

Ai Group Privacy Policy

Artificial Intelligence Group Pty Ltd (ABN: 68627324896) Artificial Intelligence Group and each of its related bodies corporate from time to time (referred to as “Ai Group”, “we”, “us” or “our”) are committed to complying with our obligations under the Australian Privacy Principles (APP) that form part of the Privacy Act 1988 (Cth) (Privacy Act). When users (referred to as “you” or “your”) register to use and/or log on to our Ai Group Intelligent Video Monitoring Service or download any mobile app provided as part of service), you may be required to provide certain information, including your, CCTV equipment details, Make, Model, Static IP address, User name, password, contact details, to access the service and the terms of this Privacy Policy will apply to that use. Ai Group may collect, use and disclose personal and other information in the circumstances set out below.

What personal information do we collect?

When you register to use and/or log on to our service, we capture the following:

- Video footage from existing or new CCTV cameras;
- Time date stamp;
- Location
- Site static IP address details
- Port details
- NVR/ DVR Username password

We respect your personal information, and this Privacy Policy explains how we handle it.

Our Privacy Policy is all about personal information – all the things we know about you. Because your information is so important to us, we'll always be honest and transparent about how we handle it.

The Policy explains how we collect your personal information, what we do with it, and, most importantly, how it's protected.

Every day we're using personal information when we employ and place people and provide service to our customers.

When you register to use and/or log on to our service, we capture the following:

- Video footage from existing or new CCTV cameras;
- Time date stamp;
- Location
- Site static IP address details
- Port details
- NVR/ DVR Username password

When you use, access or become a registered user of our service including accessing reports, we may ask for information including:

- your name;
- your email address;
- your telephone number or residential address.

The site is an Australian based website, and it is not intended to provide services to EU residents, and its terms may not be fully consistent with the General Data Protection Regulation. If you are an EU resident and you choose to use this service, then you do so at your own risk, and on the terms of our website.

We may also collect the following information from you when you access our website or use services offered by our website:

- the fully qualified domain name from which you accessed our websites, or alternatively, your IP address;
- device ID number (MAC address);
- the date and time you accessed each page on our websites;
- the URL of any webpage from which you accessed our websites;
- the URL from any webpage from which you accessed our website (the referrer);
- cookies which enable tracking or provide other information, including your visits to and interaction with our web sites; and
- the web browser that you are using and the pages you accessed.

Why we collect personal information

We collect personal information from you when it is necessary for a business purpose.

We collect the information to enable us to supply you with the services or employment that you have asked for.

We are collecting this information (and may use, hold or share this information with our trusted business partners) for the following purposes:

- to monitor patient movement and behaviour and to alert front line staff in an event an incident or emergency requiring intervention occurs e.g. fall, slip, disorderly conduct, etc.
- to assist with staffing resourcing levels to ensure
- to identify preconditions that trigger an incident and to proactively reduce or manage the likelihood of occurrence
- to provide proactive monitoring of abnormal behaviour and to trigger appropriate levels of mitigating actions

- to conduct analysis of the data captured and to provide for a safer environment with a reduction in incidents and accidents report
- we may use the anonymised data for the purposes set out above and to inform our promotional and marketing strategies, as well as for general research and profiling purposes, including visitor demographics, interests and behaviours based on personal information and other information provided to us. This research may be compiled and analysed on an aggregate basis, and we may share this aggregate data with our affiliates, agents and business partners. This aggregate information does not identify you personally. We may also disclose aggregated information in order to describe our services to current and prospective business partners, and to other third parties for other lawful purposes;
- we may connect information you provide to us for one purpose with other information for use for one or more of the above purposes. If you access or appear in video footage we capture of you or your patients, and we already hold other information (both personal or non-personal) that can be associated to you, then that information may be linked with personal information we hold about you as set out in this policy, and will be treated in the same manner as the personal information to which it has been linked;
- we may also use information we collect about you to obtain further details from available sources via our trusted data service providers, where it may help us to improve our communications and care to you

In addition to the purposes set out above, information may be used in connection with the management and security of our properties, which are under video and camera surveillance. The information may be provided to law enforcement agencies, government bodies (including, without limitation, where the information may be required for use in litigation relative to or affecting us), insurers, Ai Group staff and subcontractors, retailers and third parties who provide AiG Ai Group with services from time to time.

Other reasons we collect personal information are to:

- Understand you, and how we can meet your specific employment needs,
- So, we can fulfill our responsibilities as an employer,
- Understand your specific service requirements,
- Manage our business,
- Comply with our legal obligations.

The type of information we collect

We collect personal information like your name, address, existing/ New CCTV equipment make & Model, Static IP address, NVR/ DVR username, Password, Video footage from your CCTV system, occupation, location, contact details, payment details, financial information.

Who collects the personal information?

Personal information may be collected directly by us, our agents or by our trusted business partners acting on our behalf, such as security management companies, technology providers and trusted data service providers.

Information may also be collected by us on behalf of other people as set out in notices given to individuals, or consents given by individuals, at or prior to the time the personal information is collected.

How is your personal information stored and kept secure?

Personal information may be held securely on our electronic databases (which may be on a database maintained by a cloud hosting service provider or other third party database storage), or otherwise in hard copy form in secure storage facilities. These databases are managed in secure locations within Australia and are protected by a firewall as well as host-based security. Your personal information may be transmitted over the Internet once it has been stored in a database and may also be transferred across borders to recipients in foreign countries other than Australia, including the United States of America, and may be stored on servers, using databases or via cloud technology in a number of countries other than Australia, including regions such as the United States of America, the European Union and Asia, where doing so is part of AIG's Ai Group's ordinary business practices relating to the storage of data and where permitted by law.

If Ai Group ever has a requirement to transmit such data over the Internet (for example, to make an off-site back up) it will be in encrypted form. By providing us with your personal information, you consent to these transfers.

Disclosing your information

We will disclose the personal information we hold about you from your use of our services in certain specific circumstances, such as:

- when you agree to the disclosure;
- in relation to or for the purposes we collected it;
- when disclosure is required or authorised by law; or
- as permitted by the Privacy Act.

To the extent permitted by law, we may disclose your personal information to:

- our associated entities and related bodies corporate;
- our centre managers and trusted business partners for marketing purposes;

- trusted third parties who we engage to provide related services to Ai Group from time to time;
- our staff, agents and subcontractors in connection with the management and security of our implementations;
- government agencies as part of our statutory obligations; or
- as otherwise permitted by law.

Direct marketing

By accessing and using our Services, you consent to the use and disclosure of your information by and to our business partners for the purpose of allowing them to directly administer treatment or remediation in the event of a reported incident.

Right of access to your information

You have the right to access, update and correct your personal information held by us. We will take all reasonable steps to ensure that personal information held by us is up-to-date, accurate and complete. If you wish to access, update or correct your personal information, please contact Ai Group Risk & Compliance Officer (Privacy Officer) via the contact details below.

Parties we work with

We sometimes team up with other companies to offer services or products. If you undertake work that is delivered on the site of one of our partners, we'll give them the personal information they need to provide the service or products, and to manage their relationship with you. In these circumstances, we have arrangements in place with our partners that limit their use or disclosure of your personal information to these purposes.

Outsourcing

Ai Group work with third parties to provide some types of sales, business and customer support. They do not have access to systems that include your personal information. However, if any do or personal information is provided to them for business purposes, these companies are subject to strict controls that protect your information from unauthorised use or disclosure, and limit their access to your personal information to the extent necessary to do their job.

Access to personal information from overseas

The Ai Group maintains effective control of your information at all times, including by ensuring that if any parties located overseas they are subject to strict controls that limit access and subsequent handling of your information to the extent strictly necessary to perform the relevant function and protect your information from unauthorised use and disclosure.

Legal obligations and other privacy exceptions

We give access to personal information where we are permitted or obliged to do so by Australian law. For example, in some circumstances we will use or disclose personal information to react to unlawful activity, serious misconduct, or to reduce or prevent a serious threat to life, health or safety. We are obliged to cooperate with law enforcement bodies in some circumstances. We may disclose personal information when we receive an access request or warrant that is authorised under Australian law.

Others

We will only disclose personal information to others if you've given us permission, or if the disclosure relates to the main reason, we collected the information and you'd reasonably expect us to do so.

You can get access to personal information we hold about you, ask us to correct it, or make a complaint, as described elsewhere in this policy.

SECURITY

Security of your personal information is extremely important to us. We are committed to protecting your personal information.

Some of the security measures we use in our internal systems include:

- Firewalls and access logging tools that protect against unauthorised access to your data and our network.
- By having Process systems in AWS where any data or video footage collected for our client's site for Ai verification is processed and deleted within a 96-hour time frame. No data or video footage is saved or backed up externally outside the secure network.
- Secure work environments and workflow systems that prevent unauthorised access and copying of your personal information.
- Secure server and closed network environments.
- Encryption of data in transit.
- Virus scanning tools.
- Management of access privileges, to ensure that only those who really need it can see your personal information.
- Ongoing training and security reviews.

These measures are robust, but security risks do change. We will remain vigilant in our efforts to protect your personal information.

- Confidentiality requirements of our employees
- Only giving access to personal information to a person who is verified to be able to receive that information, for the purpose of performing their working responsibilities.
- Document storage security policies
- Control of access to our buildings
- Security measures for access to our systems, including but not limited to:

Privacy Complaints

If you believe we have breached our privacy obligations or your privacy rights in any way, please contact the Ai Group Privacy Officer. We will respond to your complaint as soon as possible, and within a reasonable timeframe.

Privacy Officer Contact Details

Ai Group Privacy Officer

Address: 7, 35 -37 Dunlop Road, Mulgrave, Vic 3107

Email: jbenedict@aintelgroup.com

Telephone: 0400 305 324

If you think we have not resolved a complaint satisfactorily, we will provide you with information about the further steps you can take. You can also contact the:

Officer of the Australian Information Commissioner

GPO Box 5218, Sydney NSW 2001

Phone: 1300 363 992

Email: enquiries@oaic.gov.au or www.oaic.gov.au

QUALITY OF PERSONAL INFORMATION

We aim to keep the personal information we hold about you accurate, up-to-date and complete. If you think our records need to be corrected, please contact us via email info@aintelgroup.com, or call us on + 61 (0) 3 9540 0708.

We encourage you to update your details with us so we can deliver better service to you, and so the others we work with (like emergency services) have access to the information they need to do their job.

HOW TO ACCESS YOUR PERSONAL INFORMATION

If you ask us, we will usually give you access to the personal information we hold about you. We will always confirm your identity before giving access to your personal information.

You can ask for access by calling us on + 61 (0) 3 9540 0708. It will really help if you tell us what you're looking for. There are circumstances under Australian privacy laws where we may not give you access to the personal information; we hold about you. For example, we can't give you access if it would unreasonably affect someone else's privacy or if giving you access poses a serious threat to someone's life, health or safety.

There is generally no cost for accessing the personal information we hold about you, unless the request is complex or resource intensive. If there is a charge, it will be reasonable, and we will let you know what it is going to be so that you can agree to it before we go ahead.

Changes to our Privacy Policy

This Privacy Policy relates to our current privacy standards. We may vary our Privacy Policy from time to time. We will notify you of any changes by publishing the updated Policy at this location from time to time. You should check this Privacy Policy regularly so that you are aware of any variations. You will be deemed to have consented to such variations by your continued access and use of our Services, following such changes being made.