

Policy – Privacy

Policy Name:	Privacy	Status:	Approved
Policy Number:	2014:10	Version:	4
Document Originated:	Governance, Risk & Compliance	To be Reviewed:	February 2022
Effective Date:	12 March 2014	Approval Authority:	IEUA-QNT Branch Executive

1. RATIONALE

Good governance is essential for effective leadership and successful outcomes. Governance is seen as the processes and structures used to direct and manage the objects, the conduct and affairs of the Union ensuring the organisation operates in a responsible and ethical manner with the goal of ensuring financial viability, enhancing reputation and creating value for its members.

IEUA-QNT is committed to the protection of the personal information of its members and others. This policy complies with relevant provisions of the Privacy Act 1988, the Privacy Amendment (Enhancing Privacy Protection) Act 2012 and the Privacy Amendment (Notifiable Data Breaches) Act 2017.

2. PURPOSE

The purpose of this policy is to explain how the IEUA-QNT will manage personal information and in the event of a loss of personal information, how it will respond. Personal information is data that could contribute to the identification of an individual. Personal data of employees of IEUA-QNT held for the proper purposes of employment, is not subject to this Policy.

3. POLICY STATEMENT

The IEUA-QNT collects personal information about members and prospective members to enable the facilitation of union services in accordance with the Objects of the Union. IEUA-QNT does not collect personal information for any other purpose than for the facilitation of membership services.

IEUA-QNT collects directly from members and prospective members their name, address, contact information and details of employment. Financial information reasonably necessary for the collection of membership fees is also requested.

Membership information is retained on an electronic database dedicated to the secure custody of membership data.

Individual data collected for the purposes of industrial representation may be retained in a file dedicated to the member.

An individual may request a copy of their personal information held by us or may lodge a complaint in relation to the privacy of information held by writing to the Branch Secretary at the registered address of the Union. The Branch Secretary will respond in writing within 14 days.

IEUA-QNT is committed to ensuring the security and accuracy of personal information in accordance with the Australian Privacy Principles and the Fair Work (Registered Organisations) Act 2009.

4. PROCEDURES

IEUA-QNT will comply with the Australian Privacy Principles in the following manner:

- 1. Open and transparent management of personal information** is achieved by adherence to this Policy. This Policy will be published on the organisation's website and made available to anyone on request and free of charge.
- 2. Anonymity and pseudonymity.** Persons who do not wish to identify themselves may make general enquiries of the Union. However, as an organisation dedicated to the service of members only, it will in most cases, be impractical for IEUA-QNT to deal with individuals who have not identified themselves or have used a pseudonym.
- 3. Collection of solicited personal information.** The Union will request such information as is reasonable for the purpose of recruiting new members and for maintaining a database of current members in accordance with the requirements of the Fair Work (Registered Organisations) Act 2009. Additional information may be requested to facilitate a member's specific industrial matter. IEUA-QNT only collects personal information, including any sensitive information that is necessary for or relates to, the activities of the organisation.
- 4. Dealing with unsolicited personal information.** Any unsolicited personal information or identifying data of a person not reasonably required for the purposes of the Objects of the Union will be de-identified or destroyed as soon as practicable.
- 5. Notification of the collection of personal information.** Notwithstanding the organisation's policy on dealing with solicited or unsolicited information, IEUA-QNT will, as soon as practicable, notify the individual that the Union is in possession of such information, why the information has been collected, any consequences for

the individual and to whom such information might be disclosed. We will direct the individual to this Policy and to their rights to correct or complain about the collection of such data.

- 6. Use or disclosure of personal information** is restricted to the purposes of the Objects of the Union and not for any other purpose.
- 7. Direct marketing** refers to unsolicited offers of goods or services for sale. IEUA-QNT will not use personal information for the purposes of direct marketing. However, we may advise members of Union related goods and services offered to Union members as part of a scheme maintained for the benefit of members.
- 8. Cross-border disclosure of personal information.** IEUA-QNT will not disclose personal information to persons or entities not located in Australia unless the recipient is subject to a law protecting the information in a way that is at least substantially similar to the Australian Privacy Principles.
- 9. Adoption, use or disclosure of government related identifiers.** Government identifiers such as, but not limited to, tax file number, Medicare number or social security information is not and will not be collected by IEUA-QNT.
- 10. Quality of personal information.** IEUA-QNT will take all reasonable steps to ensure the personal information it collects and uses is at all times accurate, up to date, complete and relevant.
- 11. Security of personal information.**
- 12.** IEUA-QNT takes security very seriously and has enacted significant security precautions in relation to electronically held personal information. We will take all reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification and disclosure. The organisation will de-identify or destroy all personal information it is not required to keep for the proper maintenance of membership records. Data breaches occur when personal information falls into the hands of unauthorised persons. Whilst the organisation takes precautions against the release of personal data it can not guarantee such loss will never eventuate. In the event such loss does occur, IEUA-QNT undertakes to advise affected individuals as soon as practicable of the details of the loss and any remedial action taken to retrieve and prevent a similar occurrence.
- 13. Access to personal information.** The organisation will make available to an individual on request, a copy of personal information it holds on the individual unless the granting of access is legally prejudicial to another individual, entity or to the organisation.
- 14. Correction of personal information.** An individual may request IEUA-QNT to correct personal information it holds. We will respond to such requests as soon as practicable and make such changes as required free of charge.

IEUA-QNT will comply with the Privacy Amendment (Notifiable Data Breaches) Act 2017 in the following manner:

1. A data breach assessment will be undertaken by the Branch Secretary or delegates(s) immediately following the identification of a data breach. In principle,

risk management techniques shall be used to assess the likelihood of harm to an individual and the consequences that may arise. The Privacy Amendment (Notifiable Data Breaches) Act 2017 only mandates notification to those individuals likely to suffer “serious harm”. However, IEUA-QNT will notify all affected individuals of a data breach, the manner in which it occurred, the assessed level of risk or harm and options available to mitigate such risk or harm. Notification is important to the individual so that they may take action appropriate in their circumstances. The Risk Management processes of IEUA-QNT will manage the environment that permitted the breach so that identified weaknesses are managed.

2. Notification to OAIC is required under the Act if a data breach is likely to result in serious harm to any of the individuals to whom the information relates. The Commissioner’s website has guidance on when and how to report.

5. APPLICABILITY

This policy applies to the IEUA-QNT.

6. DEFINITIONS

data breach means, when personal information held by IEUA-QNT is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference.

De identified: personal information is de-identified if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.

OAIC is the Office of the Australian Information Commissioner and the regulator of the Privacy Act and associated legislation.

Personal information means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Sensitive information means:

- (a) information or an opinion about an individual’s:
 - (i) racial or ethnic origin; or
 - (ii) political opinions; or
 - (iii) membership of a political association; or
 - (iv) religious beliefs or affiliations; or
 - (v) philosophical beliefs; or
 - (vi) membership of a professional or trade association; or
 - (vii) membership of a trade union; or
 - (viii) sexual preferences or practices; or
 - (ix) criminal record;

that is also personal information; or

- (b) health information about an individual; or

(c) genetic information about an individual that is not otherwise health information.

Serious harm is a term used but not defined in the Act. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm.

Solicits: an entity solicits personal information if the entity requests another entity to provide the personal information, or to provide a kind of information in which that personal information is included.

7. PERSONS RESPONSIBLE

The Branch Secretary has oversight of policy and should be consulted for interpretations, resolution of problems and special situations.

8. POLICY AUTHORITY

This Policy is authorised by the Branch Executive.

9. RELATED DOCUMENTS AND LINKS

Privacy Act 1988

Privacy Amendment (Enhancing Privacy protection) Act 2012

Privacy Amendment (Notifiable Data Breaches) Act 2017

Regulated by: www.oaic.gov.au

10. REVISION HISTORY

This policy will be reviewed in light of changes to the Privacy Act 1988 and the Fair Work (Registered Organisations) Act 2009 and the Privacy Amendment (Notifiable Data Breaches) Act 2017.

Revision	Date	Made By	Approved By	Reason
1	17 February 2014	GRC	Branch Executive	New Policy to replace Privacy Statement Ref: in8475tb:nm 30 November 2001
2	30 October 2015	GRC	Branch Executive	Review
3	4 February 2018	GRC	Branch Executive	Updated to include requirements of the Privacy Amendment (Notifiable Data Breaches) Act 2017
4	2 February 2020	Branch Secretary	Branch Executive	Review