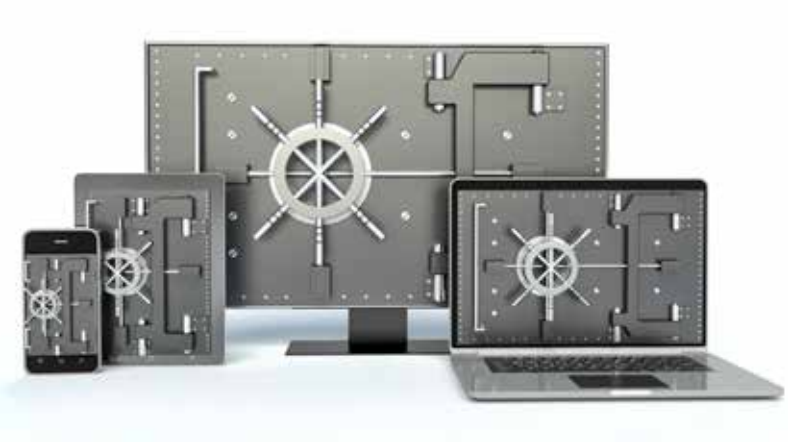
Policy Statement

Privacy Policy



The IAC Group is committed to managing the Privacy risks associated with our activities and operations. It is recognised that the Privacy of Stakeholders is important and vital to the success of our business and as such, we aim to continuously improve Privacy Provisions through consultation and increased awareness of all stakeholders.

To assist in achieving the highest level of compliance with this policy statement, the following responsibilities are allocated:

- Executive responsibility is assigned to the Managing Director. This manager is responsible for the design, establishment, implementation, maintenance and review of the overall risk management function in consultation with all relevant parties. In addition, this manager shall be responsible for ensuring that all policies, procedures, practices, rules and the like are consistent with all other management functions.
- Officers and workers at all levels are responsible for the implementation, maintenance and review of the Privacy management policies, procedures, practices, rules and the like.
- Stakeholers, students and visitors shall be made aware of our commitment. In addition, they shall be expected to comply with the relevant WHS management policies, procedures, practices, rules and the like.

The IAC Group “We” respects the privacy of those who purchase our products and services.

We are required to collect, use, store and disclose a range of personal information on students, employees and a range of other stakeholders.

We are committed to maintaining the privacy of all student, client and personnel records.

We will comply with all privacy legislative requirements which include the Commonwealth Privacy Act 1988 and the 13 Australian Privacy Principles (APPs) as outlined in the Commonwealth Privacy Amendment (Enhancing Privacy Protection) Act 2012.

Our policy is to take reasonable steps to make stakeholders aware that we are collecting personnel information about them, the purpose for which it is being collected, and who, (if applicable), we might pass the information on to.

David Conyngham Managing Director

Version 3, May 2021

Australian Privacy Principles
— a summary for APP entities

from 12 March 2014 Australian Information Commissioner

Australian Government
Office of the
Australian Information Commissioner

APP 1 — Open and transparent management of personal information
Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 — Anonymity and pseudonymity
Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 — Collection of solicited personal information
Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 — Dealing with unsolicited personal information
Outlines how APP entities must deal with unsolicited personal information.

APP 5 — Notification of the collection of personal information
Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 — Use or disclosure of personal information
Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 — Direct marketing
An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 — Cross-border disclosure of personal information
Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 — Adoption, use or disclosure of government related identifiers
Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP 10 — Quality of personal information
An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 — Security of personal information
An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 — Access to personal information
Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 — Correction of personal information
Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

For private sector organisations, Australian Government and Norfolk Island agencies covered by the Privacy Act 1988

Privacy Program

1. PROGRAM OBJECTIVE

The purpose of this Policy ('Policy') is to provide guidance on Privacy Provisions in connection with authorised work for the IAC Group and its separate business units.

2. PROGRAM APPLICATION

This Policy applies to all employees of the Company and persons authorised to provide products and services on the Company's behalf.

It is the responsibility of all employees of the Company and persons authorised to provide products and services on the Company's behalf to understand and comply with this Policy; and the responsibility of Company managers to assist with monitoring and enforcing the terms of the Policy.

This Policy does not form part of an employee's contract of employment ("Contract") or any other user's contract ("Contract").

NOTE: Where the term "we" "our" or "us" is used, it refers to the IAC Group and all of its separate business units - IAC Safety Services, Supply Workforce and ASP Assist.

3. PROGRAM GUIDELINES

To comply with the Privacy Act 1988 (Privacy Act) and Australian Privacy Principle guidelines (APP guidelines). We must make every reasonable attempt to ensure the 'avoidance of acts or practices that may or might be interferences with the privacy of individuals, or which may otherwise have any adverse effects on the privacy of individuals'.

The APPs are structured to reflect the personal information lifecycle, grouped into 5 parts:

- Part 1 — Consideration of personal information privacy (APPs 1 and 2)
- Part 2 — Collection of personal information (APPs 3, 4 and 5)
- Part 3 — Dealing with personal information (APPs 6, 7, 8 and 9)
- Part 4 — Integrity of personal information (APPs 10 and 11)
- Part 5 — Access to, and correction of, personal information (APPs 12 and 13).

Personal Information stages

Consideration » Collection » Deal with » Integrity » Access to, and correction of personal information

Part 1 — Consideration of personal information privacy (APPs 1 and 2)

Consideration » Collection » Deal with » Integrity » Access to, and correction of personal information

1APP. Open and transparent management of personal information

Our reasonable steps

The information presented in this publication detail the APP factors we have considered as they relate to us. We have taken proactive steps to establish and maintain internal practices, procedures and systems that ensure compliance with the APPs. The obligation to implement practices, procedures and systems is qualified by a 'reasonable steps' test.

Prescribed within this publication are the full details on how we manage Our Privacy Obligations.

In addition, a separate publication exists for stakeholders, that explains how we manage Our Privacy Obligaions.

Introduction

We recognise that your personal information is important to you and we respect that.

We are committed to managing your personal information openly and transparently and to keeping your personal information safe, including to:

- comply with the Australian Privacy Principles ("APPs");
- ensure that we manage your personal information openly and transparently;
- only collect personal information from you that we need in order to offer you the best possible service and customer experience;
- tell you how we might use your personal information;
- let you know if we need to disclose your personal information to anyone else (including anyone overseas) and if so, in what circumstances this might occur;
- keep your personal information secure;
- promptly respond to any request by you not to receive direct marketing material from us;
- make sure your personal information is kept accurate and up to date and to properly dispose of any personal information which is no longer required by us; and
- ensure that, where appropriate, you can access and correct your personal information.

Responsible Persons

To assist in achieving the highest possible level of compliance with this policy statement, Executive responsibility is vested in Felicity Manarin who is responsible for control and issuance of the policy and this includes the design, establishment, implementation, maintenance and review of the overall privacy program in consultation with all relevant stakeholders. This also comprises the management of privacy risks at all stages of the information life cycle such as use, storage, disclosure, and de-identification and destruction.

In addition, this manager shall be responsible for ensuring that all policies, procedures, practices, rules and the like are consistent with all other business functions.

Stakeholders are made aware of our commitment to Privacy and also are expected to comply with all policies, procedures, practices, rules and the like within their level of authority.

Should you have an issue with any aspect to do with Privacy, your contact is:

Privacy Officer
Felicity Manarin felicity@iac.edu.au 1300 887 317

Review and update of this Privacy and Confidentiality Policy

We review this Privacy and Confidentiality Policy on an ongoing basis, as suggestions or issues are raised and addressed, or as government-required changes are identified; through our internal audit processes at least annually; and as a component of each complaint investigation process where the complaint is related to a privacy matter.

Whenever this policy is updated, changes to the policy are widely communicated to stakeholders internally through staff communications, meetings, training and documentation, and externally through publishing of the policy on our websites and other relevant documentation for clients.

Under the Data Provision Requirements 2012, IAC Safety Services is required to collect personal information about you and to disclose that personal information to the National Centre for Vocational Education Research Ltd (NCVER). Your personal information (including the personal information contained on the enrolment form and your training activity data) may be used or disclosed by IAC Safety Services for statistical, regulatory and research purposes.

Business Profiles

Exactly what we do i.e., each of our businesses, have been considered as they have a direct bearing on our APP obligations. Detailed below is a summary of the purpose of each business.

The **IAC Group Mission Statement** is to nurture our Separate Business Units, enabling them to successfully expand and achieve their missions and visions.

The **IAC Group Vision Statement** is to provide an effective and efficient operating platform to enable and support our suite of Separate Business Units in their missions to provide a range of products and services to the Electricity Supply Industry.

IAC Safety Services is a Registered Training Organisation (RTO) and is regulated by the Australian Skills Quality Authority (ASQA) which requires, amongst other things that RTOs collect, hold, use and disclose a wide range of personal and sensitive information on students and customers that have enrolled in nationally recognised training courses.

Supply Workforce has arrangements with individuals under which the business:

- Supplies individuals to perform work in and as part of a host's business or undertaking and the provider is obliged to pay the individual for performance of the work.
- In the course of providing recruitment or placement services, recruits individuals for, or places the individuals with a host who has to pay the individuals to perform work in and as part of the host's business or undertaking and the provider procures or provides accommodation for the individuals for some or all of the period that they are working with the host.
- In the course of conducting contractor management services, recruits the individuals as independent contractors to perform work in and as part of a host's business or undertaking and manages the contract performance for the independent contractors.

ASP Assist is an online retail outlet that supplies goods and services to Accredited Service Providers (ASP). These service(s) assist the ASP to achieve and maintain Accreditation and Authorisation status therefore granting them the authority to perform their duties.

ASP Assist services are regulated by the Australian Competition and Consumer Commission (ACCC).

APP Privacy Policy


IAC Group

Policy Statement

Our APP Privacy Policy

The IAC Group is committed to managing the WHS risks associated with our decisions, activities and operations. It is recognised that the health and safety of all workers, visitors and students is of the utmost importance and vital to the success of our business. As such we aim to continuously improve health and safety in the workplace through consultation and increased health and safety awareness of all stakeholders.

We intend to achieve our commitment by complying with all relevant legislative requirements as a minimum standard to which we will operate.

To assist in achieving the highest level of compliance with this policy statement the following responsibilities are allocated:

- Executive responsibility is assigned to the Managing Director. This manager is responsible for the design, establishment, implementation, maintenance and review of the overall risk management function in consultation with all relevant parties. In addition, this manager shall be responsible for ensuring that all policies, procedures, practices, rules and the like are constant with all other management functions.
- Officers and workers at all levels are responsible for the implementation, maintenance and review of the WHS management policies, procedures, practices, rules and the like.
- Stakeholers, students and visitors shall be made aware of our commitment. In addition, they shall be expected to comply with the relevant WHS management policies, procedures, practices, rules and the like.

The IAC Group "We" respects the privacy of those who purchase our products and services.

We are required to collect, use, store and disclose a range of personal information on students, employees and a range of other stakeholders.

We are committed to maintaining the privacy and confidentiality of all student, client and personnel records.

We will comply with all privacy legislative requirements which include the Commonwealth Privacy Act 1988 and the 13 Australian Privacy Principles (APPs) as outlined in the Commonwealth Privacy Amendment (Enhancing Privacy Protection) Act 2012.

Our policy is to take reasonable steps to make students / individuals aware that it is collecting personnel information about them, the purpose for which it is collecting the information, and who, (if applicable), we might pass the information on to.

David Conyngham Managing Director

Version 1, January 2021

This policy is intended to explain clearly and in plain language some of the key processes and procedures that we have implemented to manage your personal information, to protect your privacy and to comply with the Privacy Act 1988 (Cth), and the 13 Australian Privacy Principles (APPs) as outlined in the Commonwealth Privacy Amendment (Enhancing Privacy Protection) Act 2012. Specifically:

- ✔ the kinds of personal information that we collect and hold;
- ✔ how we collect and hold personal information;
- ✔ the purposes for which we collect, hold, use and disclose personal information;
- ✔ how an individual may access personal information about the individual that is held by us and seek the correction of such information;
- ✔ how an individual may complain about a breach of the Australian Privacy Principles, and how we will deal with such a complaint;
- ✔ whether we are likely to disclose personal information to overseas recipients;
- ✔ if we are likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

This policy gives a broad overview of our policies in relation to privacy but if you require further information, you are welcome to contact us or to read any of the privacy statements or notices that will be issued to you as and when personal information is collected.

You must read this privacy policy before providing us with any personal information or using the website. By providing us with your personal information and using the website, you are confirming your agreement to the policies and procedures described in this privacy policy.

By agreeing to accept the terms of this privacy policy, or by providing your personal information to us, or both, you are taken to have expressly consented to the collection, storage, use and disclosure of your personal information for each of the purposes and to all of the parties outlined in this privacy policy.

Availability

Our Privacy Policy and Procedure is available free of charge, and published on our website, including our student handbook (Student Kit), staff handbook, trainer handbook and operations manual.

Privacy Program

What sorts of personal information do we collect?

We will only collect from you information that is necessary and relevant to our relationship with you. For example, employment with us, when undertaking nationally recognised training, to identify you, contact you, and to confirm your identity.

There is no obligation for you to provide us with any of your personal information but if you choose not to provide us with your personal information, we may not be able to provide the information, goods or services that you require.

There are consequences where some personal information is not collected such as failure to provide your Unique Student identifier (USI) or an exemption from it, will mean that we cannot issue you with a Statement of Attainment or Certificate at the successful completion of a course.

Where possible, we ensure that the individual confirms their understanding of these details.

It would be very unusual for us to need to collect all or even most of the information tabled below from you, however, the information we require depends on the specific service that we provide to you. We will only collect personal information from you that we reasonably require in order to satisfactorily provide the products and services that you require from us.

Personal Information we may collect and hold:

Your name	your address	your date of birth
your telephone number(s)	your e-mail address	Employment details
your user name and password	Copies of licences	Tax File Number
Course progress and achievement information	CV, resume or application related behaviour	qualifications, memberships and other accreditations
Educational background	Demographic Information	Employee record information
Financial billing information	Unique Student Identifier (USI)	Transaction information
payment information/bank account and credit or debit card details	online interactions with our website, publications, alerts and social media activity	Information/personal preferences on how you use our products and services
identification documents (such as driving licences) and, in some specific cases, where we require these to verify your identity	Advice received from the client or prospective client that may contain additional personal information, such as family relationships and other business-related connections	your Internet Protocol (“IP”) address, server address, domain name and information on your browsing activity when visiting one of our websites
Company name	business/mailing address	

Notes: Information about companies is not personal information. However, the principles will apply to an individual who is carrying on a business as a sole trader.

Sensitive information

The Act places restrictions on us collecting sensitive information about you. Sensitive information is a subset of personal information. It means information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political organisation, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, criminal record, health information about an individual, genetic information, biometric information that is to be used for the purpose of automated biometric verification or biometric identification or biometric templates.

Our policy is not to collect sensitive information, however that may not always be possible, i.e. when required by law to do so. If you elect to provide us with any sensitive personal information, we will take all reasonable steps to ensure that the sensitive information is securely protected.

In the event we propose to use such personal information other than for the reasons set out in this policy, we will first take all reasonable steps, unless unlawful for us to do so, to notify you or seek your consent prior to such use.

Sensitive Information we may collect and hold:

- Identity details: full legal name, date of birth
- Employee details & HR information including tax file number, superannuation details
- Complaint or issue information
- Disability status & other individual needs
- Language, literacy and numeracy levels
- Indigenous status
- Concession status
- Details on your next of kin or parent/guardian
- Background checks (such as National Criminal Checks or Working with Children checks)

2APP. Anonymity and pseudonymity

When can you deal with us anonymously?

Generally, you can deal with us anonymously (i.e. without identifying yourself). Individuals have the option to use a pseudonym or not to identify themselves when dealing with us, this can apply when requesting information on purchasing goods and services, employment, a course, website enquiries, anonymous complaints/feedback or other situations in which an individuals' information is not required to complete a request.

This includes using generic email addresses/usernames that do not contain an individual's actual name when individuals may access a public component of our website or enquiry forms.

We only store and link pseudonyms to individual personal information in cases where this is required for service delivery (such as system login information) or once the individual's consent has been received.

Circumstances requiring identification

In certain circumstances we will ask you to provide personal information as it is required by law to do so, or because it would be impracticable to deal with you anonymously. These circumstances include but are not limited to employment related issues, where you order goods and services online, where goods and services need to be delivered, where you enter one of our competitions, when you submit a request, enquiry, or complaint.

It is a condition of registration for our RTO under the National Vocational Education and Training Regulator Act 2011 that we identify individuals and their specific individual needs on commencement of service delivery, and collect and disclose Australian Vocational Education and Training Management of Information Statistical Standard (AVETMISS) data on all individuals enrolled in nationally recognised training programs.

Part 2 — Collection of personal information (APPs 3, 4 and 5)

Consideration » **Collection** » Deal with » Integrity » Access to, and correction of personal information

3APP. Collection of solicited personal information

We will collect information you provide that is reasonably necessary for our business activities.

We may collect personal information in a number of ways, (either online, face-to-face or over the phone) depending on the nature of the product or service that we are providing to you. These include but are not limited to:

- when you complete an enrolment form for a nationally accredited course;
- when you apply for employment with us;
- when you set up an account with us;
- when you obtain a quote or order/purchase products and services from us;
- when you subscribe to our catalogue or mailing lists;
- when you enter competitions or promotions that we may run;
- when you provide us your details for customer care purposes;
- when you browse or submit an enquiry using one of our websites;
- when you complete surveys or provide online feedback or product reviews;
- when you publicly comment about us on social media sites; and/or
- when you register or attend an event.

Primarily we will collect via the use of web-based systems (such as online enquiry forms, online enrolment form, web portals or internal operating systems). However, a paper based system does still exist to manage situations where electronic, web-based system are not available or appropriate for any reason.

Generally, we will collect your personal information directly from you. However, we also hold information, collected incidentally, concerning individuals who work for companies or organisations that have a business relationship within the IAC Group, ie prospective clients, associates of clients, our suppliers or potential suppliers, our employees or potential employees, or which is otherwise available in the public domain.

Your personal information will not be collected if you are only browsing our website but we may use cookies to better tailor our information and our products and services to meet your needs.

We may from time to time collect personal information from alternative sources, such as when you apply for a job with us. We may collect personal information about you from any third parties that you nominate as your referees in your application; and/or when we collect personal information about you from publicly available sources including but not limited to, court judgments, directorship and bankruptcy searches, Australia Post, and social media platforms.

We sometimes collect information from your employer, or other organisations where you may engage in placement for training and assessment services.

If we collect details about you from someone else, we will whenever reasonably possible, make you aware that we have done this and why, unless otherwise required or authorised by law.

In cases where we collect personal information on behalf of other parties the documentation that you sign will set out how the personal information that you provide will be used by these third parties and the privacy policies of the third parties will apply. We may also receive personal information or documents about you from these third parties where necessary in connection with the provision of goods or services by us.

Where a person represents and warrants to us that they provide personal information to us about another person:

- ✔ they are authorised to provide that information to us;
- ✔ they have obtained the express consent of the individual to disclose their personal information to us for its relevant use, including for use in our business and to provide our services;
- ✔ they have complied with the APPs in collecting that personal information, including by making all relevant notifications required under APP 5; and
- ✔ they have informed that person about the contents of this privacy policy including who we are, how we use and disclose personal information, and that they can gain access to, and correct, that information.

4APP. Dealing with unsolicited personal information

Although highly unlikely, from time to time we may receive personal information about you that we have not requested or taken steps to come to know (unsolicited information). In the event we collect personal information from you, or a third party, in circumstances where we have not requested or solicited that information, and it is determined by us (in our absolute discretion) that the personal information is not required, we will destroy the information in a safe and secure manner, or ensure that the information is de-identified (unless it would be unlawful to do so).

In the event that the unsolicited personal information collected is in relation to potential future employment with us, such as your CV, resume or candidacy related information, and it is determined by us (in our absolute discretion) that we may consider you for potential future employment, we may keep the personal information on our human resource records.

5APP. Notification of the collection of personal information

When information is collected, including that from third parties, we take all reasonable steps to notify the individual of the details of the information collected or otherwise ensure that the person is aware of those matters. This notification is scheduled to occur at or before the time of personal data collection, or as soon as practicable via our websites.

Our notifications to individuals on data collection include:

- ✔ our details, including our contact details;
- ✔ that we are collecting your information and the reasons why we are collecting your information;
- ✔ if the collection is required or authorised by law, the details of the law, court or tribunal order, along with the possible cosequences of not disclosing your information.
- ✔ the facts and circumstances of collection such as the date, time, place and method of collection, and whether the information was collected from a third party, including the name of that party and other organisations or persons to which the information is usually disclosed, including naming those parties;
- ✔ Where we collect personal information from another organisation, we will confirm whether the other organisation has provided the relevant notice above to the individual; or whether the individual was otherwise aware of these details at the time of collection; and if this has not occurred, we will undertake this notice to ensure the individual is fully informed of the information collection

By agreeing to accept the terms of this privacy policy or by providing your personal information to us, or both, you are taken to have consented to the use and disclosure of your personal information for the above purposes.

We will not use your personal information for any other purpose without your consent or where we do use your information for another purpose, it will either be for a purpose which we believe is related to the purpose for which you first provided us with the information or for a purpose which you would expect.

Part 3 — Dealing with personal information (APPs 6, 7, 8 and 9)

6APP. Use or disclosure of personal information

Use your personal information?

We will use personal information about an individual for the "primary purpose" of collection (i.e. the dominant or fundamental purpose for which that information is collected), purpose such as, but not limited to:

- facilitating our internal business processes;
- communicating with clients, prospective clients and other external parties;
- to contact you in relation to an event, special offer or product you may be interested in;
- to assist us to run our business and to develop and improve our products, services and performance, including staff training, accounting, risk management, record keeping, archiving, systems development and testing, developing new products and services and undertaking planning, research and statistical analysis;
- the operation and administration of accounts or subscriptions that you have with us (including certain features of our accounts or subscriptions through which other users can view certain information about you, unless you opt out of these features);
- to consider your request for a product or service;
- to enable us to provide a product or a service to you, process your orders, including delivery, payments and collecting debts;
- to provide information to you that you have regarding requests, enquiries, advice, complaints, consumer guarantee or warranty claims, and other customer care related activities;
- to facilitate your entry into competitions run through the website;
- to facilitate online chat;
- to our third party service providers to assist us in providing and improving our services to you, and to analyse trends in sales and better understand your needs or to develop, improve and market our products and services to you;
- for regulatory reporting and compliance with our legal obligations, governmental or regulatory requirement that we have to comply with, or in connection with legal proceedings, crime or fraud prevention, detection or prosecution;
- to facilitate product and service reviews and to seek your feedback in relation to particular products or services, customer satisfaction and our relationship with you and to manage any customer complaints;
- for use in direct marketing of promotions, products and services, including to add to a database compiled by us for this purpose;

- to monitor or improve the quality and standard of service that we provide to you;
- to manage employees and human relations
- we may use the information provided to remind you of licence expiration, upcoming events and marketing of products and services offered by the group.
- to market our products and services and provide advice on our products;
- to carry out certain checks (for example, for our fraud or theft prevention processes, if you wish to open an account with us, obtain credit from us or pick-up goods in-store that have been ordered online);
- when interacting with companies or organisations with whom we have a business relationship (where you work for, or otherwise represent, such an organisation);
- for purposes relating to any third party acquisition or potential acquisition of an interest in our assets, to our agents, successors and/or assigns;
- when complying with our obligations under agreements with third parties; and
- information is also collected and used to enable compliance with Electricity Supply Industry Network Access Issues and WHS compliance obligations in relation to the services we supply.

Job applications

If you apply for a job with us, you will be required to provide us with certain personal information in relation to your job application. We will hold, use and disclose that information solely for the purpose of considering your application. In particular, in considering your application, it may be necessary for us to disclose some of that information to third parties to verify the accuracy of that information. In considering your application, we may also collect personal information about you from any third parties that you nominate as your referees in your application.

Disclosure Obligations

We may also use or disclose your personal information and in doing so we are not required to seek your additional consent:

- when it is disclosed or used for a purpose related to the primary purposes of collection detailed above and you would reasonably expect your personal information to be used or disclosed for such a purpose;
- if we reasonably believe that the use or disclosure is necessary to lessen or prevent a serious or imminent threat to an individual's life, health or safety or to lessen or prevent a threat to public health or safety;
- if we have reason to suspect that unlawful activity has been, or is being, engaged in; or
- if it is required or authorised by law.

Stakeholders are advised that legal obligations exist that may require the disclose of certain information to a range of entities, including but not limited to: Governments (Commonwealth, State or Local); Employers (and their representatives), Parents and Guardians, including:

- Standards for Registered Training Organisations (RTOs) 2015
- Data Provision Requirements 2012
- AVETMISS standards
- Fairwork Commission
- Other entities required by law and in accordance with the Privacy Act 1988.
- WHS Workers compensation laws
- Labour hire industry laws
- Consumer Safety Act
- Student Identifiers Regulation 2014
- National VET Data Policy – November 2017
- Registering bodies such as the ASQA, NSW dept Trade & Investment
- Government funding bodies in each state and territory and/or Commonwealth Government
- Apprenticeship Centres
- Electricity Supply Distribution Network Operators
- superannuation details to a fund administrator;
- Tax File Number Declaration to the Australian Taxation Office;
- court orders, subpoenas or other legislation that requires us to provide personal information (for example, a garnishee order).

We may disclose your personal information for these purposes to third parties, including:

- School – if you are a secondary student undertaking VET, including a school-based apprenticeship or traineeship;
- Employer – if you are enrolled in training paid by your employer;
- Commonwealth and State or Territory government departments and authorised agencies;
- NCVER;
- Organisations conducting student surveys; and
- Researchers

Personal information disclosed to NCVER may be used or disclosed for the following purposes:

- Issuing statements of attainment or qualification, and populating authenticated VET transcripts;
- Facilitating statistics and research relating to education, including surveys;
- Understanding how the VET market operates, for policy, workforce planning and consumer information; and
- Administering VET, including programme administration, regulation, monitoring and evaluation

You may receive an NCVER student survey which may be administered by an NCVER employee, agent or third party contractor. You may opt out of the survey at the time of being contacted. NCVER will collect, hold, use and disclose your personal information in accordance with the Privacy Act 1988 (Cth), the VET Data Policy and all NCVER policies and protocols (including those published on NCVER's website at www.ncver.edu.au).

Where we use or disclose personal information in accordance with an enforcement-related activity we will make a written note of the use or disclosure, including the following details:

- The date of the use or disclosure;
- Details of the personal information that was used or disclosed;
- The enforcement body conducting the enforcement related activity;
- If the organisation used the information, how the information was used by the organisation;
- The basis for our reasonable belief that we were required to disclose the information.

Secondary use or disclose use of personal information may occur for purposes in cases where:

- An individual consented to a secondary use or disclosure;
- An individual would reasonably expect the secondary use or disclosure, and that is directly related to the primary purpose of collection; or
- Using or disclosing the information is required or authorised by law.

We may share your personal information within the IAC Group. By agreeing to accept the terms of this privacy policy or by providing your personal information to us, or both, you consent to your personal information being shared within the IAC Group.

We deal with third party service providers who may assist us with a variety of functions including with research, mail and delivery, security, insurance, professional advisory (including legal, accounting and auditing advice), banking, payment processing, facilitating credit arrangements, credit reporting, fraud checks, data storage, information processing, order tracking, marketing, product reviews, online competitions, responding to customer queries, complaints or technology services, customer support, administration, archival, hosting, research, installation, distribution, logistics, debt collection, and the operation of our services and other websites.

By agreeing to accept the terms of this privacy policy or by providing your personal information to us, or both, you are taken to have consented to us disclosing your personal information to our third party service providers.

Should it be necessary for us to forward personal information to third parties, we will make every effort to ensure that the confidentiality of the information is protected. Wherever possible, we will limit the information provided to independent third parties to that information required for those third parties to properly perform their functions.

In some cases these service providers may collect your personal information on our behalf.

7APP. Direct marketing

We do not use or disclose the personal information that we hold about an individual for the purpose of direct marketing, unless:

- The personal information has been collected directly from an individual, and the individual would reasonably expect their personal information to be used for the purpose of direct marketing; or

- The personal information has been collected from a third party, or from the individual directly, but the individual does not have a reasonable expectation that their personal information will be used for the purpose of direct marketing; and
- We provide a simple method for the individual to request not to receive direct marketing communications ('opting out').

On each of our direct marketing communications, we provide a prominent statement that the individual may request to 'opt out' of future communications, and how to do so. An individual may also request us at any stage not to use or disclose their personal information for the purpose of direct marketing, or to facilitate direct marketing by other organisations. If you are a subscriber to our marketing database you can also update your details via the "unsubscribe" option in one of the emails that you receive from us.

We will comply with any request promptly and undertake any required actions for free.

APP 8

We are not likely to disclose the personal information that we collect and hold about you to third parties who are not in Australia. However, there may be circumstances where we need to disclose personal information that we hold about you to a third party overseas ("Overseas Recipients"). This may occur, for example, where we have a database or server hosted outside Australia or where you are interacting with an application which is based overseas.

Prior to us disclosing your personal information to an Overseas Recipient, we have an obligation under APP 8.1 to take reasonable steps to ensure that the Overseas Recipient does not breach the APPs in relation to your personal information, as well as an obligation under APP 6 to only disclose your personal information to an Overseas Recipient for the primary purpose for which that personal information was collected (unless an exception applies under APP 6) (the "Overseas Disclosure Obligations").

We will take all reasonable steps to satisfy our Overseas Disclosure Obligations. The countries to which we are most likely to send your personal information include the United States of America, India and the United Kingdom.

9APP. Adoption, use or disclosure of government related identifiers

We are restricted regarding how we are permitted to handle government related identifiers, irrespective of whether a particular identifier is the personal information of an individual. An identifier will be personal information if the individual is identifiable or reasonably identifiable from the identifier, including from other information held by, or available to, the entity that holds the identifier. If it is personal information, the identifier must be handled by the entity in accordance with other APPs.

We generally do not adopt, use or disclose a government related identifier related to an individual except:

- In situations required by Australian law or other legal requirements eg, TFN;
- Where reasonably necessary to verify the identity of the individual eg, USI;
- Where reasonably necessary to fulfil obligations to an Agency or a State or Territory authority; or
- As prescribed by regulations.

Part 4 — Integrity of personal information (APPs 10 and 11)

10APP. Quality of personal information

We take reasonable steps to ensure that the personal information we collect is accurate, up-to-date and complete. We also take reasonable steps to ensure that the personal information we use or disclose is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant. Quality measures in place supporting these requirements include:

- Internal practices, procedures and systems to audit, monitor, identify and correct poor quality personal information (including training staff in these practices, procedures and systems);
- Protocols that ensure personal information is collected and recorded in a consistent format, from a primary information source when possible;
- Ensuring updated or new personal information is promptly added to relevant existing records;
- Providing individuals with a simple means to review and update their information on an on-going basis through our online portal;
- Reminding individuals to update their personal information at critical service delivery points (such as completion) when we engage with the individual;
- Contacting individuals to verify the quality of personal information where appropriate when it is about to be used or disclosed, particularly if there has been a lengthy period since collection; and
- Checking that a third party, from which personal information is collected, has implemented appropriate data quality practices, procedures and systems.

11APP. Security of personal information

Once we collect your personal information, we will either hold it securely and store it on infrastructure owned or controlled by us or with a third party service provider who have taken reasonable steps to ensure they comply with the Privacy Act.

We may need to maintain records for a significant period of time. However, when we consider information is no longer needed, we and our third party service providers take all necessary

steps to destroy or permanently de-identify your personal information where it is no longer required and to protect your personal information from loss, misuse and interference and from unauthorised access, modification or disclosure.

We hold personal information in a number of ways, including:

- as part of customer records and other electronic documents on which personal information is contained which are stored on our information technology systems and servers operated by third parties who provide services to us in connection with our business; and
- by securely storing hard copy documents on which personal information is contained, at our various premises and using third party document management and archiving services.

We have implemented appropriate processes and techniques (including physical security such as locks and security systems and computer and network security, including firewalls and passwords) to protect personal information from loss, misuse and interference and from unauthorised access, modification or disclosure. In addition, access to your personal information is limited to those who specifically need it to conduct their duties.

While care is taken to protect your personal information on our websites, unfortunately no data transmission over the Internet is guaranteed as 100% secure. Accordingly, we cannot ensure or warrant the security of any information you send to us or receive from us online. This is particularly true for information you send to us via email as we have no way of protecting that information until it reaches us. Once we receive your personal information, we are required to protect it in accordance with the Act.

We ensure the robust storage and security measures at all times. Information on collection is as soon as practical, converted to electronic means, stored in secure, password-protected systems, and monitored for appropriate authorised use at all times.

Destruction of paper based records occurs as soon as practicable in every matter, through the use of secure shredding and destruction services.

Staff are trained/informed on privacy issues, and how the checked and verified APPs apply to our practices, procedures and systems. All staff hold current National Police Checks.

We conduct an internal audit of the adequacy and currency of security and access practices, procedures and systems implemented.

Security of personal information

Confidential information must not be left unattended where non authorised persons, including internal staff, may gain access. Controls may include but are not limited to:

Access to our offices and work areas is limited to our personnel only - visitors to our premises must be authorised by relevant personnel and are accompanied at all times.

With regard to any information in a paper based form, we maintain storage of records in an appropriately secure place to which only authorised individuals have access.

Paper Files

- Close all folders, binders; and / or remove confidential information from the desk.
- Filing cabinets and archive facilities are to be locked when the office is unattended.
- Restricted access to authorised staff.
- Redundant personal and sensitive information will be destroyed by Commercial document destruction.

Record Control Outside of Office

Prior to any confidential information being taken off premises, it must be verified that it is really necessary for this to occur. In any case, confidential information must not be left attended where others may gain access. At all times ensure the security of the confidential information, for example whilst in vehicles, hotel rooms, family home, training facilities etc.

Training and Assessment

Staff must not share personal information with anyone outside of the IAC Group. Personal information should not be left unattended where others may have access to the materials. For example, staff must:

- Close all folders, binders; and / or remove personal information from the desk.
- When leaving the training room during a break period or leaving the classroom unattended, lock all personal information including that of the learner in a secure cabinet, or take materials with them in a secure manner.
- Trainers/assessors are to personally collect personal information from the learner. Learners are not to pass from learner to learner the collected personal information.
- Trainers/assessors are not to publicly and verbally collect or confirm personal information.
- The same controls apply to both computer and paper files and they must be followed.
- Upon collection of completed learner materials, trainers/assessors are to immediately send the materials to PO Box head office, via secure post or hand delivery.
- Personal information must not be left unattended where others may gain access to the materials. At all times ensure the security of the personal information, for example whilst in vehicles, hotel rooms, family home, training facilities etc.

Electronic Files

Only authorised personnel are provided with login information to each system, with system access limited to only those relevant to their specific role.

Our systems are hosted in secure cloud-based environments, with robust internal security to server systems access.

Virus protection, backup procedures and ongoing access monitoring procedures are in place.

- Individual information held across systems is linked through an allocated identification number for each individual.
- Programs must be turned off or logged out, automatic time out settings applied, password protect screensavers and password protected access.

- Computer screens viewable in areas where the public, visitors or non personnel may gain access, where practicable, be turned away so they are difficult to read.
- Each staff member is issued a unique access password in accordance with our IT Configuration Specification Plan – Security Configurations.
- Redundant personal and sensitive information will be deactivated/deleted.

We leverage many of the controls provided by Microsoft, as well as industry standards for the protection and privacy of data in its systems. Controls currently include:

Multifactor Authentication is a core component of our Identity Access Management (IAM) policy and has been enabled on privileged accounts.

Note: Not all admin / privileged accounts have this enabled yet. Recommended: Legacy authentication methods have been blocked using policy to restrict compromising sign-in attempts from legacy authentication (the most common route for compromise).

Due to the transient nature of students interaction with us, MFA is not currently an appropriate control for student accounts. Work is in progress to automatically disable these accounts when not required, and re-enable when required again.

Administration accounts with elevated access are separated from general user accounts and where feasible apply the principle of separation of duties. This includes the use of Service Accounts for underlying system processes.

Access to systems & data is managed through Active Directory Groups. Principle data repositories such as SharePoint and One Drive utilise these groups for access control.

External sharing for OneDrive and SharePoint has been disabled. Only authenticated users of the system can share and view files. With regard to email & file protection, we are implementing:

- Zero day malware protection is active for email messages and files in SharePoint, OneDrive and Microsoft Teams;
- Zero day anti-phishing protection is active for impersonation and spear phishing threats; and
- Safe Link protection is active so that malicious links are blocked across inbound and intra-org messages using Safe Links time of click protection.

Data loss prevention (DLP) policies are being evaluated to help identify and protect IAC Group sensitive information. For example, setting policies to help make sure information in email and docs isn't shared with the wrong people.

Information governance tools are being evaluated to classify our content and set appropriate retention periods to help manage the full content lifecycle, from importing and storing data at the beginning, to retaining and then deleting it at the end.

These policies will assist in pre-empting GDPR style compliance.

Default Microsoft alerting is currently in place. New alerting is being considered based on key events that need to be monitored.

The Microsoft Secure Score is regularly monitored for identified vulnerabilities & rectified as appropriate. Audit logs are also monitored.

Data Breach

A data breach involves the loss of, unauthorised access to, or unauthorised disclosure of personal information. This plan sets out the procedures and processes to be followed in the event the entity experiences an actual or suspected data breach.

We have necessary preparations to be able to respond to any privacy data breach. Where unauthorised access or disclosure is detected, or information has been lost in circumstances where unauthorised access is possible, we will promptly activate its Data Breach Response Plan.

Our Data Breach Response Team is responsible for ensuring the plan is followed and for assessing and managing any breach and will determine whether the incident is an eligible data breach under the Notifiable Data Breach (NDB) scheme. The Data Breach Response Team is also responsible for delivering any notifications that may be required in a timely manner.

We take all reasonable steps to limit the consequences of a data breach and to preserve and build public trust in our management of personal information.

Where a breach has occurred or is suspected to have occurred, the person who has become aware of this must notify a member of the Data Breach Response Team as soon as is reasonably practicable, however, an obligation exists to ensure that this occurs prior to the completion of their shift. The notification must include all known details of the breach or suspected breach, and be recorded on the Data Breach Process Form, which includes:

a) date and time of the breach (if known);

b) description of the personal information involved;

c) if known, the cause of the breach; otherwise, an explanation of how the breach was discovered;

d) which systems (if any) have been affected;

e) which business or businesses are involved;

f) any corrective actions that have already been taken.

On receipt of the above notification, the Data Breach Response Team must determine whether or not a privacy data breach has or is likely to have occurred and assess the potential harm.

The Data Breach Response Team must take all necessary steps to manage any data breach as appropriate to the specific instance. The particular course of action will depend on the nature of the breach, but these are the key steps that may be taken.

- Immediately contain the breach (if this hasn't already been done).
- Engage an independent expert in cyber security, if relevant.
- Determine if a Notifiable Data Breach (NDB) has occurred. Under the NDB scheme, an eligible data breach is one that meets the following three criteria:

- there is unauthorised access, unauthorised disclosure or loss of personal information; and
- from the perspective of a reasonable person, serious physical, psychological, emotional, financial or reputational harm to an individual whose information is involved in the breach is likely (more probable than not); and
- it has not been possible to prevent the likely risk of serious harm with the remedial actions taken.

- If required, ensure notification of the incident to the affected parties and contact the Office of the Australian Information Commissioner as soon as possible using the NDB Statement form.
- Record any instructions issued, the actions that have been taken and any recommendations made in Section 3 of the Data Breach Process Form.
- Consider developing a communication strategy with method, content and timing of any announcements to staff, students or media.
- Identify actions to reduce the likelihood of recurrence and ensure their implementation.
- Consider conducting an audit to ensure that any changes in systems or processes have been properly implemented and are effective.
- Consider whether any changes to this plan are needed.

Part 5 — Access to, and correction of, personal information (APPs 12 and 13).

Consideration » Collection » Deal with » Integrity » **Access to, and correction of personal information**

12APP. Access to personal information

Usually we will be able to provide you with access to your personal information upon receipt of your written request. There are some limited circumstances in which we may not be able to provide you with access to your personal information when requested. Such circumstances might include where access would pose a serious threat to the life, health or safety of another person or where such access would unreasonably impact on the privacy of others.

No personal information will be released unless it was requested by an approved entity, or due to an enforcement related activity or in an emergency situation; and only after correct Privacy Policy and Procedures were followed, specifically the requestor or by another person who is authorised to make a request on their behalf, had proven a valid reason for requiring the personal information, had proven their identity and their details were confirmed prior to personal information release to ensure correct and safe delivery.

Where you request access to your personal information, we will respond to any such request within a reasonable period (usually within 14 days) after the request is made and if possible, we will provide you with access to your information in the manner requested by you, if specified (usually within 30 days). In any event, we will take all reasonable steps to give you access to your information in a way that meets your needs.

If you would prefer to submit a privacy request using a pseudonym or otherwise keep your identity secret, we will do its best to support that request if it is feasible to do so under the circumstances.

If we deny you access to your personal information for any reason, or if we are unable to provide you with access to your information in the manner requested by you, then we will provide you with a written notice confirming:

(a) the reason for such refusal; and

(b) the procedure to complain about the refusal.

We may recover from you our reasonable costs of supplying you with access to your personal information but we will not charge you for any request to access your information.

13APP. Correction of personal information

Under the Australian Privacy Principles, you have the right to request access to any personal information that we may hold about you and to advise us if the information should be corrected. The Australian Privacy Principles set out the circumstances when we can refuse those requests. If we do refuse your request, we will provide you with a written notice that sets out the reasons (unless it would be unreasonable to provide them to you), and the complaint mechanisms available to the individual, upon request by the individual whose correction request has been refused, take reasonable steps to associate a statement with the personal information that the individual believes it to be inaccurate, out-of-date, incomplete, irrelevant or misleading, and respond usually within 14 calendar days to these requests.

Subject to our right to refuse access, we will provide you with a report that lists any personal information that we may hold about you.

We take reasonable steps to correct personal information we hold, to ensure it is accurate, up-to-date, complete, relevant and not misleading, having regard to the purpose for which it is held.

You may request us to correct the personal information that we hold about you. If you do so and we are satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, we will take such steps as are reasonable in the circumstances to correct your personal information to ensure that, having regarding to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.

If you subscribe to one of our services you can also update your details via that service.

If we correct any of your personal information and that information has previously been disclosed to another entity that is required to comply with the APPs, then, upon your request to do so, we will take reasonable steps to notify that other entity of the correction unless such notification is impracticable or unlawful.

We will not charge you for any request to correct your personal information, nor will we pass on to you any costs incurred by us in correcting your personal information or for associating a statement with your personal information.

As the accuracy of personal information largely depends on the information that you provide to us, we request that you advise us of any errors in or updates required to your personal information. If you believe that the information we hold about you is inaccurate or out of date, you may contact us and we will update the relevant information accordingly.

In order to request access to personal records, individuals are to make contact with:

Felicity Manarin felicity@iac.edu.au 1300 887 317

A number of third parties, other than the individual, may request access to an individual's personal information. Such third parties may include employers, parents or guardians, schools, Governments and other stakeholders. In all cases where access is requested, we will ensure that:

- Parties requesting access to personal information are robustly identified and vetted;
- Where legally possible, the individual to whom the information relates will be contacted to confirm consent (if consent not previously provided for the matter); and
- Only appropriately authorised parties, for valid purposes, will be provided access to the information.

Correcting at our initiative

We will take all reasonable steps to correct personal information in cases where we are satisfied that the personal information held is inaccurate, out-of-date, incomplete, irrelevant or misleading. This awareness may occur through collection of updated information, in notification from third parties or through other means.

Complaints about a breach of the APPs or a binding registered APP code

We are committed to maintaining and protecting your privacy but it is possible that in limited circumstances, mistakes might be made. If you are concerned with the way your personal information has been handled then you are entitled to make a complaint. If you would like to lodge a complaint, please contact us through our Privacy Compliance Officer, whose details are set out below. In order to resolve a complaint, we:

- will liaise with you to identify and define the nature and cause of the complaint;
- may request that you provide the details of the complaint in writing;
- will keep you informed of the likely time within which we will respond to your complaint; and
- will inform you of the legislative basis (if any) of our decision in resolving the complaint.

- conduct internal discussions with the relevant business units which are the subject of your complaint, and evaluate whether we believe that breach of Division 3 of Part IIIA of the Privacy Act 1988 (Cth) or the registered Credit Reporting Privacy Code; and
- notify you of the results of our investigation of your complaint.

If the conclusion of our investigation is that our collection, holding, use or disclosure of your Application Documentation Information was in breach, we will take steps to remedy the breach as soon as reasonably practicable.

We will endeavour to notify you of the results of our investigation of your complaint (usually within 30 days of receiving your complaint). However, if your complaint involves complex matters or requires extensive investigation and consultation, it may not be possible to respond within this timeframe. In these circumstances, we will seek your agreement to a longer period for us to respond to your complaint.

If you are not satisfied with our response to your complaint you are entitled under Part V of the Privacy Act 1988 (Cth) to make a complaint to the Office of the Australian Information Commissioner. Information about how to make a complaint is available from the Office of the Australian Information Commissioner's website (www.oaic.gov.au).

4. BREACHES OF PROGRAM

Any breach of this Policy will be considered serious and may result in disciplinary action up to and including summary dismissal.

5. CHANGES TO PROGRAM

The Company reserves the right to amend this Policy from time to time in accordance with legislative changes and business requirements. Employees will be informed of any changes that are made.