Policy Number: PP026

POLICY AND PROCEDURE NAME: Privacy

Preamble / Context

MACE Incorporated (MACE) is committed to protecting the privacy of personal information which the organisation collects, holds, and administers.

Policy Statement

MACE Privacy policy is guided by the *Australian Charities and Not-for-profits Commission Act 2012* (Cth) (ACNC Act) principles:

Principle 1: MACE will manage personal information in an open and transparent way.
Principle 2: MACE will comply with the Australian Privacy Principles in the way it collects, holds, uses, and discloses personal information.

Scope

This policy applies to all employees, volunteers, participants, learners, and contractors within the workplace, or participating in MACE-related activities across various sites.

Purpose

This policy sets out how MACE will comply with the Australian Privacy Principles (APPs) contained in Schedule 1 to the *Privacy Act 1988* (Cth) (the Privacy Act). In particular, this policy demonstrates MACE's compliance with APP 1 - Open and transparent management of personal information.
The APPs are legally binding on MACE and regulate the way in which MACE can collect, store, use and disclose personal information and how you can access and correct that information.

Procedure

MACE adheres to Schedule 1 of the *Privacy and Data Protection Act 2014* (Vic) which contains the Information Privacy Principles (**IPPs**).

The full text of the IPPs is detailed below.

SCHEDULE 1 – THE INFORMATION PRIVACY PRINCIPLES

In these Principles—
sensitive information means information or an opinion about an individual's—
(a) racial or ethnic origin; or

(b) political opinions; or
(c) membership of a political association; or
(d) religious beliefs or affiliations; or
(e) philosophical beliefs; or
(f) membership of a professional or trade association; or
(g) membership of a trade union; or
(h) sexual preferences or practices; or
(i) criminal record—
that is also personal information;

unique identifier means an identifier (usually a number) assigned by an organisation to an individual uniquely to identify that individual for the purposes of the operations of the organisation but does not include an identifier that consists only of the individual's name and does not include an identifier within the meaning of the **Health Records Act 2001**.

1. Principle 1—Collection

1.1. MACE must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2. MACE must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3. At or before the time (or, if that is not practicable, as soon as practicable after) MACE collects personal information about an individual from the individual, MACE must take reasonable steps to ensure that the individual is aware of—
- (a) the identity of MACE and how to contact us; and
- (b) the fact that the individual is able to gain access to the information; and
- (c) the purposes for which the information is collected; and
- (d) to whom (or the types of individuals or organisations to which) MACE usually discloses information of that kind; and
- (e) any law that requires the particular information to be collected; and
- (f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.4. If it is reasonable and practicable to do so, MACE must collect personal information about an individual only from that individual.

1.5. If MACE collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in IPP 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

2. Principle 2—Use and Disclosure

2.1. MACE must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless—
- (a) both of the following apply—
  - (i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;
  - (ii) the individual would reasonably expect MACE to use or disclose the information for

the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

(c) if the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest, other than for publication in a form that identifies any particular individual—

(i) it is impracticable for MACE to seek the individual's consent before the use or disclosure; and

(ii) in the case of disclosure—MACE reasonably believes that the recipient of the information will not disclose the information; or

(d) MACE reasonably believes that the use or disclosure is necessary to lessen or prevent—

(i) a serious threat to an individual's life, health, safety, or welfare; or

(ii) a serious threat to public health, public safety, or public welfare; or

(e) MACE has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or

(f) the use or disclosure is required or authorised by or under law; or

(g) MACE reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of a law enforcement agency—

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or

(h) the Australian Security Intelligence Organisation (ASIO) or the Australian Secret Intelligence Service (ASIS), in connection with its functions, has requested MACE to disclose the personal information and—

(i) the disclosure is made to an officer or employee of ASIO or ASIS (as the case requires) authorised in writing by the Director-General of ASIO or ASIS (as the case requires) to receive the disclosure; and

(ii) an officer or employee of ASIO or ASIS (as the case requires) authorised in writing by the Director-General of ASIO or ASIS (as the case requires) for the purposes of this paragraph has certified that the disclosure would be connected with the performance by ASIO or ASIS (as the case requires) of its functions.

2.2. If MACE uses or discloses personal information under IPP 2.1(g), it must make a written note of the use or disclosure.

3. Principle 3—Data Quality

3.1. MACE must take reasonable steps to make sure that the personal information it collects, uses, or discloses is accurate, complete and up to date.

4. Principle 4—Data Security

4.1. MACE must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification, or disclosure.

4.2. MACE must take reasonable steps to destroy or permanently de-identify personal information

if it is no longer needed for any purpose.

5. Principle 5—Openness

5.1. MACE must set out in a document clearly expressed policies on its management of personal information. MACE must make the document available to anyone who asks for it.

5.2. On request by a person, MACE must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses, and discloses that information.

6. Principle 6—Access and Correction

6.1. If MACE holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that—

(a) providing access would pose a serious threat to the life or health of any individual; or

(b) providing access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access is frivolous or vexatious; or

(d) the information relates to existing legal proceedings between MACE and the individual, and the information would not be accessible by the process of discovery or subpoena in those proceedings; or

(e) providing access would reveal the intentions of MACE in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) providing access would be unlawful; or

(g) denying access is required or authorised by or under law; or

(h) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(i) providing access would be likely to prejudice—

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction; or

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or

(iii) the protection of public revenue; or

(iv) the prevention, detection, investigation or remedying of seriously improper conduct; or

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders—

by or on behalf of a law enforcement agency; or

(j) ASIO, ASIS or a law enforcement agency performing a lawful security function asks MACE not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2. However, where providing access would reveal evaluative information generated within MACE in connection with a commercially sensitive decision-making process, MACE may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

6.3. If MACE is not required to provide the individual with access to the information because of one or more of IPP 6.1(a) to (j) (inclusive), MACE must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4. If MACE charges for providing access to personal information, MACE —

(a) must advise an individual who requests access to personal information that MACE will

provide access on the payment of the prescribed fee; and

(b) may refuse access to the personal information until the fee is paid.

6.5. If MACE holds personal information about an individual and the individual is able to establish that the information is not accurate, complete, and up to date, MACE must take reasonable steps to correct the information so that it is accurate, complete, and up to date.

6.6. If the individual and MACE disagree about whether the information is accurate, complete, and up to date, and the individual asks MACE to associate with the information a statement claiming that the information is not accurate, complete, or up to date, MACE must take reasonable steps to do so.

6.7. MACE must provide reasons for denial of access or a refusal to correct personal information.

6.8. If an individual requests access to, or the correction of, personal information held by MACE, they must—

(a) provide access, or reasons for the denial of access; or

(b) correct the personal information, or provide reasons for the refusal to correct the personal information; or

(c) provide reasons for the delay in responding to the request for access to or for the correction of personal information—

as soon as practicable, but no later than 45 days after receiving the request.

7. Principle 7—Unique Identifiers

7.1. MACE must not assign unique identifiers to individuals unless the assignment of unique identifiers is necessary to enable MACE to carry out any of its functions efficiently.

7.2. MACE must not adopt as its own unique identifier of an individual a unique identifier of the individual that has been assigned by another organisation unless—

(a) it is necessary to enable MACE to carry out any of its functions efficiently; or

(b) it has obtained the consent of the individual to the use of the unique identifier; or

(c) it is an outsourcing organisation adopting the unique identifier created by a contracted service provider in the performance of its obligations to MACE under a State contract.

7.3. MACE must not use or disclose a unique identifier assigned to an individual by another organisation unless—

(a) the use or disclosure is necessary for MACE to fulfil its obligations to the other organisation; or

(b) one or more of IPP 2.1(d) to (g) applies to the use or disclosure; or

(c) it has obtained the consent of the individual to the use or disclosure.

7.4. MACE must not require an individual to provide a unique identifier to obtain a service unless the provision of the unique identifier is required or authorised by law or the provision is in connection with the purpose (or a directly related purpose) for which the unique identifier was assigned.

8. Principle 8—Anonymity

8.1. Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with MACE.

9. Principle 9—Transborder Data Flows

9.1. MACE may transfer personal information about an individual to someone (other than MACE or

the individual) who is outside Victoria only if—

(a) MACE reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Information Privacy Principles; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and MACE, or for the implementation of precontractual measures taken in response to the individual's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between MACE and a third party; or

(e) all of the following apply—

(i) the transfer is for the benefit of the individual;

(ii) is impracticable to obtain the consent of the individual to that transfer;

(iii) if it were practicable to obtain that consent, the individual would be likely to give it; or

(f) MACE has taken reasonable steps to ensure that the information which it has transferred will not be held, used, or disclosed by the recipient of the information inconsistently with the Information Privacy Principles.

10. Principle 10—Sensitive Information

10.1. MACE must not collect sensitive information about an individual unless—

(a) the individual has consented; or

(b) the collection is required or authorised under law; or

(c) the collection is necessary to prevent or lessen a serious threat to the life or health of any individual, where the individual whom the information concerns—

(i) is physically or legally incapable of giving consent to the collection; or

(ii) physically cannot communicate consent to the collection; or

(d) the collection is necessary for the establishment, exercise, or defence of a legal or equitable claim.

10.2. Despite IPP 10.1, MACE may collect sensitive information about an individual if—

(a) the collection—

(i) is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or

(ii) is of information relating to an individual's racial or ethnic origin and is collected for the purpose of providing government funded targeted welfare or educational services; and

(b) there is no reasonably practicable alternative to collecting the information for that purpose; and

(c) it is impracticable for MACE to seek the individual's consent to the collection.

Authorisation

Chief Executive Officer
MACE Incorporated

Responsibility

The CEO is responsible for the control and issuance of this Privacy policy and procedures.

Definitions

As identified in the chart below.

Item	Definition
Personal Information	In this policy a reference to 'information' is a reference to both health information and personal information which directly or indirectly identifies a person.
Sensitive information	Typically refers to information or an opinion about an individual that is health related or of a socio-economic nature, and may include racial or ethnic origin, or political opinions, or membership of a political association, or religious beliefs or affiliations, or philosophical beliefs, or membership of a professional or trade association, or membership of a trade union, or sexual preferences or practices, or criminal record. Refer to Principle 1 and Principle 10 for further information on how to collect sensitive information.
Primary purpose	Is one for which the individual concerned would expect their information to be used. Using the information for this purpose would be within their reasonable expectations.
Privacy principles	As defined in *the Privacy and Data Protection Act 2014* (Federal), including the 13 Australian Privacy Principles (APP) as outlined in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (C'Wlth),* and the ten Information Privacy Principles specified in Schedule 1of the *Information Privacy Act 2000 (Vic).*
Sensitive information	Typically refers to information that is health related or of a socio-economic nature e.g. 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, criminal record.
Unique Identifiers	Refers to an identifier (usually a number) assigned by an organisation to an individual uniquely to identify that individual for the purposes of the operations of the organisation but does not include an identifier that consists only of the individual's name and does not include an identifier within the meaning if the Health Records Act 2001. Refer to Principle 7 for further information on the application of unique identifiers.

Related Documents

- Privacy Statement
- Complaints and Appeals Policy PP029
- Complaints and Appeals Form MA010

- Suspension, Expulsion and Withdrawal Policy PP067
- Record Management Policy PP016
- Data Collection, Analysis and Action Policy PP015

Relevant Legislation

- Privacy Act 1988
- Privacy and Data Protection Act 2014 (Federal)
- The Australian Privacy Principles (APP), 2014 (C'Wlth.)
- Information Privacy Act 2000 (Vic.)
- Health Records Act 2001 (Vic.)

Process – Data breach response

MACE's data breach response plan comprises four steps (consistent with the Privacy Act 1988, as follows:

1. Step One – **Contain** the data breach to prevent any further compromise of personal information.

2. Step Two – **Assess** the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.

3. Step Three – **Notify** individuals and the Commissioner if required. If the breach is an 'eligible data breach' it may be mandatory for MACE to notify.

4. Step Four – **Review** the incident and consider what actions can be taken to prevent future breaches.

Refer to Complaints and Appeals Policy PP029 – Process section, for guidelines on how complaints of privacy breaches will be addressed by MACE.