Sydney University Postgraduate Representative Association (SUPRA) Privacy Procedures

A. Preamble

Name of Procedures

These are the Sydney University Postgraduate Representative Association (SUPRA) Privacy Procedures.

Commencement

These procedures commenced on 29 July 2021.

Procedures are binding

These procedures bind SUPRA, its Council, members, staff, affiliates, and contractors.

Statement of intent

These procedures:

a) support the SUPRA Constitution ('the Constitution') and the SUPRA Privacy Policy and shall not be interpreted so as to contravene either the Constitution or the SUPRA Privacy Policy;

b) detail SUPRA's plan for managing all personal and health information held by SUPRA or by a third party on behalf of SUPRA.

B. Procedures

1. Definitions

1.1 The definitions set out in the Constitution and the SUPRA Privacy Policy shall apply to these procedures.

2. Collection of Information

2.1 Collection of Information

2.1.1 SUPRA collects and holds a wide range of personal and health information relating to students, SUPRA members, staff, and members of the external community. SUPRA cannot function without collecting, holding, and using information with regard to these individuals.

2.1.2 SUPRA collects information from individuals directly, unless they have authorised collection of the information from someone else, it is provided by a parent or guardian for a person under the age of 16, or the individual lacks capacity (including temporarily) to provide that information directly (for instance, if the person is involved in an accident).

2.2 Purposes for Which Information is Collected

2.2.1 Personal and health information may be collected for the performance of SUPRA's key functions, including:

a) the provision of casework, legal, welfare, community and other services, and advocacy;

b) the provision of information, publications, and other resources;

c) development and engagement with various groups including members, students, staff, the University and its various bodies, community groups, other educational institutions, industry and government;

c) improving the experience of students;

d) managing and improving the experience of Council members, SUPRA volunteers, and staff;

e) administrative functions, including receipt, management and payment of funds and safety and security of individuals and property; and

f) meeting reporting obligations to the University.

2.3 Only Relevant Information will be Collected

2.3.1 There is no finite list of personal information and/or health information that SUPRA may collect about individuals. However, only relevant information will be collected.

2.4 Automated Collection

2.4.1 SUPRA also collects information by automated means including:

a) digital and online means (including SUPRA's website or social media services). This includes information gathered to monitor use of, or gather feedback about the quality of, SUPRA services;

b) technology and communications systems that record login and other identifiers of users or their devices;

c) audio, video or images taken at activities and events.

2.4.2 Information collected using automated means is collected from individuals through their participation in an activity or use of a system. Where possible, SUPRA will take reasonable steps to ensure that automatic collections are open and transparent through relevant notices or signage, terms and conditions or other methods of communication.

3. Holding Information

3.1 SUPRA will ensure that it does not hold personal or health information for longer than is required by the general retention and disposal authorities set out under legislation or required by any relevant professional or government body. Where no such authority exists, SUPRA will not hold personal or health information for longer than it needs to use the information.

3.2 SUPRA holds personal and health information in a variety of media, including in hardcopy form, but primarily in data management systems and SUPRA's records management system. Different parts of SUPRA hold different information in different databases or systems.

4. Storage and Maintenance of Information

4.1 Security and Access Generally

4.1.1 SUPRA will ensure that personal information and health information is protected when stored, including to prevent unauthorised use or disclosure, and to dispose of the information securely and in accordance with any other retention and destruction laws.

4.1.2 SUPRA will adopt processes to secure student and employee information, and enable access to the information only in accordance with these procedures.

4.1.3 SUPRA may receive information from third parties, including through third party suppliers or service providers. SUPRA handles that information as it does information collected directly from individuals in accordance with these procedures.

4.1.4 SUPRA sometimes receives personal information that is not actively collected or sought by SUPRA. Although this as unsolicited information, the requirements of these procedures will apply to the storage, use or disclosure of unsolicited information containing personal information.

4.2 Storage of Personal Information outside SUPRA

4.2.1 SUPRA may need to store information or data outside SUPRA or outside the University (including outside New South Wales), for example by using an off-site commercial storage facility to store paper records, or by engaging a third party to host and manage web-based resources, electronic records or data (including by means of cloud storage).

4.2.2 Where SUPRA needs to store information or data pursuant to subclause 4.2.1 of these procedures, the President, or their nominee, together with the Operations Manager, or their nominee, will complete a privacy impact assessment beforehand to ensure the activity meets privacy obligations and community expectations. For IT-related systems, this includes undertaking a security risk assessment.

4.2.3 Third party contracts will incorporate appropriate obligations to ensure compliance with these procedures.

4.3 Employee Records

4.3.1 Electronic personal or confidential information about staff shall only be held in formal SUPRA systems and shall never be held in collaborative areas, such as share drives and Sharepoint, for example.

4.3.2 Records relating to staff grievances, disciplinary matters or other sensitive information shall be held in a separate file to their employee record.

4.3.3 Information about a person's suitability for employment; for example, a selection panel report, a referee's report, a job application or records relating to misconduct, shall be treated as confidential, and restricted access should apply to those records.

5. Information Provided to Individuals

5.1 When collecting personal information, SUPRA will take all reasonable steps to ensure the individual understands how and why their information is being collected, as well as how it will be used, disclosed, and destroyed. Where applicable, individuals will be told of any consequences if they do not provide the information; for example, that a service may be unavailable or be limited.

5.2 Health information is usually collected directly by staff from students accessing the casework and/or legal services. SUPRA staff will take all reasonable steps to ensure that the provisions of subclause 5.1 of these procedures are followed in these situations. Health information relating to staff members is also collected by specific staff on an as-needed basis, such as when processing personal leave applications. This information will be dealt with in accordance with the rules related to the use and disclosure of that information as set out in the HRIPA.

5.3 SUPRA also generates some personal or health information and treats such information as personal or health information (as the case may be) and complies with the rules regarding the use and disclosure of that information in accordance with the relevant principles or legislation.

6. Use of Information

6.1 Limits on Use

6.1.1 SUPRA limits use of personal information and health information as required under the PPIPA to one or more of the

following circumstances:

a) the proposed use is the primary purpose for which it was first collected;

b) the proposed use is directly related to the purpose for which the information was collected;

c) the individual concerned has consented to the use of the personal information;

d) disclosure falls under one of the specific use and disclosure exceptions permitted under the PPIPA as set out in subclause 7.1 of these procedures.

6.2 Consent

6.2.1 SUPRA obtains consent from individuals at the first point of contact the individual makes with SUPRA and then from time to time is necessary.

6.3 Accuracy of Information held by SUPRA

6.3.1 SUPRA must take steps to ensure that the personal information it uses is relevant, up-to-date, accurate, complete and not misleading. SUPRA relies on the individuals providing the personal information to provide information that is accurate and to notify SUPRA of any changes. Individuals are usually informed of their obligations at the time the information is collected.

7. Disclosure of Information

7.1 Limits on Disclosure of Information

7.1.1 SUPRA limits disclosure of personal information as set out under the PPIPA to another person or body in one or more of the following circumstances:

a) the disclosure is directly related to the purpose of collection and SUPRA does not believe the individual concerned would object;

b) the individual concerned is reasonably likely to be aware of the disclosure;

c) disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person. This exception has been determined by the NSW Civil and Administrative Tribunal to

be permitted in very limited circumstances. The threat must be both serious and imminent. Imminent means likely to occur at any moment, or impending. There must also be a belief held on reasonable grounds about the serious and imminent threat by an appropriate Councillor or staff member of SUPRA or an affiliate when this exception is relied on.

7.2 Other Information that can be Accessed by Third Parties

7.2.1 SUPRA makes some information available through its publications including publications that are publicly accessible, for example Annual Reports.

7.2.2 SUPRA also makes information available through its website. Information about, and images of, Councillors, staff and others may be posted or uploaded to the website. SUPRA considers these to be communications in the public domain.

7.3 Use of Social Media

7.3.1 SUPRA uses social media, such as Facebook and WeChat, increasingly as a means of communicating with members.

7.3.2 Information about, and images of, Councillors, staff and others may be posted or uploaded to these social media. SUPRA considers these to be communications in the public domain.

7.4 Transborder data flow of personal information

7.4.1 There are special restrictions regarding the transborder (outside of New South Wales) data flow of personal information under the PPIPA. These align with the requirements of transborder data flow under HRIPA.

7.4.2 SUPRA may provide or receive personal information to or from individuals or organisations outside New South Wales (including outside Australia). SUPRA will only provide this information to these individuals or organisations in one or more of the following circumstances:

a) where an individual expressly consents to the transfer of information;

b) where the transfer is in the interests of the individual and is necessary for the performance of a contract between SUPRA and a third party;

c) where the transfer is otherwise required or permitted by law.

7.4.3 Examples of contracts referred to in subclause 7.4.2b) of these procedures include arrangements with third party providers providing online services, cloud-based technologies, data storage facilities or other digital services (including online and mobile services, such as "live chat").

7.5 Exemptions

7.5.1 SUPRA is not required to comply with the privacy obligations under the PPIPA if:

a) the individual concerned has expressly consented to non-compliance with particular provisions;

b) it is investigating or otherwise handling a grievance or other complaint and compliance might detrimentally affect the proper handling of the matter;

b) the information is disclosed to an individual or agency engaged to investigate or handle a grievance or other complaint;

c) the information is disclosed to an investigative agency, such as the Information and Privacy Commissioner or the Office of the Australian Information Commissioner;

d) it is lawfully authorised or required not to comply with the PPIPA, or non-compliance is permitted under any Act or law.

8. Destruction of Information

8.1 SUPRA will only retain collected personal information as long as is reasonably necessary.

8.2 Destruction of personal information by SUPRA will always be undertaken lawfully and securely.

9. Access to Information

9.1 Access

9.1.1 SUPRA must, when requested to do so, provide an individual with access to their personal information or health information which it holds.

9.1.2 SUPRA must be able to verify the identity of an individual when requests are made to access personal or health information.

SUPRA may refuse access to personal or health information if it is unable to confirm the individual's identity through the appropriate verification process.

9.2 Amendment

9.2.1 SUPRA will amend personal and health information it holds about an individual at the request of the individual to ensure it is accurate and, taking into account the purpose for which that information was collected, is relevant, up to date, accurate, complete and not misleading.

9.2.2 SUPRA must be able to verify the identity of an individual when requests are made to amend personal or health information. SUPRA may refuse to amend personal or health information if it is unable to confirm the individual's identity through the appropriate verification process.

9.2.3 SUPRA may refuse to amend information if the change would conflict with any laws or result in the information being inaccurate, out of date, or misleading.

9.2.4 If SUPRA refuses a request to amend information, the individual will be advised of the decision and reasons why, as well as any right to have that decision reviewed by the President.

9.3 Who to Contact

9.3.1 Any person who has an enquiry as to whether SUPRA holds their personal information or health information, the nature of that information and the purpose for which it was collected should contact:

a) the caseworker or solicitor handling their matter in the case of current clients of the professional services;

b) the coordinator of the casework service through SUPRA administration at admin@supra.usyd.edu.au in the case of former clients of the casework service;

c) the Principal Solicitor of the legal service at solicitor@supra.usyd.edu.au in the case of former clients of the legal service;

d) their coordinator in the case of current staff;

e) the Operations Manager through SUPRA administration at admin@supra.usyd.edu.au in the case of former staff;

f) the SUPRA President at president@supra.usyd.edu.au in the case of all other requests.

9.3.2 Irrespective of the contact people set out in subclause 9.3.1 of these procedures, any person may send their privacy enquiry directly to the SUPRA President at president@supra.usyd.edu.au

10. Complaints in Relation to Privacy

10.1 Complaints Process

10.1.1 Complaints related to privacy matters should be directed to the SUPRA President at president@supra.usyd.edu.au Where the complaint relates to the President, complaints can be made to any other member of the SUPRA executive.

10.1.2 Any person may also complain directly to the NSW Information and Privacy Commissioner.

10.1.3 Where complaints are made to SUPRA, the President, or their nominee, or the member of the executive, or their nominee, will undertake and complete an investigation of the complaint within 60 days. Once completed, SUPRA may decide to do one or more of the following:

a) take no further action;

b) make a formal apology;

c) take appropriate remedial action;

d) give an undertaking that the conduct will not recur; and/or

e) implement measures to prevent recurrence of the conduct.

10.1.4 Within 14 days of completing the investigation, SUPRA will notify the complainant of the outcome of the investigation. The following information will be provided:

a) the findings of the investigation;

b) the reasons for the findings;

c) the action(s) proposed to be taken; and

d) the reasons for the proposed action(s).

11. Privacy Breaches

11.1 Handling Process

11.1.1 A privacy breach occurs when there is unauthorised access to, or collection, use or disclosure, loss or disposal of, personal information held in the custody or control of SUPRA (or a third

party on behalf of SUPRA).

11.1.2 SUPRA will take all reasonable steps to ensure privacy breaches do not occur.

11.1.3 In the unlikely event that a privacy breach does occur, the President, in conjunction with SUPRA staff, will take all reasonable steps to limit the extent and effect of any breach.

11.1.4 Following any breach, the President, in conjunction with SUPRA staff, will investigate the cause of the breach, which may involve a security audit of physical, organisational and technological measures. Existing policies and processes will be reviewed to implement any lessons learned from that investigation to minimise the risk of such a breach occurring in the future.

NOTES

SUPRA Privacy Procedures

Date ratified by Council:	29 July 2021
Date commenced:	29 July 2021
Date last amended:	Not yet amended
Administrator:	Vice President, SUPRA
Review date:	29 July 2023

Amendment History

Dates amended:

1. Not yet amended