Code of Conduct

Confidentiality, Privacy and Data Use Policy

May 2023

Australian Carbon Industry **Code of Conduct**

Purpose

The purpose of this policy is to provide an overview of confidentiality under the Code; the processes adopted by the Code Administrator (Administrator) to maintain security and confidentiality of data; and describe relevant roles and responsibilities.

The Australian Carbon Industry Code of Conduct ('the Code') is administered by the Administrator, which is hosted by the Carbon Market Institute ('CMI'). The personnel who work on the Code of Conduct are employed by CMI. Unless specifically stated, these personnel are hereafter referred to as 'the Administrator'.

Implementation, Review and Responsibility

This Policy will be implemented from 1 May 2023 and is to be endorsed by all Code personnel and the Code Panel. The Code Panel is an independent review panel that, amongst other things, oversights, reviews and guides the activities of the Administrator. The Policy must be:

- kept in shared folders accessible to all Code Administrator personnel; and
- reviewed internally and updated as required by the relevant personnel on a regular basis.

This Policy will also be independently reviewed as part of the Code Administrator's three-yearly independent review process. The roles and responsibilities of relevant Code personnel and stakeholders in relation to this Policy are detailed below.

Functional Role	Organisational Role	Responsibility Level
Code Independent Panel (Code Panel)	Oversight over Code of Conduct	Review/Update
CEO CMI	Carbon Market Institute (CMI) host of Code Administrator	Review
Code Administrator	Implementor of Code of Conduct	Implementation/Review/Update

Scope

The Privacy Act 1988 (Cth) applies to CMI and therefore this Policy has been drafted to comply with this legislation, including adopting its principles and standards, where there is any inconsistency the legislation prevails. This Policy applies to all information assets held by the Administrator. It covers external sharing and internal management of confidential and sensitive information. The definitions below outline the relevant practices included in the scope of this policy:

External Information Sharing
Information that is shared with: any other individual, organisation or representative outside the Code Administration team. Any information shared with other CMI personnel will be considered 'external'.

Confidential and Sensitive Information
Information that is:

- Created by, intended solely for, or of sole possession of the Code Administrator (exclusive of CMI as an organisation);
- Created by, intended for, or of possession of the Code Administrator and CMI jointly; and
- Nondisclosure Agreement protected information.

Principles

This policy is aligned with key principles of the Code of Conduct:

- Promoting industry best practice;
- Promoting consumer protection;
- Providing guidance to stakeholders;
- Encouraging and ensuring market integrity, accountability, trust and transparency; and
- Promoting compliance.

Outcomes

This policy is intended to ensure:

- Transparent and clear collection of data exclusively for the purpose of ensuring management and of compliance of signatories under the Code.
- Information assets held in the Code's database are secure and appropriately managed;
- Potential risks to information security and confidentiality are identified, avoided and managed;
- Appropriate use of data for the purposes of Code compliance and implementation, ensuring that private, financial and commercially sensitive information is appropriately protected;
- Signatories, landholders and stakeholders under the Code have confidence and sufficient trust in the Administrator's management of information held by the Administrator;
- Compliance with obligations imposed by the *Privacy Act 1988 (Cth)*, including the Australian Privacy Principles

Procedure

The Code Administrator's procedure for managing information is detailed below

Procedure for Information Management	
Information held securely and only used for Code purpose	**How: all** information assets held by the Administrator are managed through a CRM software (Salesforce) and are only used for the purposes of Code compliance and implementation. The CRM is separate from the CMI database and access is strictly controlled by the Code Administrator. **When:** all the time **Who:** all Code Administrator staff and Code Panel Members are responsible for doing this.
Identify sensitive and confidential information	How: information that is sensitive or confidential (as defined above) must only be identified and shared to recipients approved by the Code Administrator for the limited purpose of administering the Code in the following ways: • For verbal communication: stating to the approved information recipient/s that the information is confidential or sensitive; • For email communication: labelling the email to the approved information recipient as confidential or sensitive at the beginning of the email; and • For documents: labelling the email as confidential or sensitive at the beginning of the document The Code Administrator will clearly state in these communications the purposes for which the information may be used to the approved recipient and that the recipient must not disclose the sensitive or confidential information to any third party.. When: at the time of the information being shared Who: all Code staff and Code Panel Members are responsible for doing this
Control information	How: restrictions on information access; restrictions on information sharing; privacy controls; implementation of nondisclosure deeds for key staff with access to confidential and sensitive information; and identification of non-compliance (see detail below).Note: there are very few personnel who currently have access to sensitive and confidential information stored on the Code database and they work closely together. When: at all times, ongoing Who: Code Administrator personnel, Code Panel members and CEO of CMI
Report breaches	How: When any person or organisation has reasonable grounds to believe there has been a breach of this policy, they must promptly notify the Code Administrator. The Code Administrator will take the following steps: 1. Contain any confidentiality breach to prevent any further compromise of sensitive or confidential information. 2. Assess the 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. Check whether the person who disclosed the information had consent to do so or had a lawful reason for the disclosure, such as risk to public safety. 4. Notify any person affected by the disclosure and escalating the disclosure to the Code Panel if required. 5. Review the incident and consider what actions can be taken to prevent future breaches.

	As relevant, breaches will be reported internally by formally communicating to the Code Administrator; and/or externally via email communication to the relevant stakeholder(s). See below for more detail on this. Where the Code Administrator believes there has been a breach of this policy, it will record the breach on the Information Confidentiality Breaches Register (see **Appendix 1**). When: as soon as possible after the breach of security or confidentiality occurs Who: all Code Administrator staff, Code Panel Members and CEO of CMI are responsible for doing this
Manage breaches	**How:** instances of non-compliance will be managed by: identifying where the controls failed; updating policies and procedures as relevant; and initiating internal or external disciplinary action where warranted **When:** the appropriate steps will be taken within 10 business days of the breach being reported **Who:** all Code staff, and Code Panel Members are responsible for doing this, however the Director Code has final oversight and responsibility for management of confidentiality breaches.

Detail on Controls

Restrictions on information access and sharing:

- Code of Conduct information (documentation, emails etc.) that is confidential or sensitive will be limited to being accessible by only Code personnel. In instances where the Administrator requires CMI support for a particular task and must share a Code document containing sensitive/confidential information, the Code personnel must with the approval of the Director Code either remove/redact the sensitive/confidential information from the document before sharing; or share the document in its unredacted form only if the relevant CMI personnel has executed a nondisclosure deed. The CMI staff member must be notified that the document/information is not to be disclosed to any third party or otherwise circulated. Information may be de-identified or disaggregated and communicated by the Administrator to CMI with the approval of the Director Code. For clarity, the sharing of the information must not compromise, undermine or negatively impact the 'owner' of the sensitive/confidential information, the CMI, the Code, any Signatory/Partner/Supporter or CMI Member.
- For confidential information that is submitted to the Administrator by Signatories (e.g. annual reports) the filing and naming of documents will be checked in accordance with the Code's document classification protocol by the Code personnel – to ensure that if a Signatory requests a copy of their documentation, the correct information is shared.
- Verbal communication of sensitive or confidential information should not be done in places where it can be overheard by persons other than Code Administration team. This also applies to de-identified and disaggregated information.
- Physical copy documents with sensitive or confidential information will not be accessed by persons other than Code Administration team and this will be implemented by ensuring the information is stored in a secured/locked filing cabinet system with access restricted to only Code Administrator personnel.
- Personnel whose duties support both the Code Administrator and the Carbon Market Institute, should ensure that distinct separation of duties are clearly defined in role descriptions, and that security and

confidentiality of information is managed with the support of relevant line managers across both operations. Relevant personnel must execute nondisclosure deeds where necessary and should ensure that sensitive or confidential information is not shared with, or used in the provision of other CMI duties, or in any other way that would represent a conflict of interest as per the *Conflicts of Interest Policy*. These deeds are legally binding documents that clearly state the person's obligation to treat all confidential or sensitive information in accordance with the deed.

Privacy (information security) controls:

- The Administrator will maintain separate software accounts with strictly controlled access (access approval can only be granted by the Director Code) of the following: Email; Salesforce; FormAssembly: Sharepoint (shared drive); Microsoft Teams, and other third party project management tools (including but not limited to Asana and Wordpress).

Record Keeping

- Code data and information assets are stored on the Code's CRM software Salesforce which has been built securely to protect Code data and applications, including password protected log-ins. This database incorporates appropriate user permissions to control access to it and contains field and record-level security (only staff of the Administrator have access, not CMI staff generally). This database securely stores confidential and sensitive information and only the Code Administrator can view, create, edit or delete any record or field in the Code database.
- Appropriate records of any breaches of confidentiality and outcomes will be maintained by the Administrator for a minimum of seven years. Records must be kept in a manner that are easily accessible for audit or other purposes. This is also relevant to the Administrator's Complaints Handling Procedure, which will be updated as relevant to reflect this policy.
- All commercial-in-confidence information will be treated with appropriate confidentiality and subject to the requirements of relevant laws, in particular the Privacy Act 1988.

Appendices

Appendix 1: Example Information Confidentiality Breaches Register

Note the format of this register is indicative only and will be adjusted as needed.

Information Confidentiality Breaches Register	
Date	2/1/21
Date of breach	1/1/21
Personnel involved	Joe Public (Code Officer)
Description of breach of information confidentiality	Joe verbally disclosed potentially sensitive information about a Signatory to a CMI staff member that is not part of the Code Administration.
Persons notified	Director Code, and the Signatory organisation in question
Public communication of the breach (if relevant)	No – it is not appropriate in this instance.
Steps to rectify the breach	Director Code to identify where the controls failed; update policy and procedure accordingly; and give formal warning to the Code Officer, within 10 business days of 2/1/21
Status of breach	Active. Oversight will continue ongoing as necessary

for more information please contact

Code Administrator

code.administrator@carbonmarketinstitute.org

Australian
Carbon Industry
Code of Conduct