

RMEA Policy | Privacy Policy

Definitions

Term	Definition
Australian privacy principles (APP)	regulate the handling of personal information by both Australian government agencies and businesses.
Personal information	means information or an opinion (including information on an opinion forming part of a database) whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. Personal information includes name, address and contact details (e.g. phone, email, fax); photographs, video recordings and audio recordings of you; information about your personal circumstances (e.g. age, gender, occupation); information about your financial affairs (e.g. bank account details, credit card details); information about your identity (e.g. date of birth, drivers licence details); information about your employment (e.g. work history, referee comments, remuneration); information about your background (e.g. educational qualifications, languages spoken, English proficiency) and government identifiers (e.g. Centrelink Reference Number, Tax File Number).
Sensitive information	personal information 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 or criminal record.

Open and transparent management of personal information

Rural Medical Education Australia (RMEA) is committed to complying with the Australian privacy principles (APPs) as provided in the privacy amendment act 2012. In addition, RMEA complies with the health records act 2001 and all other applicable legislation. Further information on the privacy amendment act 2012 and the Australian privacy principles can be accessed via the Office of the Australian Information Commissioner: www.oaic.gov.au.

The APP policy is available to all stakeholders. The policy may be accessed on the RMEA website (www.RMEA.org.au), and on the RMEA server. A copy of the APP policy is available upon request.

RMEA has committed to comply with all Australian privacy legislation by appointing a privacy officer to provide information, advice and to monitor adherence to the APP across the organisation. The position of privacy officer is to be assumed by the Chief Executive Officer (CEO). The APP policy will be reviewed annually with reference to the relevant legislation. Any amendments will be actioned and communicated to all stakeholders.

What personal information does RMEA collect?

RMEA will only collect personal information that is reasonably necessary to conduct its core functions or activities. Examples of personal information that RMEA collects includes:

- Your name, residential and work contact details
- Your academic and employment history including medical registration details, exam results or supervisor feedback
- RMEA may collect personal information which is regarded as “sensitive information” (as defined under the act). An example of sensitive information RMEA collects includes:
 - Your medical history
 - Your racial or ethnic origin
 - Any Indigenous affiliation

Sensitive information that is collected will be treated with the utmost security and confidentiality.

How does RMEA collect personal information?

RMEA will collect information by lawful and fair means. RMEA will include a statement on any of its forms and templates indicating that the information requested is related to RMEA’s primary functions or activities.

At or before the time of collection, RMEA will take reasonable steps to ensure that the individual is aware of:

- The contact details for RMEA and the privacy officer
- How information will be collected and stored
- The purpose for which the information is collected, used or disclosed
- How an individual may access personal information that is being held by RMEA
- How to make a complaint regarding a breach of the Australian privacy principles
- Third parties to whom the information may be disclosed to
- Any law or contractual agreement that requires the information to be collected; and
- The consequences (if any) for the individual if the information is not provided.

Information must be collected directly from an individual. Personal information is not collected for any purposes other than those for which RMEA has obtained the individual’s consent, unless the law requires otherwise, or where other exceptional circumstances prevail as described under the act or under RMEA’s contractual obligations. RMEA complies with the PCI Data Security Standard in protecting cardholder data under its control.

RMEA will determine whether unsolicited personal or sensitive information that it has received is collected for the purposes that solely relate to RMEA’s primary functions or activities. If it is determined

that RMEA has received or collected unsolicited information, RMEA will destroy or de-identify the information in a timely manner.

Use or disclosure of personal information

In the course of its primary functions and activities, RMEA may use or disclose personal information to third parties. Examples of how RMEA may use information collected includes:

- To administer the Griffith Longlook program
- To provide reports to the department of health and other commonwealth agencies as necessary
- To promote and market RMEA programs to prospective applicants

RMEA will only use or disclose information for the purposes for which it is being collected (primary purpose). The information may be used or disclosed for secondary purposes such as information that is related to the primary purpose, or the individual would reasonably expect the use or disclosure of the information for a secondary purpose, or RMEA has the consent of the individual concerned to use or disclose the information. RMEA may also use or disclose information where consent to do so has been given by the individual, as part of the arrangements for training to be undertaken by an outside organisation or individual, as required by law or under other circumstances where permitted under the act.

Third Parties

RMEA will not provide information to third parties except under the following conditions:

- *It is a legislative requirement;* for example, Australian Vocational Education & Training Management Information Statistical Information (AVETMISS) data reporting to the national VET provider;
- *It is a requirement under a contractual obligation;* for example, Griffith University's School Of Medicine Resource Management System (SOMRMS);
- *It is an industrial requirement;* for example, a financial institution may require evidence of consent for direct debit arrangements.
- Consent of the individual concerned is obtained

If personal information is collected from a third party, all reasonable steps will be taken to ensure that the individual is aware:

- That the information is being collected from another source
- How the information will be used
- Any other person or body to whom the information may be shared, or disclosed to

The following list outlines third-party websites and services utilised by RMEA in the collection of personal information:

Website/ service	Personal information collected	Location of 3rd party privacy policy
Jotform	Registration	https://www.jotform.com/help/9-privacy-policy
Paypal	Payment information	https://www.paypal.com/au/webAPPs/mpp/ua/privacy-full
Eway	Payment information	https://www.eway.com.au/legal#privacy
Survey Monkey	EOI surveys, workshop evaluations, other surveys	https://www.surveymonkey.com/mp/policy/privacy-policy/
Mailchimp	Newsletter subscription information, marketing, and advertising	https://mailchimp.com/legal/privacy/
ClickSend	Contact information	https://www.clicksend.com/au/legal/privacy-policy/
Little Hotelier	Accommodation management	https://www.siteminder.com/legal/privacy/

RMEA is not responsible for the content and privacy practices of these third party websites and we encourage you to examine each website's privacy policy and make your own decision regarding their reliability.

It can reasonably be expected that information collected will be disclosed to:

- Griffith University,
- Health services, practices and educational institutions associated with the clinical placement of students, and
- Contractors or agents who provide services to us, for example, medical educators or off-site data storage facilities.

It may be necessary for RMEA to send personal information overseas, for example an overseas clinical placement or training provider. Information will not be sent outside Australia without consent, or unless the transfer complies with APP 8 (cross-border disclosure of personal information), or where RMEA are obliged to do so under contract with the Commonwealth Government.

RMEA will not use or disclose personal information for direct marketing purposes unless it is required for RMEA's core functions and activities. Where possible, information will be de-identified before use.

More specific information about the way in which information is used or disclosed can be obtained upon request by RMEA's privacy officer.

Storage and protection of personal information

RMEA will take all reasonable steps to ensure that the data it collects is accurate, complete, relevant and up-to-date, and has been obtained directly from individuals or other reputable sources. Periodic reviews will be conducted by RMEA and the individuals themselves, to ensure the quality and accuracy of data.

RMEA will take all reasonable steps to ensure that personal information is protected from misuse, interference or loss, or from unauthorised access, modification or disclosure. RMEA uses a range of physical and electronic security measures to ensure that the personal information collected by RMEA is protected and managed confidentially. Information that is collected will be stored as a hard copy in a secure location or stored electronically with password protection. RMEA shall ensure that personal information is stored for only as long as is reasonably necessary. RMEA has an obligation to destroy or de-identify personal information appropriately when no longer required, or in certain circumstances.

Personal information will be stored in both hard-copy and electronic formats. Hard-copies of personal information will be stored securely on-site and off-site and secure storage facilities. Electronic formats of personal information are stored both locally on RMEA servers and on cloud servers. Personal information in electronic format is secured by user access and password protection.

An individual can request to deal with RMEA without identifying themselves or by using a pseudonym, for example, making a complaint. If it is practicable to do so, RMEA will take measures to ensure that information provided on an anonymous or pseudonymous basis is not linked with other information held about the individual.

Unauthorised disclosure of, or access to, personal information by RMEA employees, contractors or agents, will be regarded as a serious breach of this policy. Appropriate action, which may include disciplinary or legal action, will be taken in such cases. RMEA complies with the mandatory data breach legislation of the *Privacy Amendment (Notifiable Data Breaches) Bill 2016* and will notify the OAIC and individuals who may be affected in the event of a data breach.

Access to, and correction of, personal information

An individual may request access to their own personal information that is held by RMEA. If the information is not readily available, the request must be made in writing to the RMEA privacy officer in accordance with the freedom of information act. RMEA will respond within 5 business days after the request is made, and will give access in the manner requested if it is reasonable and practicable to do so.

RMEA may deny access to information in accordance with the exemptions contained in the act (privacy principle 12.3). If access is refused, RMEA will provide a reason for the refusal and take such steps to grant access through the use of a mutually agreed intermediary.

If an individual is able to establish that the information held by RMEA is inaccurate, out of date, incomplete, irrelevant, or misleading, RMEA will take reasonable steps to amend the information. If RMEA refuses an individual's request to amend or update personal information, written notice will be provided setting out the reasons for the refusal, the mechanisms available to complain about the refusal, and any other matter prescribed by regulations.

Complaints procedure

Concerns regarding the management of personal information, and compliance with the Australian privacy principles, by RMEA, should be directed to the privacy officer (contact details below). The RMEA grievance policy has been established to provide details on how an individual may make a complaint.

Under the privacy act, the privacy commissioner has the power to investigate complaints, acts or practices that may be a breach of privacy even if there is no complaint. If an individual makes a complaint about a RMEA practice that is believed to amount to arbitrary or unreasonable interference with an individual's privacy; and the individual does not believe that the matter has been resolved satisfactorily, the individual should either write to the privacy commissioner setting out the details of the practices which are believed to interfere with an individual's privacy, or telephone the privacy hotline 1300 363 992 (local call charge).

Further information on the complaints process is available in the RMEA Complaint Resolution Policy. <https://www.RMEA.org.au/module/documents/download/20>

Privacy Officer (CEO)
Rural Medical Education Australia
Toowoomba QLD 4350
m.oshannessy@RMEA.org.au
Tel: 07 4638 7999

Delegation Authority

Chief Executive Officer (COO) Contact Officer	31/03/2020 Approval Date
Chief Executive Officer (CEO) Megan O'Shannessy Approval Authority	1/06/2023 Date of Next Review

Policy Reviewed and Approved by RMEA CEO

Signed by CEO 

Megan O'Shannessy CEO's Full Name
190 Hume St EAST TOOWOOMBA QLD 4350 CEO's Address
30/06/2022 Date

Modification History

Review Date	Source	Details	Version
20 / 03 / 2013	HR	Review	1
19 / 03 / 2014	HR	Change to Australian privacy principle policy	2
02 / 02 / 2016	Admin	Removed references to GPET, AGPT, PGPPP, ACRRM and the RACGP. Australian privacy principles (no change)	3
16 / 02 / 2018	P Pura J Reid J Dillon	Updated formats of storage, 3 rd party websites, mandatory data breach notification, descriptions and conditions of providing information	4
31 / 03 / 2020	CEO	Reviewed RTO	5
30 / 06 / 2022	HR	Review	6