give clients an option of interacting anonymously, if lawful and practicable to do so.

Should RFQ obtain unsolicited personal information about clients RFQ may use or disclose this information to clients, or other parties, to ensure the information is necessary to support roles, functions or activities with RFQ.

4.3 Who collects your personal information?

Client's personal and sensitive information (including health information) is collected by authorised representatives of RFQ in the course of their normal duties and for the organisation's own use.

4.3.1 Collection of personal information - staff

Staff will be provided a copy of this policy at the time they are sent a letter of offer and employment contract, as they are required to complete and return documentation to RFQ which contains personal information.

All information supplied by staff will be placed on their personnel file which is held in both electronic and hard copy format. Both formats are securely held with access only available to those staff members who need to access the files to perform their role.

4.3.2 Collection of personal information – clients

Client personal and sensitive information, such as health information, shall only be obtained by lawful and fair means from clients, or other sources, as is necessary to support client functions or activities with RFQ.

Clients shall be provided with the *Client Consent Form* at the time of commencing to receive services from RFQ. This form shall be signed and uploaded into the client's file in the Client Information Management System. All client files and personal information is securely held with access only available to those staff members who need to access the files to perform their role.

4.4 The purpose for collecting personal information

A client's personal information is used to:

- assess and provide the services that are required;
- administer and manage those services;
- evaluate and improve the services that RFQ offers;
- contribute to research in the health, functioning and needs of people in recovery;
- contact family, carers, or other third parties as and if required; and
- meet obligations under RFQ's contract with our Government funding bodies.

As a staff member or potential staff member information is used to:

- assess an employment application;
- process payment of salary and any salary sacrifice payments and meet legislative obligations such as the payment of superannuation and taxation;
- obtain relevant security clearances required to perform roles within RFQ;
- meet duty of care obligations, particularly in relation to any disclosed medical conditions;
- contact family, carers, or other third parties as and if required; and
- ensure that staff hold a current driver's licence and private motor vehicle registration as required to perform their role.

If RFQ is not able to obtain personal information, it may limit RFQ's ability to provide a quality service, or meet duty of care and legislative responsibilities as an employer and service provider.

4.4.1 Unsolicited personal information

Unsolicited information is information received about either a staff member, prospective staff member, or a client that was not requested or sought by RFQ.

If this occurs RFQ is required to determine if RFQ could have collected the information if solicited. RFQ can do that by disclosing the information to the staff member, client or other parties. If it is determined that the information could not have been obtained by us then the information must be destroyed, if it is lawful and reasonable to do so. If it is determined the information could have been obtained, then it is to be placed on the staff or client file and used in the provision of employment and support functions and activities.

4.5 When do RFQ disclose personal information?

RFQ respects and shall uphold a client's right to privacy and confidentiality, to the extent that it does not impose a serious risk to the client and/or others. For the purposes set out above, RFQ may disclose clients' personal information to people, organisations or service providers outside RFQ. This may include disclosure to:

- medical and allied health service providers who assist with the services RFQ provide to clients;
- a 'person responsible' if the client is unable to give or communicate consent e.g. next of kin, carer, or guardian;
- the client's authorised representative/s e.g. legal adviser;
- RFQ's professional advisers, e.g. lawyers, accountants, auditors;
- regulatory authorities, e.g. Centrelink, Queensland Health, the Australian Taxation Office;
- organisations undertaking research where information is relevant to public health or public safety; and
- when required or authorised by law.

4.6 Disclosure of personal information overseas

Whilst your personal information is only disclosed as detailed above, RFQ does utilise a provider for email anti-spam whose servers are located in both the USA and Europe. This means that any emails sent through an RFQ email address will be passed offshore through these servers for processing. No data contained within these emails is either stored or copied to these overseas servers and only header data is displayed on emails that are quarantined due to anti-spam detection.

4.7 Accessing your personal information

Staff and clients can request and be granted access to their personal information, subject to exceptions allowed by law.

Any requests for access to personal information must state what information is to be accessed and should be forwarded to the responsible Manager either verbally, or in writing to:

Richmond Fellowship Queensland
PO Box 655
ANNERLEY Q 4103

On receipt of a request to access information the Manager will then assess the granting of access based on current issues that may exist with the staff or client, and whether these issues relates to any exceptions allowed by law to granting access to personal information.

Should the Manager decide that access to personal information will not be given they shall put the reasons for the refusal and the mechanisms available to complain in writing to the staff or client within 30 days of receipt of the request.

Should access be granted the Manager is to contact either the staff or client and arrange for access to their personal information. Access will normally be provided by sighting personal information in the company of staff.

Should RFQ incur charges in providing access RFQ may charge the staff member, or client for the associated costs, as long as they are reasonable.

4.8 Security of personal information

RFQ take all reasonable steps to protect personal information from loss, interference, misuse, unauthorised access, modification, or disclosure. RFQ will destroy, or permanently de-identify personal information that is no longer needed, is unsolicited and RFQ could not have obtained this information directly, or is not required to be retained by, or under, an Australian law or a court/tribunal order. Appropriate security measures are in place to protect electronic materials and materials stored and generated in hard copy. RFQ has an archiving process for client files which ensures files are securely and confidentially stored and destroyed in due course.

4.9 Help to ensure RFQ hold accurate information

RFQ take all reasonable precautions to ensure that the personal information RFQ collect, use and disclose is accurate, complete, up-to-date, relevant and not misleading. The accuracy of the information RFQ holds often depends on the quality of the information provided including any changes. When RFQ receives advice that personal information has changed, or is incorrect, RFQ

will update records and if requested will advise other parties of the correction where practicable and lawful to do so. There will be no charge for any correction of personal information.

Should RFQ be unable to correct your personal information RFQ will provide a written notice outlining the reasons for the refusal, the mechanisms available to complain about the refusal and any other matter prescribed by regulations.

Staff are required when reviewing a client's service to confirm the accuracy of the personal details that are currently held on the client's files. Any changes are to be noted on the clients file.

Where RFQ may have previously disclosed client personal information to other parties, should the client request us to notify these parties of any change to their details, RFQ must take reasonable steps to do so.

4.9.1 Staff

All staff shall notify corporate support of any changes to their personal information such as a change of address, bank details, superannuation fund, or private motor vehicle being used for work purposes.

At regular intervals RFQ will issue all staff, via email, a staff details form to complete and return to ensure personal information is up to date.

4.10 Breach of Privacy

When RFQ is aware of a breach in privacy (computer system hacked, laptop stolen etc.) to client's personal information the Chief Executive Officer will immediately notify the relevant funding body as per their service agreement guidelines. Also refer to the *Data Breach Policy*.

4.11 Complaints

If either a staff member or client has any questions or concerns about RFQ's privacy practices, in the first instance they should approach their support worker or manager.

If a client's concerns are not able to be resolved, they shall be referred to the Client Privacy Collection Statement and Client Complaints information sheets available to the public on the RFQ website www.rfq.com.au, and handled in accordance with the *Client Complaints and Disputes Policy*.

If a staff member's concerns are not able to be resolved, the *Governance Policy G10 – Formal Disputes Process* shall be applied.

4.12 Direct marketing opt out requests

RFQ does not use any personal information held for the purpose of direct marketing.

5.0 Related Documents

- Quality Management System Manual
 - Data Breach Policy and Assessment Tool
 - Acceptable Use of Information Communication Technology Policy
 - BYO Device Policy
 - RFQ Human Resource processes
 - Client Files Archiving Policy
 - Case Note Recording Guideline
 - Client Complaints and Disputes Policy
 - Client Privacy Collection Statement Information Sheet
 - Client Consent Form
 - RFQ Ethical Code and Guidelines Information Sheet
 - Client Complaints Information Sheet
 - Client Rights and Responsibilities Information Sheet
 - Measures Collection Information Sheet
 - Family Member / Carer Rights and Responsibilities Information Sheet
 - Audit Participation Consent Form
- Other - Governance Policy G10 – Formal Disputes Process