Policy

Privacy Policy Australia

Document number:	XXX-YYY-100001 AUS-X200-570-POL-009
Document owner:	HR Manager – Australia West and HR Manager – Australia East
Document author:	Josephine Robinson
Revision:	1
Revision date:	22-Dec-2015
This document supports Human Resources	

About this document:	This is a policy document to provide rules for the Australian business to operate to protect the privacy of individuals in accordance with the Privacy Act 1988 (Cth) (the Act)
Who this document applies to:	This document applies to Amec Foster Wheeler Australia locations
Responsibility for this document:	The functional responsibility for the development, review and maintenance of this document rests with the HR Manager – Australia West and HR Manager – Australia East

Contents

1 Purpose and Scope

Amec Foster Wheeler is committed to protecting the privacy of individuals in accordance with the Privacy Act 1988 (Cth) (the Act). The Act establishes practices to be adopted by organisations in respect of the protection of all personal information about individuals which is collected, held, used, disclosed, processed or otherwise handled. The Act includes the Australian Privacy Principles (APPs) which set out obligations in respect of the handling of personal information and are binding on Amec Foster Wheeler.

2 Policy

2.1 Criteria for Use

This policy shall apply to all Amec Foster Wheeler's Personnel in Australia to whom the Act applies.

It should be noted that certain particulars in the Employee Records are exempt from the Act (but only to the extent that the relevant act or practices are directly related to the employment relationship). These particulars include:

1. Health information about an employee (although state based legislation regulating health records will apply)
2. Personal information relating to the engagement, training, disciplining, resignation or termination of employment of an employee
3. Personal information relating to the terms and conditions of employment of an employee
4. Personal information relating to the employee's performance or conduct, hours of employment, salary or wages, personal and emergency contact details
5. Personal information relating to the employee's membership of a professional or trade association or trade union membership
6. Personal information relating to the employee's recreation, long service, sick, maternity, paternity or other leave
7. Personal information relating to the employee's taxation, banking or superannuation affairs.

2.2 Privacy Protection

Under the Act, protecting the privacy of individuals relates to safeguarding their personal information. '*Personal information*' is information or an opinion about an identified individual, or an individual who is reasonably identifiable. Some information collected by Amec Foster Wheeler may also be considered sensitive information. Sensitive information includes information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, sexual preferences, criminal record, health information, and biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or biometric templates.

2.3 Types of Personal Information Held

We will only collect and hold personal information that is reasonably necessary for one or more of our functions or activities, including in order to engage Personnel. Therefore, we will hold personal information such as, but not limited to, an

individual's name, address, telephone numbers, email address and other contact details, bank account details, and tax file number.

2.4 How We Collect and Hold Personal Information

Except as set out below, personal information will generally be collected directly from an individual unless it is unreasonable or impractical to do so or the individual was recruited or put forward to Amec Foster Wheeler by an agency (and subsequently has consented to their personal information being provided to Amec Foster Wheeler by the agency).

Sensitive information will only be collected with the individual's consent and if such information is required or authorised by or under Australian law. Sensitive information will also be collected for Permitted General Situations and Permitted Health Situations.

All information will be collected by lawful and fair means.

We can collect personal information from a variety of sources, including the following:

- An employee's resume and job application
- Third parties such as medical service providers and referees
- Publicly available sources
- Our own records of an individual's possible previous engagement with us
- The individual's use of computer facilities provided by us, including e-mail and internet facilities.

Our HR department holds both electronic and paper based files of all of our Personnel. Those files contain relevant information about each employee, contractor and subcontractor. Access to these files is limited to Amec Foster Wheeler's Payroll department, HR department and IT department.

If an individual chooses not to provide us with his or her personal information, we will not be able to engage that individual as an employee, independent contractor or subcontractor.

2.5 Collection of Personal Information from Unsolicited Sources

In the event we receive personal information and we did not solicit that information, we will, within a reasonable period after receiving the information, determine whether or not we could have lawfully collected the information. If we determine that we could not have lawfully collected the personal information, we will, as soon as practicable, and only if it lawful and reasonable to do so, destroy the information. If however, we determine that we could have lawfully collected the personal information, we will manage the personal information in accordance with this policy.

2.6 Notification of the Collection of Personal Information

We will, at or before the time, or if that is not practicable, as soon as practicable after the collection of personal information, notify the individual that we are collecting the individual's personal information and we will also notify them of certain things and obtain their consent to the same. This notice will also contain the following:

1. Our contact details
2. The purpose for which we are collecting the personal information

3. The consequences (if any) for the employee if all or some of the personal information is not collected by us
4. Any other related body corporations or entity to which we usually discloses personal information
5. Our disclosure of personal information to our overseas related corporate bodies and their relevant countries.

2.7 General Disclosure or Use of Personal Information

We will only use and disclose an individual's personal information for the primary purposes for which it was collected (primary purpose). For example, information may be collected for employment purposes or to discharge our obligations to comply with our duty of care to Personnel.

We will only use or disclose personal information without the individual's consent in situations where the individual could reasonably expect Amec Foster Wheeler to use or disclose that information for another purpose (secondary purpose) and that secondary purpose is:

1. For sensitive information, directly related to the primary purpose or
2. For information that is not sensitive, related to the primary purpose

Secondary purposes may include our disclosure of an individual's personal information to organisations outside of Amec Foster Wheeler in order to fulfil our obligation to our workforce and our clients. For example, we may disclose personal information to

1. Companies, firms or individuals who assist us in providing services to our clients or who perform functions on our behalf, including our Subconsultants
2. Our prospective clients when we bid for jobs or to our clients when required to do so by the client
3. An individual's authorised representatives or legal advisers
4. The employer of Subconsultants
5. Our related companies, including those in overseas jurisdictions
6. Our professional advisors, including insurance brokers and insurers, accountants, auditors and solicitors
7. Government and regulatory authorities and other organisations, as required or authorised by law
8. Anyone else to whom the individual has consented for us to disclose it.

We will take reasonable steps to ensure that these organisations are bound by confidentiality and privacy obligations in relation to the protection of an individual's personal information.

We will also only use or disclose personal information without the individual's consent if

- That information is required for a Permitted Health Situation
- That information is required for a Permitted General Situation
- We reasonably believe that the information is required or authorised by or under Australian law or by a court/tribunal order

or

- We reasonably believe that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on

behalf of, an enforcement body and the employee is notified in writing of this disclosure

In the event that collection, use or disclosure of personal information results in a Permitted Health Situation, we will ensure that the information collected cannot be identified as the relevant individual's personal information.

We may disclose an individual's personal information to clients and other parties located outside Australia including, but not limited to, the Philippines. We will ensure that the individual is notified of the same and will take reasonable steps to ensure that such recipients respect the individual's privacy by abiding by the Act or equivalent privacy laws.

2.8 Storage and Security of Personal Information

We will take every reasonable step to protect the security of personal information. As part of that obligation, we recognise that certain departments within our organisation require access to other people's personal information consistent with their professional responsibilities. Consequently, this requirement brings with it an obligation for these individuals to understand and acknowledge the nature and limits of their access to and use of personal information.

We require our Personnel to respect the privacy of other people and to comply with this Privacy Policy together with any internal procedures.

We will also take reasonable steps to protect personal information from misuse, loss, interference, unauthorised access, modification or disclosure by means of physical security and restricted access to electronic and paper based records.

We may archive personal information where appropriate.

2.9 Updating Personal Information

Amec Foster Wheeler endeavours to ensure that the personal information it holds is accurate, complete and up-to-date. However, the accuracy of that information depends to a large extent on the information individuals provide to us. Therefore, we encourage everyone to contact relevant Amec Foster Wheeler personnel using the details set out in section 2.10 below in order to update any personal information we hold about them. We will periodically audit the personal information we hold so as to ascertain if that information is accurate, complete and up-to-date.

2.10 Individual Access to Personal Information

Subject to the exceptions set out in the Act, such as in relation to employee records, or to Amec Foster Wheeler's obligations under the Freedom of Information Act, individuals may, in most circumstances, seek access to the personal information which we hold about them by contacting:-

HR Manager – Australia West Level 7, 197 St Georges Terrace Perth WA 6000	OR	HR Manager – Australia East Level 4,144 Edward Street Brisbane QLD 4000

For security reasons, we require requests to be put in writing. We may charge a fee for providing access and we will advise you of the likely cost in advance. We will not charge for simply making the request and will not charge for making any corrections to an individual's personal information. We will endeavour to provide the requested information as soon as practicable.

2.11 Breach of the Act and Complaints

If a breach of the Act occurs, we may, depending on the nature of the breach, report that breach to the Office of the Australian Information Commissioner and will follow any directions the Commissioner makes in respect to the same.

If an individual wishes to make a compliant regarding an apparent breach of the Act or the treatment of their personal information, the individual must issue Amec Foster Wheeler with a written statement advising of the same and the consequences (if any) of that breach. All written statements can be sent to:-

Amec Foster Wheeler's Senior Legal Counsel – Asia Pacific
Level 7, 197 St Georges Terrace
Perth WA 6000

We will treat all requests or complaints confidentially. Our representative will contact the individual within a reasonable time after receipt of the individual's complaint to discuss his or her concerns and outline options regarding how they may be resolved. We will aim to ensure that the complaint is resolved in timely and appropriate manner.

If, after investigation of the complaint by Amec Foster Wheeler, we agree that a breach of the Act has occurred, Amec Foster Wheeler may refer the matter to the Commissioner for directions.

2.12 Privacy Enquiries or Concerns

If individuals have any privacy queries or requires advice about this Policy, individuals should contact Amec Foster Wheeler's Senior Legal Counsel – Asia Pacific on (08) 9347 4777, or the HR Manager - Australia West on (08) 9347 4777, or the HR Manager - Australia East on (07) 3033 5600 in the first instance. Written correspondences can be sent to:

Level 7, 197 St Georges Terrace
Perth WA 6000

Or

Level 4,144 Edward Street
Brisbane QLD 4000

We may change this Privacy Policy from time to time. Any updated versions of this Policy will be posted on our website at www.amecfw.com and will be provided to all Personnel.

3 Definitions

The following terms are used within this document.

Term	Definition
Act	The Privacy Act 1988 (Cth)
Amec Foster Wheeler	Amec Foster Wheeler Australia Pty Limited and includes any subsidiary that operates within Amec Foster Wheeler's Australia region and is operating within this Human Resource Policy Framework as referred to in the HR Mandate. Amec Foster Wheeler is also referred to as "the Company", "we", "us" and "our"
Australian Privacy Principles ("the APPs")	The set of binding obligations in the Act regarding the collection, use, disclosure, management and processing

Term	Definition
	of personal information. A copy of these principles are attached in **Annexure A**
Contractor	A person under a contract for services, who undertakes business or trade through a third party
Employee	A person who is under a contract of services, is a salary or wage earner, is employed within an enterprise agreement; and subject to tax deductions from a company in the Amec Foster Wheeler group of companies
Employee Record	The record of personal information relating to an employment relationship between an individual an Amec Foster Wheeler
Permitted General Situations	The following situations in which the collection, use or disclosure of personal information is necessary a) Situations in which it is unreasonable or impracticable to obtain consent and Amec Foster Wheeler reasonably believes the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual or to public health or safety b) Situations in which Amec Foster Wheeler has reason to suspect that unlawful activity or misconduct of a serious nature that relates to Amec Foster Wheeler's business function has been, is being, or may be engaged in and that Amec Foster Wheeler reasonably believes that the collection, use or disclosure is necessary in order for it to take appropriate action in relation to that unlawful activity or misconduct c) Situations in which Amec Foster Wheeler reasonably believes that collection, use or disclosure is reasonably necessary to assist in locating the employee's whereabouts if that employee is reported as missing; d) Situations whereby it is necessary for the establishment, exercise or defence of a legal or equitable claim e) Situations whereby it is necessary for the purposes of a confidential alternative dispute resolution process
Permitted Health Situation	The following situations in which the collection, use or disclosure of health information by Amec Foster Wheeler about an individual is necessary include a) Research relevant to public health or public safety b) The compilation or analysis of statistics relevant to public health or public safety

Term	Definition
	c) The management, funding or monitoring of health services and d) The particular purpose cannot be served by collecting de-identified information and e) It is impracticable for the organisation to obtain the individual's consent to the collection; and f) The collection is required by or under Australian Law or g) The information is collected in accordance with rules established by health or medical bodies; or h) That the purpose for collection of the information is approved by the Commissioner and the collection of that information is in the public's best interest
Privacy Protection	Protecting the privacy of individuals relates to safeguarding their personal information
Personal Information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable
Personnel	Employees, independent contractors and subcontractors
Sensitive Information	Includes information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, sexual preferences, criminal record, health information, and biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or biometric templates
Subconsultant	A person under a contract for services, who operates on business or trade, paid by submitting invoice from this business to a company in the Amec Foster Wheeler group of companies and is responsible for managing their business activities and associated taxes and includes independent contractors and/or consultants

4 References

Document type	Document title	Document no.
Delivery Strategy	HR Mandate	AUS-X200-570-REG-001
Procedure	Privacy Procedure	AUS-X200-570-PRO-021

5 Revision History

Revision no.	Revision date	Summary of changes
0	Mar-2014	First Issue
1	Oct-2015	Update to company name, brand and format

6 Appendices

Appendix A Australian Privacy Principles ("the Principles")

1. Principle 1 – Open and Transparent Management of Personal Information

Organisations must take steps as are reasonable to implement practise, procedures and systems relating to the organisation's function or activities that will ensure that organisation's compliance with these Principles and will enable the organisation to deal with inquiries or complaints from individuals about the organisation's compliance with these Principles.

An organisation must have a clearly expressed and up-to-date policy about the management of personal information by the organisation.

The organisation's policy must contain the following information

1. The kinds of personal information that the organisation collects and holds
2. How the organisation collects and holds personal information
3. The purposes of which the entity collects, holds uses or discloses personal information
4. How an individual may access personal information about the individual that is held by the organisation and seek the correction of such information
5. How an individual complaints about a breach of these Principles and how the organisation will deal with such complaint
6. Whether the organisation is likely to disclose personal information to overseas recipients and
7. If the organisation is likely to disclose personal information to overseas recipients, the counties in which such recipients are likely to be located if it is practicable to specify those counties in the policy

Organisations must make its privacy policy available free of charge and in such form as is appropriate. If a person requests a copy of the organisation's privacy policy in a particular form, the organisation must take such steps as are reasonable in the circumstances to give the persona copy of the policy in that form.

2. Principle 2 – Anonymity and Pseudonymity

Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an organisation, unless this is impracticable.

3. Principle 3 – Collection of Solicited Personal Information

In respect to the collection of solicited information, personal information must not be collected unless it is necessary for, or directly related to, an entity's functions or activities. An entity must collect information directly from an individual unless it is unreasonable or impracticable to do so. Sensitive information must not, subject to the below, be collected except with consent.

Sensitive information can also be collected for Permitted General Situations or for Permitted Health Situations or if such information is required or authorised by or under Australian law.

Permitted Health Situations means situations in which the collection, use or disclosure of personal information that is necessary

1. So to lessen or prevent a serious threat to the life, health or safety of any individual or to public health or safety
2. As the organisation has reason to suspect that unlawful activity or misconduct of a serious nature that relates to the organisation's business function has been, is being or may be engaged in and that the organisation reasonably believes that the collection, use or disclosure is necessary in order for it to take appropriate action in relation to that unlawful activity or misconduct
3. As the organisation reasonably believes that collection, use or disclosure is reasonably necessary to assist in locating the individual's whereabouts if that individual is reported as missing
4. For the establishment, exercise or defence of a legal or equitable claim and
5. For the purposes of a confidential alternative dispute resolution process

Permitted Health Situations means situations in which the collection, use or disclosure of health information about an individual is necessary as

1. Such collection is necessary for
   - Research relevant to public health or public safety
   - The compilation or analysis of statistics relevant to public health or public safety
   - The management, funding or monitoring of health services and
2. The individual's information is de-identified and therefore, the purpose cannot be specified by the collection of the information and
3. It is impracticable for the organisation to obtain the individual's consent for the collection and
4. The collection is required by or under Australian Law or
5. The information is collected in accordance with rules established by health or medical bodies or
6. That purpose for collection of the information is approved by the Commissioner as the collection of the health information is in the public's best interest

4. Principle 4 – Dealing with unsolicited personal information

When an organisation receives unsolicited personal information, it must, within a reasonable period, determine whether it could have collected that information under Principle 3. If so, it must treat that information in accordance with Principles 5 to 13. If not, it must destroy or effectively de-identify that information.

5. Principle 5 – Notification of the collection of personal information

An organisation must provide privacy notification statements at, before or as soon as practicable after collecting personal information. The notice must contain the following information

1. The organisation's contact details
2. Notice that the organisation is collecting the individual's personal information
3. The purpose for which the organisation is collecting the personal information
4. The consequences (if any) for the organisation's personnel if all or some of the personal information is not collected by the organisation

5. Notice of any other related body corporations or entity to which the organisation usually discloses personal information
6. The organisation's privacy policy containing information as to how individuals may access their personal information and how they are to correct such information
7. Information regarding how individuals may complain about a breach of these Principles and how the organisation will deal with such complaints
8. The organisation's disclosure of personal information to its overseas related corporate bodies and their relevant countries

6. Principle 6 – Use or Disclosure of personal information

Personal information can be used or disclosed for the purpose for which it was collected, or a related (or in the case of sensitive information, directly related) purpose that the affected individual would reasonably expect. The exception to this rule is

1. If the individual has consented to use or disclosure for another purpose
2. Whereby that information was required for a Permitted General Situation
3. Whereby that information was required for a Permitted Health Situation
4. In circumstances whereby the organisation reasonably believes that the information is required or authorised by or under Australian law or by a court/tribunal order or
5. The organisation reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities and in this regard, the individual has been notified in writing of this disclosure

In the event a collection, use or disclosure of personal information resulted due to a Permitted Health Situation, the organisation will ensure that the information cannot be identified as the relevant individual's personal information.

7. Principle 7 – Direct marketing

There are special rules for direct marketing, other than direct marketing that will be governed by the *Spam Act 2003* (Cth) or the *Do Not Call Register Act 2006* (Cth) (that is, these Principles will not apply to electronic marketing or telemarketing). Sensitive information cannot be used for marketing without the consent of the individual. In general, if the personal information used was collected from the individual, it can be used for marketing if this would be reasonably expected by the individual. If the information was collected from a third party or if the individual would not otherwise reasonably expect the direct marketing then it can be used for marketing only if the individual consents or it is impracticable to get consent. In all cases an opt-out from marketing must be provided.

8. Principle 8 – Cross-Border disclosure of personal information

In respect to cross-border disclosures of personal information, before an organisation discloses personal information to an overseas recipient, the organisation must take reasonable steps to ensure that the recipient does not breach these Principles. If the overseas entity is not bound by these Principles, any act by the overseas entity that breaches these Principles will be taken to have been committed by the Australian entity. However there will be a number of exceptions to

these general rules. One is where the overseas recipient is subject to a law or binding scheme that provides substantially similar, or higher protection, than these Principles and the individual has access to mechanisms that enforce those protections. Another exception is where the affected individual consents to the disclosure overseas, after having been expressly informed that the entity will, as a result, not be required to take reasonable steps to ensure that the overseas recipient will comply with these Principles.

9. Principle 9 – Use or disclosure of government related identifiers

Organisations must not adopt government-related identifiers.

10. Principle 10 – Quality of personal information

Organisations must take reasonable steps to ensure that personal information collected, used or disclosed is accurate, up-to-date and complete and (in the case of disclosure) relevant.

11. Principle 11 – Security of personal information

An organisation must take reasonable steps to protect personal information from misuse, interference, loss and unauthorised access, modification and disclosure. Personal information must be destroyed or de-identified if no longer needed for the purposes for which it may be used or required to be retained for legal reasons.

12. Principle 12 – Access to personal information

Individuals have a right to access their personal information within a reasonable period after the request is made and that personal information shall be provided in the manner requested by the individual, if that manner is reasonable and practicable to do so.

If the organisation cannot provide the information in the manner requested by the individual, the organisation must take steps as are reasonable in the circumstances to give access in a way that meets the needs of both the organisation and the individual.

The organisation is not required to give the individual access to the personal information to the extent that

1. The organisation reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or safety
2. Giving access would have an unreasonable impact on the privacy of other individuals
3. The request for access is frivolous or vexatious
4. The information relates to existing or anticipated legal proceedings between the organisation and the individual and that information would not be accessible by the process of discovery in those proceedings
5. Giving access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations

6. Giving access would be unlawful
7. Denying access is required or authorised by or under Australian law or a court/tribunal order
8. The organisation has reason to suspect that the unlawful activity or misconduct of a serious nature that relates to the organisation's functions or activities have been, is being or may be engaged and giving access would be likely to prejudice the taking of appropriate action in relation to the matter
9. Giving access would likely prejudice one or more enforcement related activities or
10. Giving access would reveal evaluative information regarding the organisation in connection with a commercially sensitive decision-making process

If access cannot be provided and the information falls within the categories referred to above, the organisation must provide the individual with written notice setting out the reason for the refusal together with a copy of the organisation's privacy policy. The written notice must highlight the mechanisms available for the individual to complain about the refusal.

The organisation can charge the costs incurred for giving individual access to their information, however the charge must not be excessive. The organisation cannot charge the individual for making the request.

13. Principle 13 – Correction of personal information

Organisations must ensure all personal information is accurate, complete and up-to-date. In the event an individual notifies the organisation that the personal information is not accurate or up-to-date or the organisation ascertains the same from its own investigations, the organisation must amend its records to correct such information within a reasonable time after notification of the same. If the personal information was disclosed to a third party, the organisation must ensure that third party is notified that the personal information needs to be amended. The organisation cannot charge the individual for making such modifications.