1. Purpose

The Chamber of Minerals and Energy of Western Australia (CME) accept and acknowledge the importance of confidentiality. The CME is committed to maintaining the security of all personal information including employees, members, stakeholders, and visitors.

The *Privacy Act 1988* and Australian Privacy Principles (APPs) govern the way in which CME collects, uses, discloses, stores, secures and disposes of personal information.

2. Policy Application

This Policy applies to all employees (includes consultants and casual staff) of CME.

3. Personal Information

Personal information under the *Privacy Act 1988* is defined as information or an opinion that identifies an individual.

3.1 Collection of Employee Personal Information

Examples of personal information CME may collect from its employees includes but is not limited to:

- Personal details such as name, gender, postal and residential address, telephone number or email address; and
- Employment details such as salary, bank account, superannuation, and tax file number.

Sensitive information such as criminal and medical records will be requested as part of the CME pre-employment due diligence process and Occupational Safety, Health and Wellbeing requirements. Such information is only accessible to Human Resources personnel and senior executives.

3.2 Collection of Member and Stakeholder Personal Information

CME will only collect personal information from its members and stakeholders that is necessary for its business functions and activities.

The types of personal information CME collects from members and stakeholders may include their name, company/organisation, position, business address, business telephone number, email address, mobile telephone number and the details of an individual's membership of CME councils, committees, forums, roundtables and working or other groups.

CME will only collect personal information by lawful and fair means and subject to the requirements of the Australian Privacy Principals.

CME collects personal information via various ways including:

- Directly from an individual, such as via phone, email, registration forms, file sharing services or any other agreements, or when personal details are submitted through the CME website, a shared CME SharePoint site or the CME Survey Portal;
- From third parties such as member companies or authorised representatives;
- From publicly available sources of information; and
- When legally required to do so.

This document is protected by copyright. No part of this document may be reproduced, adapted, transmitted, or stored in any form by any process (electronic or otherwise) without the specific written consent of the Chief Executive. All rights are reserved.

4. Storing of Personal Information

CME outsources its IT management and services to a contracted IT services provider who have established policies and procedures to ensure data is stored in a manner which minimises the risk of data loss and the risk of a notifiable data breach. Refer to the *OSIT Data Storage Policy* and *OSIT Notifiable Data Breaches Policy.*

CME also outsources its payroll services to a contracted Payroll services provider who have established confidentiality policies and procedures to ensure CME employee information is stored securely and in line with the *Privacy Act 1988*.

All personal information is hosted in Microsoft 365 cloud storage platforms and all 365 user accounts accessing data are protected with 2 Factor Authentication. The security of personal information is highly important to CME and CME takes reasonable steps to protect it from misuse, loss, unauthorised access, modification, or disclosure. This includes:

- Requiring our staff to maintain privacy and confidentiality as specified in the *Code of Conduct (HR01);*
- Document storage security measures; and
- Imposing computer access security measures, including password protection

The internal systems used by CRM for member and stakeholder communication and activities have strict security and restricted access permission measures applied. Personal information stored on these systems is for internal CME use only.

CME will destroy or permanently de-identify personal information when it is no longer required for use or disclosure, and where CME is not required to retain the information in accordance with an Australian law.

Individuals can also opt out of any marketing communications from CME at any time by following the unsubscribe instructions on such communications.

5. Purposes of Collecting, Storing and Using Personal Information

CME maintains personal information on members and other stakeholders, to:

- Provide information relating to CME's activities, events, and projects; and
- Provide information that may assist the business operations of the company/organisation to which individuals belong.

CME will only use personal information for the purposes of which it was collected. Personal information may be used for secondary purposes closely related to the primary purpose, in circumstances which would be reasonably expected. Where appropriate and where possible, CME will provide notification of the purposes of collection at or before the time the information is collected or as soon as practicable after collection.

In the event CME is required to disclose personal identifiable information of its members to an independent consultant engaged under contract to CME to provide data collation, cleansing, modelling and analysis, it will only do so with prior notification. Personal information from member companies will only be disclosed to the broader public in an anonymised and aggregated format, abiding by the Australian Privacy Principles. No

This document is protected by copyright. No part of this document may be reproduced, adapted, transmitted, or stored in any form by any process (electronic or otherwise) without the specific written consent of the Chief Executive. All rights are reserved.

identifiable commercially sensitive information is disclosed, which could reasonably lead to member companies breaching their continuous disclosure obligations under the *Corporations Act 2001 (Cth).*

Aggregated and anonymised information may be used in (including but not limited to) CME publications, presentations, public website materials, social media networks, television exclusives, radio news, newspapers, opinion editorials and other traditional print media. It may also be used in correspondence with the government, Members of Parliament, politicians, and other key stakeholders. It is only used for purposes directly related to CME policy and advocacy or for related purposes where it is reasonably expected CME will use the information for, which are listed in the CME Constitution & Operating Procedures located on the CME website.

Images of individuals used in CME marketing material will only be used with prior consent. Individual identifiable quotes and statements listed in member publications, public websites or on member professional and social networking channels, may also be used in CME marketing material i.e., publications, websites and across professional networking and social media channels, such as Facebook, Twitter, Instagram, YouTube and LinkedIn.

6. Accessing and Updating Personal Information

All individuals are entitled to access their personal information held by CME or to seek to have it corrected or updated. CME will action requests for access to personal information within 30 days or as soon as reasonably practical after the request is made.

7. Reporting Data Breaches

Where an individual has a complaint about how CME collects, holds, uses, or discloses personal information, or any breach or perceived breach of the *Privacy Act 1988* and associated Privacy Principles, the complaint process outlined in the CME *Complaint and Grievance Policy (HR11)* should be followed.

CME will endeavour to investigate and resolve all complaints however if the individual is not satisfied with the outcome, they are entitled under law to pursue the complaint further with the Office of the Australian Information Commissioner (AIOC) https://www.oaic.gov.au/privacy/privacy-complaints/.

8. Obligations

All CME employees are required to adhere to this Policy.

Where there is a question about how this Policy or CME's *Code of Conduct (HR01)* should be applied, advice should be sought from CME Management or HR.

9. Breaches of this Policy

Violation of the law or this Policy may result in disciplinary action up to and including termination of employment as outlined in CME's *Unsatisfactory Performance and Discipline Policy (HR13).*

Disciplinary action may also be taken against any employee who directly approves of or has knowledge of violations of the law or this Policy.

This document is protected by copyright. No part of this document may be reproduced, adapted, transmitted, or stored in any form by any process (electronic or otherwise) without the specific written consent of the Chief Executive. All rights are reserved.

10. Policy Deviation

Requests to deviate from this Policy must be discussed with the Chief Executive who will assess the impact of the deviation across CME. Deviations from this Policy may only be approved where there is a supporting business case or justification for the deviation.

11. Policy Review

This Policy shall be reviewed by CME at least every two (2) years or as necessary to ensure compliance with legislative requirements.

12. Related Documentation

HR01	Code of Conduct
HR06	Electronic Communications and Computer Use Policy
HR11	Complaint and Grievance Policy
HR13	Unsatisfactory Performance and Discipline Policy
	Office Solutions IT Data Storage Policy
	Office Solutions IT Notifiable Data Breach Policy

This document is protected by copyright. No part of this document may be reproduced, adapted, transmitted, or stored in any form by any process (electronic or otherwise) without the specific written consent of the Chief Executive. All rights are reserved.

Appendix A: Summary of the information CME collect and what it is used for.

Data / Information Type	What is this information collected/used for?
Employees	
Identification (such as name, gender, address, passport or visa, drivers' licence, date of birth).	To verify identity and working rights in Australia and for the Nationally Coordinated Criminal History Check.
Contact details (such as telephone, home address, email address, emergency/next of kin contact).	To enter into an employment agreement contract with CME and to ensure next of kin/emergency contact can be contacted in case of an emergency.
Background details (such as qualifications, previous employment, referees, criminal records).	To undertake due diligence as part of the recruitment and selection process.
Employment details (such as position title, employment contract, performance and disciplinary records, personal and annual leave records, promotions, transfers and secondments, training).	To carry out the employment contract between the employee and employer and ensure compliance with company policies, and regulations and legislation relevant to the workplace.
Medical history and current prescribed medications, drug and alcohol screening testing results.	To undertake due diligence as part of the recruitment and selection process and to adhere to the CME Occupational Safety, Health and Wellbeing and Fitness for Work Policies.
Financial information (such as bank account, tax file number, salary, allowances, superannuation).	To carry out the employment contract, remunerate the employee, and ensure finance and tax compliance.
Diversity information (such as gender, age, cultural group i.e., Indigenous, carer responsibilities).	For accurate and meaningful internal reporting purposes.
Members	
Contact details (such as name, current and past employer/company, position title, work telephone, work email address, workplace address).	To provide information to members relating to CME's activities, events, and projects, and to provide information that may assist the business operations of the company/organisation to which individuals belong.
Identification (such as name, gender, address, passport or visa, drivers' licence, date of birth).	To provide the Australian Criminal Intelligence Commission and Police, in order to conduct the Nationally Coordinated Criminal History Check.
Data collected through annual CME surveys including but not limited to: - Employee information (such as gender, ATSI descent, occupational category, employment status, residential postcode) - Financial information (such as employee	To accurately represent the contributions and demographics of the sector and to use the data as an evidence base to advocate and inform the government on policy and regulatory decision-making processes that may impact members.

This document is protected by copyright. No part of this document may be reproduced, adapted, transmitted, or stored in any form by any process (electronic or otherwise) without the specific written consent of the Chief Executive. All rights are reserved.

wages, salaries, superannuation and allowances) - Payments made to suppliers, labour-hire and services, local councils and government - Other relevant vendor or organisational details (such as ABNs, the primary purpose of the payment and identification as an Indigenous-owned or Indigenous-run business).	
Employee photo images.	For marketing purposes.
Third Parties including suppliers	
Contact details (such as work telephone, work email address, workplace address).	To carry out due diligence prior to entering into a relationship with the third party and/or to decide whether to continue a business relationship with the third party.
Financial information (such as ABN, bank account).	To carry out the contract and pay the supplier.

This document is protected by copyright. No part of this document may be reproduced, adapted, transmitted, or stored in any form by any process (electronic or otherwise) without the specific written consent of the Chief Executive. All rights are reserved.