RIVERSIDE
STUDENT SUPPORT CENTRE

2025
RIVERSIDE STUDENT SUPPORT CENTRE
PRIVACY POLICY

DOCUMENT DETAILS

Version	Date Amended	Person Responsible	Date for next review (Annually or when processes change)
2025 Version 1	27/12/2024	Kate Bevan	27/12/2025

CONTENTS

GENERAL OUTLINE

FEDERAL PRIVACY LAWS AND RIVERSIDE STUDENT SUPPORT CENTRE (RSSC)

RSSC is bound by the *National Privacy Principles*, *The Privacy Act 1988* including the Privacy Amendment (Notifiable Data Breaches) Act 2017. This act is available at https://www.legislation.gov.au/C2004A03712/latest/text.

WHAT KIND OF INFORMATION DOES RSSC COLLECT?

RSSC can collect information about:

- clients and parents and/or guardians before, during and after the course of a client's enrolment at RSSC
- job applicants, staff members, volunteers and contractors
- other people who come into contact with RSSC.

PERSONAL INFORMATION PROVIDED TO US BY THE INDIVIDUAL

RSSC will generally collect personal information then hold about an individual by way of forms filled out, face-to-face meetings, interviews, telephone calls and other communications such as text or email. On occasions people other than staff, parents and clients provide personal information.

PERSONAL INFORMATION PROVIDED BY OTHER PEOPLE

In some circumstances we may be provided with personal information about an individual from a third party, for example a report provided by a medical professional or a reference from another organisation. If you provide information to us about other people, we encourage you to inform them that you have provided us with information.

HOW WILL RSSC USE THE PERSONAL INFORMATION YOU PROVIDE?

RSSC's primary purpose is for assistance and the duty of care of its clients. We will use personal information from an individual for the primary purpose and for such other secondary purposes that are related to the primary purpose, including:

- Keeping parents informed about matters related to their child, through correspondence, newsletters, magazines and reports.
- Day-to-day administration.
- Looking after client's emotional, social and medical well-being.
- Seeking donations and marketing for RSSC.
- To satisfy RSSC's legal obligations and allow RSSC to discharge its duty of care.

CONSEQUENCES OF NOT SUPPLYING INFORMATION

If we do not obtain the information referred to above we may not be able to enrol or continue the enrolment of a client. If you do not agree to this, please advise us in writing.

JOB APPLICANTS, STAFF MEMBERS AND CONTRACTORS

In relation to personal information of job applicants, staff members and contractors, our primary purpose of collection is to assess and (if successful) to engage the applicant, staff member or contractor. The purposes for which we use this information include:

- administering the individual's employment or contract
- insurance purposes
- seeking funds and marketing for RSSC
- conducting checks including but not limited to Disability Worker Exclusion scheme, national/international police checks and working with children checks
- satisfying RSSC's legal obligations, for example, in relation to child protection legislation.

WHO MIGHT RSSC DISCLOSE PERSONAL INFORMATION TO?

RSSC may disclose personal information, including sensitive information, held about an individual to:

- another centre, or school as required
- government departments
- medical Practitioners
- people providing services to RSSC
- recipients of centre publications, like newsletters and magazines
- parents
- anyone an individual authorise RSSC to disclose information to.

We will obtain your consent to share sensitive information as per the form in the Appendix.

HOW WILL RSSC TREAT SENSITIVE INFORMATION?

'Sensitive information' is defined in the Privacy Act to mean information or an opinion about an individual's:

- racial or ethnic origin
- political opinions
- membership of a political association
- religious beliefs or affiliations
- philosophical beliefs
- membership of a professional or trade association
- membership of a trade union
- sexual preferences or practices
- health information and genetic information (that is not otherwise health information)
- criminal record.

Unless a client or staff member agrees otherwise, or is allowed by law, sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose.

MANAGEMENT AND SECURITY OF PERSONAL INFORMATION

RSSC has in place steps to protect the personal information RSSC holds from misuse, loss, unauthorised access, modification or disclosure by use of various methods including locked storage of minimal paper records and pass-worded access rights to computerised records. This is outlined in our *Process and Protocol Document*.

UPDATING PERSONAL INFORMATION

RSSC endeavors to ensure that the personal information it holds is accurate, complete and up-to-date. A person may seek to update their personal information held by RSSC by contacting RSSC at any time.

YOU HAVE THE RIGHT TO CHECK WHAT PERSONAL INFORMATION RSSC HOLDS ABOUT YOU

Under the *Commonwealth Privacy Act,* an individual has the right to obtain access to any personal information which RSSC holds about them and to advise RSSC of any perceived inaccuracy. To make a request to access any information RSSC holds about you or your child, please write to: kate@rssc.org.au.

YOUR PERSONAL HEALTH INFORMATION

OUTLINE

The *Privacy Act 1988* (Privacy Act) protects client's personal information. Personal information is information or an opinion that identifies a client or could identify a client, and includes information about a client's health.

RSSC may have cause to obtain, record and share health information.

Health information is any information about a client's health or a disability, as well as any other personal information collected while they are receiving a health service, including:

- notes about the symptoms described or the health service provider's observations and opinions of the client's health
- prescription information
- contact and billing details
- test results and reports, such as those relating to blood samples and X-rays
- dental records
- Medicare number
- private hospital and day surgery admission and discharge records
- other sensitive information about the client such as race, sexuality or religion.

HOW WE HANDLE HEALTH INFORMATION

Health information is sensitive information under the Privacy Act. This means there are added restrictions on how health service providers can handle health information compared to other types of personal information.

A health service provider (provider) is any organisation that:

- assesses or records information about your health, including any disability
- maintains or improves your health, including any disability
- gives out prescription drugs or medicines.

Generally, a provider can only collect a client's health information when:

- a client consents to them doing so, and
- the information is reasonably necessary for them to carry out their functions or activities (such as diagnosing or treating your illness).

A provider should only collect a client's health information directly from the client, unless it is unreasonable or impractical for them to do so. If we are going to collect information about a client we will get them to fill in a consent form to authorise us to do this.

EXCEPTIONS

There are certain situations where a provider can collect a client's health information without their consent.

These situations include where getting a client's consent is not practical due to the circumstances but a provider reasonably believes that they need the information to lessen or prevent a serious threat to any individuals' life, health or safety, or the public's health or safety.

For example, in an emergency where a client is seriously injured, or unconscious, and requires urgent healthcare, a doctor could collect relevant health information about an individual from their family or General Practitioner (GP) without their consent so they can give them the healthcare they need.

CONSENT

When we obtain consent to collect a client's health information for a particular purpose, we should ensure the client understands what will happen to their information and what they are consenting to.

Consent should be given voluntarily. Clients also need to have the capacity to consent to their health information being collected. There may be situations where a guardian or person who is responsible for a client will need to provide consent on their behalf.

There may be times where consent to a provider collecting health information can be implied. For example, in a counselling session we would not normally need to specifically ask a client for permission to make notes of the information shared during an appointment because consent can be implied from a client's conduct in attending the appointment and participating in the session.

A client can withdraw consent to RSSC collecting their health information. However, this may impact on our ability to provide our services.

NOTICE

Generally, we will inform clients of the following:

- the purposes for which we are collecting their information
- the main consequences, if any, for the client if we do not collect their information
- any other third parties to which we usually disclose their information
- information about our privacy policy.

We inform clients of this verbally in the induction meeting, through our privacy policy and in our enrolment form.

Generally, we can only use and/or disclose health information for the particular purpose for which we originally collected the information (known as the 'primary purpose').

We can also use and/or disclose health information for another purpose (a 'secondary purpose') where the client consents to us doing so. We have a form for client's to fill out to enable us to do this. It is included at the end of this document and stored in the client's file.

EXCEPTIONS

There are situations where we can use and/or disclose health information for a secondary purpose even if a client has not consented to us doing so. These situations include where clients would be reasonably expecting us to use or disclose their health information for a secondary purpose that is directly related to the primary purpose of collection.

A 'reasonable expectation' about what health information might be shared with other providers might vary depending on the situation. For example, where a GP refers someone to a specialist doctor for the treatment of a serious condition, it may reasonably be expected the GP to give the specialist doctor their complete medical history and any related test results so the specialist doctor can decide how to treat the client's condition.

DIRECT MARKETING

We can only use and/or disclose a client's health information for direct marketing purposes where they have consented to us doing so.

Where a client has previously consented to receiving direct marketing from us, we should provide them with the option of stopping any more marketing communications in the future.

CAN CLIENTS USE OUR SERVICES ANONYMOUSLY?

There may be situations where a client does not want to give their identity information (such as name) to us. Clients have a right to not identify themselves, or to use a pseudonym, when dealing with providers. However, a provider does not have to provide a client with these options where it is impractical to do so or they are required or authorised by law to deal with identified individuals. Given the nature of services we provide at RSSC we do not provide our service anonymously.

CLIENT ACCESS AND/OR CORRECTING HEALTH INFORMATION

Access

Generally, clients have the right to ask us for access to records of their health information in a particular way and we are required to give them access to that information in the way the client has requested. However, there are some situations where we can refuse the access request or give the client access in a

different way from that which they requested. For example, we may be allowed or required to refuse access because of a law or a court/tribunal order.

Correction

The client has a right to ask us to correct information they think is not accurate in their health information records. However, we can refuse this request where for example, we have taken reasonable steps to satisfy them that the information is accurate.

MAKING A COMPLAINT

Clients can make a complaint if they believe we have not handled their health information properly under the APPs.

Client's should first make a complaint to us as outlined in our *Complaints and Grievances Policy* and give us an adequate opportunity to deal with the complaint. We will generally respond to the complaint within 30 days.

We cannot charge a client for making a complaint.

If the client is not satisfied with our response to their complaint, they may then complain to The Office of the Australian Information Commissioner. For more information about their process, please refer to the OAIC's privacy complaints webpage: https://www.oaic.gov.au/individuals/what-can-i-complain-about

NOTIFIABLE DATA BREACH SCHEME

OUTLINE

RSSC is committed to strengthening data protection as this benefits everyone and helps to reduce the risk of regulatory burdens, financial losses, damaged reputation, and loss of client trust. It also ensures we meet our obligations in regards to the safety of children and young people as set out in the Child Safe Standards.

We maintain a proactive approach when it comes to managing personal information and aim to develop a culture engrained in data privacy, ensuring that any client information collected is treated as an asset to be protected and managed with the utmost care.

Currently the General Manager oversees the Data Breach policy and procedure and should be the first point of contact if you suspect a data breach, want to report a data breach or have any questions regarding data breaches. More information is available in the *Riverside Student Support Centre Data Breach Policy*.

OUR OBLIGATIONS

Under the new National Data Breach scheme, we have data breach notification obligations when a data breach is likely to result in serious harm to any individuals whose personal information is involved in the breach.

The scheme applies to all kinds of personal and sensitive information. Examples include names, addresses, email addresses, genders, family members, financial information, tax file numbers and medical history.

We take steps to ensure personal information is secure and safe and to avoid loss and unauthorised disclosure. The way we ensure the security of the data we collect is outlined in the *RSSC Process and Protocol* document.

NOTIFIABLE BREACHES

According to the *Privacy Amendment (Notifiable Data Breaches) Act 2017*, an 'eligible data breach' is notifiable when the following three criteria are satisfied:

1. There is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information that an entity holds.
2. This is likely to result in serious harm to one or more individuals. 'Serious harm' could include risks to personal safety, damage to reputation, or serious psychological harm.
3. The entity has not been able to prevent the likely risk of serious harm with remedial action.

The Notifiable Data Breach scheme only applies to eligible data breaches that occur from 22 February 2018. There are a few exceptions which may mean notification is not required for certain eligible data breaches.

IF A DATA BREACH OCCURS

If a notifiable breach has occurred, RSSC must report details of it to those affected by it, and to the OAIC (Office of the Australian Information Commissioner). The police may also need to be notified if a crime is suspected.

The notification must set out:

- the identity and contact details of the practice
- a description of the data breach
- the kind of information involved in the data breach
- recommendations about the steps that individuals should take in response to the data breach.

We will investigate the breach and to determine if serious harm is likely to occur. This needs to be done within 30 days of the breach. A review will then occur to determine what steps need to be taken to prevent any further harm or damage from happening. This will be discussed in the next staff meeting and action decided upon.

EXAMPLES OF NOTIFIABLE BREACHES

A data breach could occur due to a cyber attack, loss or theft of a device that contains sensitive personal information, or because personal information gets published or shared without authorisation (whether deliberate or inadvertent).

Examples of a data breach include when:

- any electronic or cloud-based database containing client records is hacked
- Client information is mistakenly provided to the wrong person (for example, via email)
- an electronic device containing records is lost or stolen.

CONCLUSION

RSSC understands an individual's right to keep their personal information private is highly important.

We are committed to protecting and maintaining the privacy, accuracy and security of personal information.

For more information, to raise a concern or to discuss the privacy policy please contact the General Manager: kate@rssc.org.au

This document has been prepared in accordance with the guidelines as set by the National Privacy Principles, the Health Privacy Principles and together with information from the office of the Federal Privacy Commissioner and Minter Allison.

Further information may be obtained by contacting the office of the Australian Information Commissioner (https://www.oaic.gov.au/).

APPENDIX

A: CONSENT TO SHARE INFORMATION FORM

The following is an example only please refer to the Consent to Share Information Form in the forms folder or ask the General Manager if you require this form.

Consent to share information

Purpose: to record freely given informed consumer consent to share their information with a specific agency/ies for a specific purpose/s.

Consumer

Name:

Date of Birth: dd/mm/yyyy / /

Sex:

UR Number:

or affix label here

Section 1: Personal/health information to be shared

Service Type Examples: – physiotherapy – counselling	**Name of Agency** Examples: – Strawberry Community Health centre – Blueberry City Council	**Type of Information** Examples: – all relevant information – exceptions as stated by consumer	**Purpose/s** Examples: – referral – shared care/case planning -- informing services participating in consumer's care

Section 2: Record of consent

☐ **Written consumer consent**

The worker/practitioner has discussed with me how and why certain information about me may be shared with other service providers, as above. I understand this and I give my consent for the information to be shared.

Signed:_____

Dated (dd/mm/yyyy): / /

or

☐ **Verbal consumer consent**

I have discussed with the consumer how and why certain information may be shared with other service providers. I am satisfied that this has been understood and that informed consent for the information to be shared as detailed above has been given.

or

☐ **Consumer does not have the capacity to provide consent**

(that is, they do not understand the nature of what they are consenting to, or the consequences)

☐ Consent given by authorised representative _____

(name of authorised representative)

☐ There is no Authorising representative or they were uncontactable; therefore, the information will be shared as set out in the *Health Records Act 2001**

Consent to Share Information

*If it is not reasonably practical to obtain consent from an authorised representative or the consumer does not have an authorised representative, health information can still be shared in the circumstances set out in the *Health Records Act 2001*. This includes where the sharing of information is done by a health service provider and is reasonably necessary for the provision of a health service or where there is a statutory requirement.

To ensure that the consumer's authorised representative can make an informed decision about consenting to the sharing of information as detailed above, the worker/practitioner should (tick when completed):

1. Discuss with the consumer the proposed sharing of information with other services/agencies ☐
2. Explain that the consumer's information will only be shared with these services/agencies if the consumer has agreed and, when referring, advise that referral for service can still proceed if the consumer does not want information disclosed ☐
3. Provide the consumer with information about privacy, such as the brochure *Your Information – It's Private* ☐
4. Provide the consumer with a copy of this form once completed. ☐

Produced by the Victorian Department of Health, 2012

Consent obtained/witnessed by: CSI Page 1 of 1

Name: Position/Agency:

Sign: Date: dd/mm/yyyy / / Contact number: