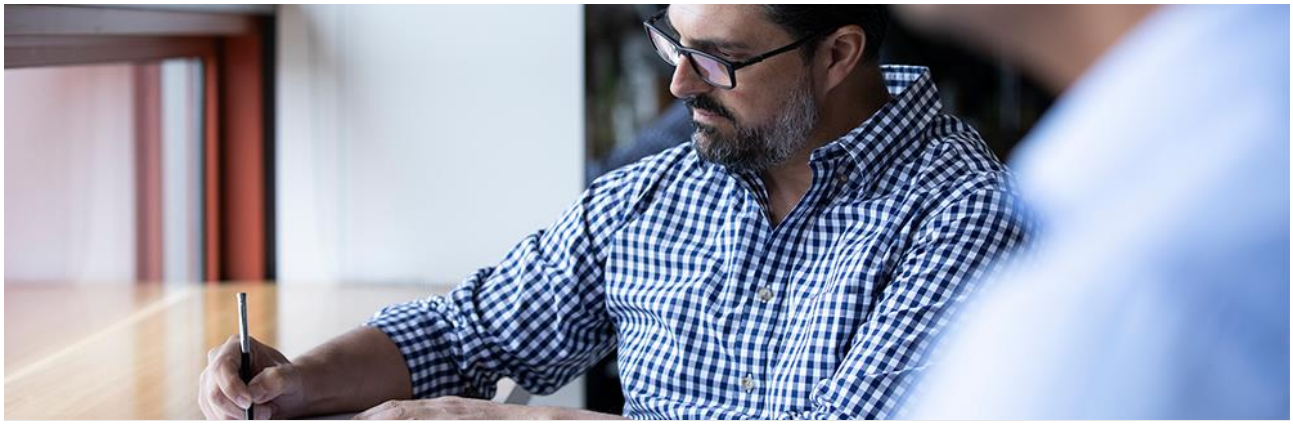
Australian Centre for Advanced Computing and Communication

Privacy Policy



November 2023

Notices

Table of Contents

Executive Summary

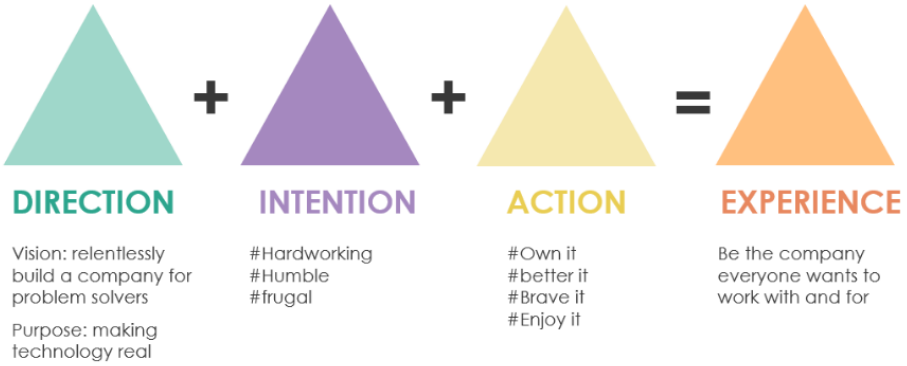
AC3's Privacy Policy sets out how AC3 manages Personal Information that we may receive or collect, use and disclose.

"Personal Information" has the meaning as set out in the *Privacy Act 1988* (Cth). Personal information is any information or opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not, or whether recorded in a material form or not

We are committed to ensuring the proper, open and transparent management and use of all Personal Information we collect and handle in accordance with applicable privacy laws, including the Australian Privacy Principles and the New Zealand Privacy Principles.

All our employees and contractors have responsibilities in respect of this privacy policy, which will be regularly communicated.

This policy reflects and operates within the context of The AC3 Way, components of which are represented in the image below. AC3's Vision and Purpose direct our collective action, i.e. Ways of Being, which is underpinned by our intention, Ways of Thinking. Working with these components, we strive to be the company everyone wants to work with and for.



This policy forms part of your employment agreement or engagement; any breach of this policy may result in disciplinary action which could lead to termination of employment or engagement with AC3. Because we're always looking for ways to Better It, we reserve the right to vary or rescind this policy at any time.

Management of Personal Information

We are strongly committed to ensuring that we are open and transparent about the way we manage Personal Information. The AC3 Privacy Policy covers:

1. the kinds of Personal Information that we collect and hold
2. how, and the purposes for which, we collect, hold and use Personal Information
3. who we disclose Personal Information to
4. how you may access Personal Information about yourself that we hold and seek the correction of such information
5. how you may complain about a privacy issue or alleged breach of the Australian Privacy Principles and how we will manage such a complaint
6. whether we are likely to disclose Personal Information to overseas recipients.

Collection and Storage

We will only collect Personal Information that is necessary for our functions and activities. We will only collect Personal Information by lawful and fair means and not in an obtrusive way.

We collect and hold different categories of information depending on the nature of your interaction with us.

Employees, Contractors, Suppliers and Customers

We generally collect Personal Information directly from our employees, contractors, customers and suppliers. Depending on the nature of your interaction with us, this Personal Information may include names and contact details so that we can contact you. For employees and contractors, we may also collect certain sensitive information, such as a tax file number, next of kin name and contact details, banking and superannuation details, remuneration details, employment checks (reference checks, Police Checks, Working with Children Checks, etc.), injuries and attendance records.

The purpose of collecting such information is so we can meet our employer obligations (such as payroll and making superannuation contributions), to contact next of kin in an emergency, and to ensure that our people (employees and contractors) have the skills, experience, qualifications and clearances required to perform services for us and our customers. All Personal Information about employees and contractors will be held securely. Secure storage methods include, but are not limited to, locked filing cabinets with restricted access (for physical documents), and approved cloud-storage services, with relevant access and other security controls (for electronic records).

We may also collect feedback and information from third parties relating to our employees, contractors and suppliers' performance of services for us. This information is collected for the purposes of monitoring our contractors and suppliers' performance of services and to ensure that we can provide the highest quality products and services to our customers.

Job Applicants

If you apply for a position at AC3 we may collect your name, contact details and any information that you have provided us as part of your job application. This may include information contained in your CV, your driver's license and/or passport. We may also collect Personal Information relating to you from third parties you have identified as referees or references in your job application. We may also require you to undertake criminal record check ("Police Check"), Working with Children Check and/or other pre-employment checks that are required for either ours or our customer requirements. This information is solely used for the purposes of determining your suitability for the role that you have applied for.

Customers and their employees

When you become a customer we may collect Personal Information from you such as your name, contact details and email address.

As part of our due diligence on customers that request commercial credit from us, we may use a credit monitoring & reporting company to provide us with credit information ("credit reporting agency"). We will only use or disclose your credit-related information for the primary purposes for which it was collected or as consented to, or as otherwise set out below:

1. to review the customer's credit score and assess the terms we offer to the customer;
2. lodge defaults with the credit reporting agency after having followed the proper process;
3. periodically reviewing that credit-related information for existing customers to ensure continued credit worthiness;

4. disclose that information to our Related Bodies Corporate if required, or a person who manages credit, to process an application or manage credit or discuss an enquiry with you or for related internal management purposes that are directly related to the provision or management of commercial credit;
5. the administration and management of our products and services, including charging, billing;
6. third parties, such as external debt collectors or external dispute resolution providers in relation to any complaints or disputes concerning the credit offered to you;
7. other credit providers where you have consented and where permitted by law; and
8. other persons where required or authorised by law.

In addition to using and disclosing credit-related information as set out above, all customer Personal Information collected by us is solely used for our business functions and activities. It may be used for the following purposes:

1. for billing purposes (e.g. invoicing) and order fulfilment
2. to contact you in relation to our provision of services to you
3. to respond to your requests, enquires, complaints and/or other customer service related activities
4. to maintain your account details
5. to provide technical support – for example, account creation, password reset
6. to provide you with information in relation to our products, services or other information that you may have requested
7. to streamline and personalise your experience while dealing with us
8. to undertake customer satisfaction surveys and to tailor our information, services or products to improve and enhance those services and products provided to the customer.

We may also collect from our customers Personal Information relating to its employees and customers; for example, payroll information. This Personal Information is solely used so that we can facilitate provision of the services our customers have requested.

We may use de-identified Personal Information derived from:

1. our customers and our customers' employees
2. customers use of our products and services in order

to create anonymous demographic and customer usage information. We will then use this anonymous, aggregated information to develop new and or more appropriate services and products to offer to our customers.

Quality of Personal Information

We will ensure, to the extent reasonably possible, Personal Information collected, used or disclosed is accurate, up-to-date, complete, and relevant. If we become aware that any Personal Information, we hold is inaccurate we will take prompt steps to update and correct our records.

If you believe the information we hold is in-accurate, not up-to-date, incomplete or irrelevant, you can ask us to correct the information. Refer to the "Access and Correction of Personal Information" section below.

Data Security

We take active measures to ensure the security of Personal Information we hold against misuse, interference, loss and unauthorised access, modification, or disclosure.

All Personal Information is stored at secure premises. Electronic Personal Information is stored using the highest quality data management tools and IT security systems and controls including passwords and firewalls.

When we no longer require Personal Information, it is securely destroyed and disposed of.

Our security systems are regularly reviewed and internally and externally audited so that we can identify any potential security weaknesses and take steps to promptly rectify them. We are certified to ISO 27001 Information Security Management Systems and ISO 9001 Quality Management Systems standards.

Access to Restricted Information

Our employees and or contractors, while employed or engaged, may have access to Restricted Personal Information about our Customers while working on our Customers' IT Systems.

Restricted Personal Information includes but is not limited to:

- Personal Information our Customers hold about their customers and/or clients
- Criminal Records, such as criminal convictions, spent criminal convictions, and other corrective services records
- Personal Information about children and children-at-risk
- Personal Information which is protected at law by the Privacy Act and/or other legislation.

Prior to being granted access to IT Systems that contain such Restricted Personal Information, we require relevant employees to undergo Police and other relevant Checks to ensure there is not a prohibited reason preventing them being in contact with such Restricted Personal Information.

Under no circumstance is such Restricted Personal Information permitted to be used, disclosed, collected, stored. or illegally accessed by our employees. Nothing in this policy gives permission to employees to breach the privacy of such Restricted Personal Information.

We take breaches or suspected breaches of such information privacy very seriously, and not just as a breach of this policy but as a breach of relevant legislation. As a result, any breach or suspected breach of policy and/or legislation will be treated as such, with immediate referral after becoming aware to relevant law enforcement authorities for investigation, and or disciplinary action, up to and including termination of employment may result.

Direct Marketing

From time to time, AC3, our related bodies corporate and third parties who provide services to AC3, may also use your personal information to tell you about products and services we think may be of interest and value to you. We may contact you by various means, including, but not limited to, telephone, email, or other electronic means (such as social media).

If you do not want to receive direct marketing offers from us, you can opt-out at any time, by contacting marketing@ac3.com.au or unsubscribing directly from marketing emails using the unsubscribe function on those emails.

Disclosure and Retention of Personal Information

As part of providing our services, we may disclose Personal Information to third party suppliers and contractors of services, banks, or other financial institutions, and to customers. In these cases, we expect these organisations to protect the privacy of that Personal Information.

In particular, if a customer requires us to provide Personal Information about our staff (employees and contractors) who will be providing services to our customers (for example, Police Clearance Certificates, Working with Children Checks, professional experience/qualifications), this Personal Information is subject to the relevant customer signing a Non-Disclosure Agreement about the collection, use, storage and retention of such Personal Information.

Other than in the cases outlined above, we will not disclose Personal Information to any other third party unless we have reasonable grounds to believe:

- the individual has authorised the disclosure
- the safety of the individual, or the safety of others in the community is at risk
- we are required or permitted by law to do so (includes responsibilities related to statutory reporting and preventing breaches of the law).

As a provider and user of cloud services, we generally retain Personal Information on servers within Australia. However, we may also disclose Personal Information overseas, including to:

- AC3 Group Members based in New Zealand and support staff based in South Africa, Ireland and the Philippines.
- service providers or other third parties located in the United Arab Emirates, Canada, Pakistan and Thailand.

Unless we have an individual's consent, or an exception under Australian privacy law applies, we will take all reasonable steps to ensure that no person or entity, including any overseas entity, breaches any privacy laws applicable either locally, or in the country where the entity is located.

We will store any credit information provided to us, or which we obtain about you, with any other personal information we may hold about you, which shall include but is not limited to the use of paper files, electronic files, and databases.

We only retain Personal Information for as long as required by law and needed for our business functions and activities. It is then securely destroyed and disposed of.

Website Browsing

Accessing our websites will result in some information being logged including the time of access, your IP address and the pages that have been viewed or accessed.

Our websites may contain links to external websites. We are not responsible for the content or privacy policies that govern such external websites.

Access and Correction of Personal Information

Subject to verification of your identity, if we hold Personal Information about you, you may make a request to access, update or correct this Personal Information.

Access and correction requests should be made in writing to one of the contact addresses below.

We will endeavour to respond to written requests for access and correction of Personal Information within 10 business days after a request is received by us unless extenuating circumstances exist.

We will take all reasonable steps to ensure that Personal Information is accessed by employees/contractors only to the extent necessary for us to undertake our business activities.

BYOD Policy

As part of our Bring Your Own Device (BYOD) Policy, we may use a Mobile Device Management (MDM) solution which may install software onto employees' Personal Electronic Devices to enforce the BYOD policy and make management of company confidential data easier and keep personal data separate from work-related data.

We take our employee's privacy seriously, therefore any MDM solution we select will, as far as reasonably practical, prevent us from accessing your personal data (including personal: messages, photos, emails, internet usage, phone calls and other personal data contained on your Personal Electronic Device), and where not reasonably practicable to prevent us from accessing your personal data on your Personal Electronic Device, our policy is that we will not access your personal data, and any breach of our policy will be treated as such.

Complaints

All complaints relating to the handling and management of Personal Information by us or any breach of the applicable privacy laws, including the Australian Privacy Principles should be addressed to one of the contact addresses below.

To deal with complaints appropriately, please include the information listed below together with your complaint:

- a summary of the privacy concern or alleged breach
- any action, or inaction, we have taken, or failed to take, regarding the matter
- copies of any relevant documentation in connection with the complaint, including any communications that we have had with you.

Our Privacy Officer will investigate the complaint, and, where necessary refer the complaint to the relevant department that the complaint relates to or refer the complaint to an external investigator contracted by us. We will endeavour to respond to complaints within 20 business days unless extenuating circumstances exist.

We will take immediate steps to redress proven privacy concerns or breaches.

If you are not satisfied with our response and your complaint relates to a privacy concern or alleged breach, you may take your complaint to the Office of the Australian Information Commissioner (Telephone: 1300 363 992) or the New Zealand Privacy Commissioner (Telephone 0800 803 909).

Access to This Policy

This policy can be viewed on our website at www.ac3.com.au

You can also request a copy of this policy from one of the contact addresses below.

Contact Information

The Privacy Officer, AC3

Level 7, 477 Pitt Street. Haymarket 2000 NSW

Email: privacy@ac3.com.au

Policy Information

Compliance applicability

This policy helps AC3 meet our compliance obligations for the following controls:

Standard	Control Reference	Control Description
ISO27001:2022	5.34 - Privacy and protection of PII	The organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.
ISO27001:2022	6.1 - Screening	Background verification checks on all candidates to become personnel should be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. Verification should take into consideration all relevant privacy …[and] PII protection [legislation].

Acronyms

Term	Meaning
BYOD	Bring Your Own Device
MDM	Mobile Device Management

Definitions

Term	Meaning
Personal Information	Information or an opinion, whether true or not, and whether recorded in material form or not, about an identified individual, or an individual who is reasonably identifiable. Personal Information for the purposes of this policy includes credit-related information where the context permits.
We/Our/Us	Australian Centre for Advanced Computing and Communication Pty Limited and Australian Centre for Advanced Computing and Communication Pty Limited NZ ("AC3") and associated entities
You/Your	An eligible person covered by this policy

Document Credentials

Contact Details

We welcome any enquiries regarding this document, its content, structure or scope. These should be directed to:

Name:	Tristan Williams
Position:	Privacy Officer
Email:	tristan.williams@ac3.com.au

Document Control

Document Reference

Department:	Corporate Services
Document Name:	AC3 Privacy Policy
Reference Number:	KB0010786

Preparation

Version	Date	Change	By (Name, Position)
1.0	6/04/2011	Created	I Halforty
1.1	18/11/2011	General revision to clarify purpose and requirements	I Halforty
2.0	23/06/2015	Update to comply with Australian Privacy Principles	Warren Hackett, QA Manager
2.1	09/05/2017	Re-formatted	Bindi Kelly, Administration Assistant
2.2	22/05/2020	Updated template & language	Nadja Lorenz, People & Culture Coordinator
2.3	19/06/2020	Updated to refer to credit-related information	Margarita Donaghey, Legal
2.4	17/7/2020	Change of document owner	Warren Hackett, Corporate QA Manager
2.5	19/10/2020	Adding phone number of NZ Privacy Commissioner	Warren Hackett, Corporate QA Manager
2.6	14/6/2023	Minor wording updates; added compliance applicability	Tristan Williams, Senior Compliance Officer
2.7	21/11/2023	Updates to directing marketing and disclosure/retention sections based on feedback from 2.6 review	Tristan Williams, Compliance and Legal Counsel

Reviewers

Version	Date	By (Name, Position)
2.0	8/10/2015	Kathy Seymour, Head of People and Culture
2.1	03/07/2017	Kathy Seymour, Head of People and Culture
2.1	06/07/2017	Warren Hackett, QA Manager
2.2	25/5/2019	Warren Hackett, Corporate Quality Assurance Manager
2.2	02/07/2020	Kathy Seymour, Head of People and Culture
2.5	13/11/2020	James Meharg, Head of Corporate Services
2.5	16/11/2020	AC3 IS&Q Management System Committee
2.6	31/07/2023	Damien Luke, Head of Cyber Security
2.6	03/08/023	Emma Flanery, General Counsel
2.6	05/09/2023	Stephanie Challinor, GM Customer Experience & Alliances; Ash Baker, Marketing Manager
2.6	27/09/2023	Parul Shah-Batra, Head of People and Culture

Approvals

Version	Date	By (Name, Position)
1.0	18/04/2011	Harry Kassianou, Managing Director
2.0	09/10/2015	Simon Xistouris, CEO
2.1	10/07/2017	Simon Xistouris, CEO
2.2	17/7/2020	Simon Xistouris, CEO
2.5	16/11/2020	Simon Xistouris, CEO
2.7	21/11/2023	Christina Temme, GM Finance and Corporate Services

Distribution

Version	Date	To	Position
1.0	19/04/2011	All staff	All positions
2.0	12/10/2015	All staff	All positions
2.1	10/07/2017	All staff	All positions
2.2	17/07/2020	All staff	All positions
2.5	16/11/2020	All staff & contractors	All positions
2.7	21/11/2023	All staff & contractors	All positions

Classification

Classification	Description
Release for General Use	A document that can be released without approvals

Related Documents

Document Name	Reference Number
Code of Conduct	KB0011094
IT Acceptable Use Policy	KB0010777
Anti-Discrimination and Harassment Policy	KB0015842
Managing Underperformance and Misconduct Policy	KB0010797
Social Media and Media Policy	KB0010790
Bring Your Own Device (BYOD) Policy	KB0010731

Next Review

New Review Date	Responsible Officer
2 years from most recent review	Privacy Officer

End of Document