AICIP TERMS AND CONDITIONS

1. Collection: When you access this site, AICIP collects information relating to your visit including personal information as defined by the Privacy Act in Australia. When you submit any Visitor Data to us, your submission is an acknowledgment of your agreement with the terms of our policy on privacy as set out in these Terms.
Purpose of collection: Any Visitor Data of a personal or sensitive nature that is collected from this site by AICIP will only be used as necessary for the business to be transacted between us and for the purposes of providing our Members with better services.

2. Disclosure & use: We will not sell or transfer your information to a third party for marketing purposes without your consent. Sometimes we need to share information with recognised authorities, regulatory bodies, governments and organisations such as banks to investigate possible fraud or other unlawful activities.
We will not disclose your personal information to anyone else for any other purpose unless we are required by law to disclose it or you tell us we can or should. Other information collected on site might be used by us to enable us to be proactive in assisting you in matters that either you or we have identified as relevant. We may also use the information to contact you and alert you to regulatory or compliance matters that might affect you. Emailed responses and additional or new information regarding the services of AICIP may be accessed on this site based on information we have collected from our Visitors. Much of the information can be collected automatically when a Visitor uses this site.

3. Access: AICIP's access to the Visitor Data is limited to authorised persons – employees and in some cases contractors and consultants who are all bound by contractual obligations to maintain the confidentiality (where applicable) and privacy of personal information in that data. Where there is a password or keyword provided to you to access this site or any secure part of it, then it is important to keep that password or keyword secret like an ATM PIN.
Subject to the rights of other visitors and persons whose information may be collected and aggregated with yours, you may request access to your personal information that we hold at any time and you may at any time request that AICIP to delete your personal Visitor Data held by us. We will take all reasonable steps to action that request promptly. However, there may be technical or other constraints to comprehensively identifying all such information and completely destroying all details of your visit and the information contained in your Visitor Data, as well as legal and statutory duties and responsibilities imposed on us that might also prevent us from destroying or removing from our records all such information. Nevertheless, your request will be treated, to the best of our ability given those constraints, as a signal that the information cannot be disclosed or used by us without your consent.
Given our commitment to your privacy, we can request verification from you and evidence to support such a request to ensure that the person who so requests that information is the person entitled at law to receive it.

5. Security: AICIP is continually assessing and updating its systems to ensure the security of information on the website as well as that retained on our independent systems. All reasonable efforts are made to provide an acceptable level of confidence that data cannot be used by unauthorised persons or in a manner likely to affect the reputation or standing of visitors or members. We cannot be responsible for events arising from unauthorised access to the information you provide.

6. External links: This web site may contain links to web sites of third parties ("external sites"). We are not required to maintain or update them and such links should not be construed as any endorsement,

approval, recommendation or preference by AICIP of the owners or operators of the external sites, or for any information, products or services referred to on the external sites unless expressly indicated on this web site. If you access another organisation's website using a link from our website, you will leave AICIP's website and will be subject to the terms, conditions and circumstances of the site you visit, including the level of privacy protection offered on that site. AICIP's policies and protections will no longer apply once you leave this site.
AICIP makes no warranties and accepts no liability in relation to material contained on external sites. Those sites will probably also have different privacy provisions. AICIP is not responsible for those sites or for any consequences of you accessing them through our website.

7. Communications between us: Where you have provided personal information to us by email, this electronic method will be used in preference to other methods of communication by us. You should indicate in your email if you prefer not to receive material in this manner.

8. Updating: If any of the personal information which you submit to us through the website, changes or becomes inaccurate, we ask that you notify us of the changes through the appropriate forms on the website or you can personally make the changes through your login..

9. Storage: Much of what is collected and stored is for our own use only. The sort of information we store might include personal information such as:

- Your organisation's legal name or business name.
- Your individual name and title or that of the individual who represents your organisation.
- Your email address of that individual and the organisation.
- The website address and the domain type of your organisation.
- The landline, mobile, postal and street addresses of you or the organisation.
- Information disclosed about yourself or your organisation in the enquiry or message submitted in the Visitor Data.
- The subject matter of an enquiry or message.
- Application information includes personal information; work history; ID number; past examination information.
- Inspector information may include personal information; work history; ID number; examination information.
- Examiner information may include personal information; ID number; past examiner activities.
- Invigilator information may include personal information; ID number; past invigilation activities.
- Examinations are stored for 12 months – complying with ISO 17024.

Cookies may be used to gather statistical information that will assist in understanding what users find interesting and useful on our Web site. No personal information can be identified about the user through cookies. However, they will enable you to take full advantage of the services we offer. The use of cookies is an industry standard and you'll find most major websites use them. Most Internet browsers are pre-set to accept cookies. If you prefer not to receive cookies, you can adjust your Internet browser to disable cookies or to warn you when cookies are being used. Alterations to these settings may, however, affect the functionality of our website.
A piece of code may also be embedded into pages of our website. This provides statistical site usage- AICIP uses Google Analytics and other web analytic tools from time to time to analyse usage statistics on our website. This analysis is performed using anonymous data collected from the AICIP website. No personally identifiable information is collected and we cannot link this anonymous statistical

data to any personal information you may have volunteered to AICIP for registration purposes or for any other requests.

AICIP REFUND POLICY

AICIP has a refund policy for cancellations.

Deferral of an ISI or SISI Application Fee: Deferral prior to 3 weeks before the examination date – Credited to the next examination round.
Deferrals of an ISI or SISI Application Fee: Deferral received less than 3 weeks before the examination date – attracts an Administration charge 10% 0f original fee.
Cancelation of an ISI or SISI Application that was deferred previously – 50% refundable

Cancellation of an ISI or SISI Application Fee: Cancellation prior to 4 weeks before the examination date - 80% refundable
Cancellation of an ISI or SISI Application Fees: Cancelled less than 4 weeks but greater than 1 week before the examination date - 50% refundable
Cancellation of an ISI or SISI Application Fees: Cancelled less than 1 weeks before the examination date - 30% refundable

AICIP DISCLAIMER

The Australian Institute for the Certification if Inspection Personnel (AICIP) provides the www.aicip.org.au web site as a service to candidates; invigilators; examiners; industry; regulators and the public.

AICIP is not responsible for, and expressly disclaims all liability for, damages of any kind arising out of use, reference to, or reliance on any information contained within the site. While the information contained within the site is periodically updated, no guarantee is given that the information provided in this web site is correct, complete, and up-to-date.

Links from AICIP to third-party sites do not constitute an endorsement by AICIP of the parties or their products and services. The appearance on the web site of information does not constitute an endorsement by AICIP, and information is based solely on material received from suppliers.

AICIP USE OF CERTIFICATE, LOGOS AND MARKS

You may use the AICIP logo on your business card; letterhead; email signature and/or website. However, any use of the AICIP logo or name must be carried out in accordance with the rules specified in this document and the AICIP style guide. The following restrictions apply to any use of the AICIP logo:

- AICIP logo may be used on business cards, company websites or signatures of Certified Inspectors. Any exemptions must be approved by AICIP in writing.

- The AICIP logo may NOT be used on badges, clothing, hats or any type of apparel, or physical displays.
- AICIP certification is NOT to be used in such a manner that may bring AICIP is disrepute, and not to make any statement regarding the certification that is deemed misleading or unauthorised by AICIP.
- AICIP logo shall NOT be used in any manner that violates federal, state or local law.
- The AICIP logo, identification card and certificate are NOT to be used in any misleading manner.
- If you are found to be suspended or your certification has been withdrawn you MUST discontinue the use of all claims or references to your AICIP certification and immediately return your certificate and identification card issued by AICIP.

If the above requirements are not met AICIP reserves the right to request those using AICIP's name, logo, or reference to AICIP in an unacceptable manner, to immediately desist and withdraw such documentation.

Where doubt exists on the use of the AICIP name, or logo, advice should be sought from AICIP before using.

Privacy Policy Statement - 2017

The Australian Institute of the Certification of Inspection Personnel (AICIP) is bound to the Australian Privacy Principles (APPs) and the conditions protecting your personal information as set out in the *Privacy Act 1988* and amended by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012.* This Privacy Policy Statement (PPS) provides only a snapshot of how AICIP implements and observes the APPs. References in this PPS to 'you' are references to the individual reading it or submitting personal information to us. References to AICIP include each of our related parties in context. The small citations next to the relevant paragraphs headed 'APP' refer to the APP in the amended Act.

Summary of Policy Principles

This summary sets out the basic tenets of our protection principles which we employ across our businesses. To assist in understanding how our Policy works for you, this summary includes both specific membership issues as well as those applicable to visitors to and users of our website; invigilators; examiners; candidates; regulators; and other stakeholders. In all cases, you should refer to the Privacy Policy 2017 for express terms and conditions.

The APPs

APP 1 - Open and transparent management of PI

Our Privacy Policy, meets the new requirements of the amending Act and provides some information on forecasted amendments for 2018.

APP 2 - Anonymity and pseudonymity

If you want to communicate with us on a particular matter you may ask to remain anonymous or use a pseudonym provided that if we are collecting your personal information like your real name because we:

- need to verify membership with AICIP and your authority to act;
- need it to properly provide whatever service or advice you are seeking from us and it is impracticable for us to do that using a pseudonym or anonymity;
- to verify or assist you with passwords or other security matters or other technical services; or
- we are required or authorised by law or a court or tribunal to identify you.

For our membership, we are contractually committed to protect your confidentiality and we implement a number of governance measures to help protect your privacy when dealing with us. For that reason, we need to know that the information or advice we provide is going to the right person. Accordingly, it will be only in isolated cases (e.g. when we are doing industry wide surveys) that your personal information can be obscured by anonymity or pseudonymity.

APP 3 - Collecting solicited PI

AICIP only collect the personal information that we need to do what you want us to do (subject to any lawful requirements that compel us to collect more).

We collect the personal information that is reasonably necessary for us to efficiently professionally and relevantly provide you with our services and to give you the ease of access and opportunities to use other services we may have available from time to time.

We will only collect your personal information directly from you.

In that case notifying us of the changes you require you can use the form provided or make the changes through your login.

APP 4 - Unsolicited PI

Sometimes we receive personal information that we have not asked for directly from the individual (unsolicited). When that happens, we will determine whether that information could have been collected directly by us. If we could not have collected it directly, and the information is not part of a record (e.g. a document or record held by a government agency), then we are required to destroy it or de-identify it as soon as practicable (provided that would be lawful and reasonable to do in the circumstances).

APP 5 - Collection notices

However, if we determine that it was reasonable to have collected it directly then we will give you a notice or take steps to make you aware that we have so received it (sometimes called 'collection notice') and in particular:

- Who we are and how you can contact us
- If it is likely that you are not aware we have your personal information, the circumstances by which we came to collect it, and what that personal information is comprised of

- If the collection was a requirement or authorised by law, then we will identify the law and the circumstances which gave rise to us collecting it
- The purposes for which we collected and use it
- The consequences (if any) for you if we do not collect it
- Who we usually would disclose that information to and why
- How you can access it for verification alteration or removal and how and to whom you can complain if you are unhappy with the way we have handled your personal information.

In addition, we have to tell you if it is likely that this information will be disclosed to an overseas recipient, and if so which countries may be involved if that is practicable or at least make you aware of the fact.

APP 6 - Hold, Use, Disclose, and Purpose

If we hold your personal information for a particular purpose this is the primary purpose and we cannot use it for any other reason (a secondary purpose) unless:

- you have consented to that use or disclosure; or
- you would have reasonably expected it to be used for that secondary purpose.

We will always try and get your consent wherever practicable. We also try not to deal in sensitive information unless it's necessary for the service we provide or we are compelled to do so for legal reasons. If we do have to collect your sensitive information then your written informed consent will be obtained before it's disclosed.

If we collect personal information from one of our related parties or they collect it from us, then the primary purpose of the collector is considered to be the primary purpose for the related party. In this respect, as outlined in this summary and more fully in the Policy.

However, we cannot share your personal information with related parties if the purpose involves direct marketing unless you have requested or consented to it.

APP 7 - Direct Marketing

It is important that you be aware that the Act and particularly the APPs prohibit the use or disclosure of personal information for the purpose of direct marketing unless:

We have collected the data directly from you and you would reasonably expect us to use or disclose it for that purpose. In that case we will always provide you with an easy way of requesting us not to bother you again with any marketing material. This is in the form of a telephone call, an email, provided we can verify the caller. We will immediately take steps to remove you from marketing communications; or

We collected it from you (but you would never reasonably expect to receive marketing material from us or for your data to be disclosed for that purpose); or

We collected it from someone else; and
In either case you have consented to the use or disclosure or it's impracticable to get your consent.

(In either of these instances we will offer you the same easy means of removing yourself from that marketing list and we will include a prominent statement in every such communication that you can request to be so removed.).

In all cases where we use or disclose personal information (whether for membership or otherwise) for the purposes of our own direct marketing or to facilitate another organisation's direct marketing, you can always request that you be removed from the marketing list and or ask us not to disclose your data to the other organisation(s) for that purpose and also require us to tell you where we got the information from. There is no charge for you to action this right.
(Note that the *Spam Act* and the *Do Not Call Register Act* both continue to apply regardless of the APPs.)

APP 9 - Government identifiers

AICIP does not use government identifiers (e.g. Medicare numbers, Tax File Numbers, etc) for the purpose of identification of individuals.

APP 10 - Quality of PI held
APP 11 - Security
APP 12 - Access
APP 13 - Correction

We use strict protocols to guard the integrity and quality of and access to the personal information we collect or hold. We review our service providers' contracts to ensure as far as practicable that they have implemented the security measures appropriate to reasonably protect us and you from misuse, interference and loss and particularly from unauthorised access amendment or disclosure. In particular, credit card and financial information is held under strict security until able to be deleted or destroyed: unless you tell us to do so, we do not retain such information for future transactions.

We have implemented procedures that facilitate the destruction or de-identification of personal information when it is no longer necessary for the purposes for which it was collected (unless it is needed for legal reasons).

Accessing your personal information for verification amendment or removal can be effected in any of the ways mentioned above including emailing the AICIP Administration; calling our office, or through the Contact Us form on the website. Quality assurance, security and risk management are all continuously being monitored and enhanced or improved as technology and regulation change.

There is no charge for this service and we promise to action your request as promptly as possible (subject only to the usual qualifications like legal compulsion or compliance obligations).

PART 111C - Notifiable breaches

This new Part 111C of the Act deals with notifiable breaches of the Act. AICIP has already instigated some internal controls and processes to address the identification and notification rules that will apply to us as an entity subject to the Act. While specific guidelines have yet to issue in respect of compliance with this Part 111C, the intention is for AICIP to ensure that in both cases where it controls the PI and where the control is vested in a third party (e.g. servers or data storage are based

overseas) eligible data breaches are promptly managed in accordance with following general requirements of the Act:

- 'eligible data breaches' will be notified to the Information Commissioner and to relevant individuals in connection with the PI affected.
- notification is mandatory where serious harm to any of the individuals is likely. The threshold tests which trigger the notice obligations are based on an objective test of what a reasonable person would conclude.
- An 'eligible data breach' occurs when, in respect of personal information, the following conditions are satisfied:
- there is unauthorised access to, or *unauthorised disclosure* of, the information, or where the information is lost, unauthorised access to, or unauthorised disclosure of, the information, is likely to occur; and
- a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to which the information relates (in the case of lost information assuming that unauthorised access or unauthorised disclosure were to occur).
- There are some important exceptions to notification:
- where remediation is taken that has reduced the risk of serious harm.
- Where legal enforcement obligations or secrecy provisions apply
- If a notifiable breach occurs which is not subject to an exception or exemption, then we must issue the notification of breach to the individuals affected. Where the actual identity of a single individual is not the issue (i.e. where a group of individuals or a class of persons may have been subject to a breach) then the statement will be published on our website and in any other format required by the OAIC without identifying the individuals themselves.