AICOOP: Privacy Policy

---

1. **Scope:**

This co-operative policy applies to all members, member and non-member directors and officers (and stakeholders including employees) of the co-operative.

2. **Definitions:**

the co-operative is the Auto Industry Co-op Ltd
the law is the Co-operative National Law (and associated Regulations) as enacted in each Australian jurisdiction (except in Queensland where the Co-operatives Act of 1997 and associated Regulation apply)
officer of a co-operative means a director or secretary of the co-operative or a person who makes, or participates in making, decisions that affect the whole co-operative (including financial) and may include an employee of the co-operative or administrator, liquidator or trustee
a ***platform co-operative*** is a digital platform — a website or mobile app that is designed to provide a service or sell a product — that is collectively owned and governed by the people who depend on and participate in it
a ***stakeholder*** is an individual and/or group who is impacted by the operations of the co-operative (including staff of the co-operative), or have an interest in the operations of the co-operative, or can influence co-operative operations.

3. **Preamble**:

As part of their active membership in the co-operative members participate in the formation, organisation, funding and operation of new sustainable co-operative enterprises by providing and receiving mutual support within an online peer-to-peer community.

So as to establish and maintain this community as a platform co-operative, members provide information about themselves as part of their legal relationship with the co-operative as well as in relation to their participation in the activities of the co-operative undertaken with other members for mutual benefit. Furthermore, the co-operative is required by the law to collect and use information held in registers kept by the co-operative under the law.

Within this environment it has been found necessary to to protect member privacy through the provision of a legally compliant policy framework, as set out in this document.

4. **Co-operative Values and Principles:**

The co-operative supports co-operative identity, ethical values and principles of the international co-operative movement including *voluntary and open membership* (first co-operative principle) that requires members to accept the responsibilities of membership, *democratic member control* (second principle) that requires members to actively participate, *member economic participation* (third principle) that requires the co-operative to gather information about financial contribution and provision of information between member and co-operative (education, training and information - *principle* 5). All member information should be used in a way that is consistent with these and other co-operative principles and co-operative values, including the ethical values of honesty and openness.

5. **Position:**

The co-operative believes that members should be able to freely exchange information between each other and with the co-operative whilst ensuring that private information is only used when necessary to carry out the activity of the co-operative in compliance with the law and the Privacy Act 1988 (Commonwealth of Australia).

6. **Policy**

6.1 Co-operative commitments

The co-operative will collect only information which the organisation requires for its purposes and will use and disclose personal information only for its primary activities or a directly related purpose, or for another purpose with member (or stakeholder) consent. Furthermore, the storage of personal information will be maintained securely to protect it from unauthorised access; and, the co-operative will ensure that members (and stakeholders) are informed as to why the co-operative collects personal information and how it administers the information gathered.

6.2 Information gathering

Information will only be gathered or used:

- to fulfill obligations under any contract between a member or other individual with the co-operative;
- in relation to its legal requirements under the law (including the keeping member registers) and providing notice to members;
- in relation to rendering services related to the business of the co-operative such as warranty or after sales service); and,
- to provide information that may be of interest about upgrades, products, special offers and other miscellaneous matters that may be of interest and the dissemination of information such as newsletters).

6.3 Privacy and co-operative member registers

The law requires the use of registers to collect member information including in relation to: relevant to the holding of the directorship, membership, shares, co-operative capital units, loans, securities, debentures or deposits concerned or the exercise of the rights attaching to them. The co-operative must not use or disclose this personal information about an individual for a purpose other than the primary purpose of the co-operative unless the use or disclosure is required or authorised by or under law.

6.4 Co-operative website and use of tracking technologies and links to other websites

The co-operative provides links to websites outside of the Auto Industry Co-op Ltd site. These linked sites are not under the control of the co-operative, and it is not responsible for the conduct of companies linked, nor for the performance or otherwise of any content and/or software contained in such external websites. The co-operative also uses tracking technologies such as cookies and web beacons to make use of the co-operative website and related services as convenient as possible.

6.6 General Data Protection Regulation

In accordance with GDPR enforcement commencing 25th May 2018 all users should be aware of the following before accepting any terms and conditions related to Membership of Auto Industry Co-op Ltd or use of the technology, tools and website that form aiCOOP

Auto Industry Co-op Ltd Co-op Reg (NSWC32915) collects your personal information to the extent we require to allow membership, allocation of membership shares, participation in the technology, tools and website that form aiCOOP

Your data is not sold, licensed, leased or transferred to 3rd parties. Some of your data specifically related to Membership and Member Shares is reported to the regulator (ASIC and or Consumer Affairs Victoria, Australia) in accordance with our legal obligations

Your data is collected for the intention of providing better services and convenience for you. However, you can withdraw consent for use of your data at any time except data we are legally required by law to hold for the purposes of owning shares.

Your data is stored securely however should you have any concerns please contact privacy@aicoop.com.au and to request retrieval of your data.

Should we experience a data breach you will be notified according to our data breach policy within 24 hours of our knowledge.

Data Breach Procedure

This Procedure sets out the processes to be followed by aiCOOP staff in the event that aiCOOP experiences a data breach or suspects that a data breach has occurred. A data breach involves the loss of, unauthorised access to, or unauthorised disclosure of, personal information.

---

1. Policy
This Procedure is governed by the Co-operative Incubator Privacy Policy.
2. Introduction
The Privacy Amendment (Notifiable Data Breaches) Act 2017 (NDB Act) established a Notifiable Data Breaches (NDB) scheme requiring organisations covered by the Act to notify any individuals likely to be at risk of serious harm by a data breach. The Office of the Australian Information Commissioner (OAIC) must also be notified. Accordingly, AiCOOP needs to be prepared to act quickly in the event of a data breach (or suspected breach), and determine whether it is likely to result in serious harm and whether it constitutes an NDB.
Adherence to this Procedure and Response Plan will ensure that we can contain, assess and respond to data breaches expeditiously and mitigate potential harm to the person(s) affected.
This Procedure and Response Plan has been informed by:

- The Office of the Australian Information Commissioner's "Guide to developing a data breach response plan"
- The Office of the Australian Information Commissioner's "Data breach notification guide: a guide to handling personal information security breaches"
- NDB Act
- The Act and Australian Privacy Principles (Schedule 1 of the Act)

This document should be read in conjunction with our Privacy Policy.
3. Process where a breach occurs or is suspected
3.1 Alert
Where a privacy data breach is known to have occurred (or is suspected) any member of staff who becomes aware of this must, within 24 hours, alert a Board Member or the Chief Executive Officer in the first instance.
The Information that should be provided (if known) at this point includes:

a. When the breach occurred (time and date)
b. Description of the breach (type of personal information involved)

c. Cause of the breach (if known) otherwise how it was discovered

d. Which system(s) if any are affected?

e. Which technology is involved?

f. Whether corrective action has occurred to remedy or ameliorate the breach (or suspected breach)

3.2 Assess and determine the potential impact

Once notified of the information above, the Chief Executive Officer must consider whether a privacy data breach has (or is likely to have) occurred and make a preliminary judgement as to its severity. The Co-operative Secretary should be contacted for advice.

3.2.1 Criteria for determining whether a privacy data breach has occurred

a. Is personal information involved?

b. Is the personal information of a sensitive nature?

c. Has there been unauthorised access to personal information, or unauthorised disclosure of personal information, or loss of personal information in circumstances where access to the information is likely to occur?

For the purposes of this assessment the following terms are defined in section 9 of the Privacy Policy: personal information, sensitive information, unauthorised access, unauthorised disclosure and loss.

3.2.2 Criteria for determining severity

a. The type and extent of personal information involved

b. Whether multiple individuals have been affected

c. Whether the information is protected by any security measures (password protection or encryption)

d. The person or kinds of people who now have access

e. Whether there is (or could there be) a real risk of serious harm to the affected individuals

f. Whether there could be media or stakeholder attention as a result of the breach or suspect breach

With respect to 3.2.2(e) above, serious harm could include physical, physiological, emotional, economic/financial or harm to reputation and is defined in section 9 of the Privacy Policy and section 26WG of the NDB Act.

Having considered the matters in 3.2.1 and 3.2.2, the Chief Executive Office must notify the Board within 24 hours of being alerted under 3.1.

3.3 Chief Executive Officer to issue pre-emptive instructions

On receipt of the communication by the relevant member the Chief Executive Officer will take a preliminary view as to whether the breach (or suspected breach) may constitute an NDB. Accordingly, the Chief Executive Officer will issue pre-emptive instructions as to whether the data breach should be managed at the local level or escalated. This will depend on the nature and severity of the breach.

3.3.1 Data breach managed at the local level

Where the Chief Executive Officer instructs that the data breach is to be managed at the local level, the relevant staff must:

- ensure that immediate corrective action is taken, if this has not already occurred (corrective action may include: retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system); and
- submit a report via the Chief Executive Officer within 48 hours of receiving instructions under 3.3. The report must contain the following:
    - Description of breach or suspected breach
    - Action taken
    - Outcome of action
    - Processes that have been implemented to prevent a repeat of the situation.
    - Recommendation that no further action is necessary

The Cooperative Secretary will be provided with a copy of the report and will sign-off that no further action is required.

The report will be logged by the Cooperative Secretary.

3.3.2 Data breach managed by a Response Team

There is no single method of responding to a data breach and each incident must be dealt with on a case by case basis by assessing the circumstances and associated risks to inform the appropriate course of action.

The following steps may be undertaken by the Response Team (as appropriate):

- Immediately contain the breach (if this has not already occurred). Corrective action may include: retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system.

- evaluate the risks associated with the breach, including collecting and documenting all available evidence of the breach having regard for the information outlined in sections 3.2.1 and 3.2.2 above.
- Call upon the expertise of, or consult with, relevant staff in the particular circumstances.
- Engage an independent cyber security or forensic expert as appropriate.
- Assess whether serious harm is likely (with reference to section 3.2.2 above and section 26WG of the NDBAct).
- Make a recommendation to the Chief Executive Officer whether this breach constitutes an NDB for the purpose of mandatory reporting to the OAIC and the practicality of notifying affected individuals.
- Consider developing a communication or media strategy including the timing, content and method of any announcements to students, staff or the media.

The Response Team must undertake its assessment within 48 hours of being convened.
The Chief Executive Officer will provide periodic updates to the Cooperative Secretary as deemed appropriate.

3.5 Notification

Having regard to the Response team's recommendation in 3.4 above, the Chief Executive Officer will determine whether there are reasonable grounds to suspect that an NDB has occurred.
If there are reasonable grounds, the Chief Executive Officer must prepare a prescribed statement and provide a copy to the OAIC as soon as practicable (and no later than 30 days after becoming aware of the breach or suspected breach).
A template can be found at OAIC.
If practicable, we must also notify each individual to whom the relevant personal information relates. Where impracticable, aiCOOP must take reasonable steps to publicise the statement (including publishing on the website).
The prescribed statement will be logged by the Cooperative Secretary.

3.6 Secondary Role of the Response Team

Once the matters referred to in 3.4 and 3.5 have been dealt with, the Response team should turn attention to the following:

- Identify lessons learnt and remedial action that can be taken to reduce the likelihood of recurrence – this may involve a review of policies, processes, refresher training.
- Prepare a report for submission to the Board.
- Consider the option of an audit to ensure necessary outcomes are effected and effective.

4. Updates to this Procedure

In line with the Good Governance Policy, this procedure is scheduled for review every five years or more frequently if appropriate.

5. Contact details

Contact for all matters related to privacy, including complaints about breaches of privacy, should be directed as follows: privacy@aicoop.com.au

7. Action:

Procedures that explain the steps to be followed in the performance of tasks and/or in the implementation of this policy shall be developed by the Managing Director in consultation with the Secretary and will be appended to this policy.

8. Responsibility:

On a day-to-day basis the Managing Director is responsible for the implementation of this policy. The Secretary is ultimately responsible for the security and integrity of co-operative registers. The Secretary, and Co-operative Responsibility Committee, are responsible for monitoring compliance.

9. Related documents:

- Co-operatives National Law Application Act 2013
- Privacy Act 1988 of the Commonwealth
- The Rules of the co-operative
- Electronic Communications Policy of the co-operative
- The Platform User Agreement of the co-operative.