Policy

Subject Description:	Privacy and Confidentiality
Approved By:	David Stockwell
Written By:	Nicole McLean
Pages:	Five

Stockwell International Pty Ltd considers best practice when it comes to maintaining privacy and confidentiality in the workplace. It is important for employees to understand what information may be collected and retained by their employer. Stockwell International will take all necessary steps to ensure the responsible handling of employee and client data.

What is privacy?

The **Australian Privacy Principles (APP's)** protects all kinds of personal information. This includes any information that could identify you, including:

- Written records that identify you by name, address, date of birth, place of work, including medical records, driver's licences.
- Photos, images, video or audio footage

These laws set out the ways in which companies can collect, use, disclose, and maintain the security of your data. The most important include:

- Ensuring that personal information is managed in an open and transparent manner
- Making sure that personal information remains anonymous or uses a pseudonym (alternate name) where personal information must be used.
- Personal information may only be collected by a company where there is a need to, such as if it is required by law.
- Unnecessary information recieved by an employer must be destroyed
- Maintaining that personal information may only be disclosed by an organisation with permission from its owner.

Employer obligations

The Fair Work Act 2009 (Cth) requires employers to make and keep employee records for a period of 7 years. This includes information such as full name, date of birth, next of kin, wage/salary details, tax file numbers and bank details

Stockwell International takes all steps to protect this data, as per the **IMS Network Security Policy**.

Stockwell International will not collect, use or disclose employee information without the consent from the employee, unless it is required by law. This includes when data is requested by police, government agencies, Fair Work inspectors, Australian Border Force or in cases of emergencies. Under the Privacy Act 1988 (Cth), companies may only collect data that is *'reasonably necessary'* for a company to perform its regular functions.

Stockwell International must destroy 'unsolicited' personal information from its systems or ensure that the information is de-identified.

Stockwell International will never use or disclose held or collected information for the purpose of direct marketing unless consent is obtained.

Employee obligations

It is the employee's responsibility to ensure that their personal information is up to date and accurate. Please consult with the HR department to complete any relevant forms.

Data breaches

As data breaches are unfortunately becoming more common, Stockwell International is pro-active in protecting employee, client and business data. However, as data threats become increasingly complex, we require all staff to be vigilant to prevent these occurrences. A data breach occurs when any unauthorized entity, whether a person or organisation, can access or steal personal information. This not only includes actual personal information, such as name, address or driver's licence credentials, but any information that could be combined with other information to be able to identify a person.

Stockwell International is required to notify anyone who's data has been affected by a data breach. This includes when there has been unauthorised access to personal information and it may result in serious harm to the individual. If we attempt to fix the data breach and are unable to, we will inform our staff of this.

Data breaches can cause significant harm to employees and the company, including:

- Financial fraud, such as unauthorised bank transactions
- Identity theft that causes financial loss, emotional and psychological harm
- Physical harm or threats
- Breach to reputation

Stockwell International asks that all its employees take the following steps to prevent data breaches from occurring.

- Using **strong, unique passwords** and never reusing work passwords elsewhere
- **Never sharing** passwords, MFA codes, or access tokens

- Locking your computer when away from your desk
- Logging out of systems when finished
- Check emails carefully for suspicious links, attachments, or urgent requests
- Verify requests for payments, credentials, or sensitive data
- Be cautious of phone calls or messages claiming to be IT, management, or vendors
- Report suspected phishing immediately
- Only accessing data required for your role (least privilege)
- Not downloading or copying sensitive data unless authorised
- Using approved systems (no personal email, USBs, or cloud storage)
- Avoid installing unauthorised software
- Secure laptops and mobile devices physically
- Prevent shoulder-surfing or screen exposure in public places
- Understand and follow cybersecurity, acceptable use, and data protection policies
- Complete mandatory security training
- Comply with instructions during security incidents or audits

Protecting against data breaches protects **your** personal data and privacy. If you are unsure about any email you receive, please forward it to droussos@stockwells.com.au before taking any action on it.

Client Information Privacy

Stockwell International has set guidelines and procedures when collecting client information.

We only collect and use information that is solicited for a necessary purpose and consented by its owner. Information will only be collected if necessary for one or more business processes.

Collection of information

For new account set ups, we use government approved identity checking systems. We do not hold any identification documents within Stockwell International systems. We only hold verification confirmation once the identity has been confirmed. For more privacy information, visit www.nationalcrimecheck.com.au/

It is important to know that a member of Stockwell's will never ask a client or 3rd party for a copy of identification. These are only required to be visually sighted.

Any collected information will not be disclosed to overseas recipients.

Clients and affiliates can update their information by contacting a Stockwell's Customer Service representative or Reception. Clients and affiliates can update details about their business, such as contact

details and delivery addresses at any time. Changing details that are of a more sensitive nature, such as bank details, will be subjected to stricter security procedures.

Questions/Complaints

To ask a question or make a complaint, you may contact the HR Director on (02) 8335 1200 or contact your local state office for privacy

State	Contact	Website
QLD	(07) 3234 7373	www.oic.qld.gov.au
NSW	(02) 8688 8585	https://www.ipc.nsw.gov.au/
VIC	1300 666 444	https://ovic.vic.gov.au/
WA	(08) 6551 7888	www.oic.wa.gov.au

Relevant legislation

State / Territory	Act	Regulation
New South Wales	Privacy And Personal Information Protection Act 1998 No 133	Privacy And Personal Information Protection Regulation 2019
Northern Territory	Information Act 2002	Information Regulations 2003
Queensland	Information Privacy Act 2009	Information Privacy Regulation 2009
South Australia	South Australia Government's Information Privacy Principles	
Tasmania	Personal Information Protection Act 2004	Proclamation Under The Personal Information Protection Amendment Act 2009
Victoria	Privacy And Data Protection Act 2014	-
Federal	Privacy Act 1988	Privacy Regulation 2013
Western Australia	Freedom Of Information Act 1992	

Conduct that breaches this policy

Conduct that breaches this policy is unacceptable and will not be tolerated.

Where a breach of this policy occurs, Stockwell International will assess the nature and circumstances of the conduct and may take appropriate disciplinary action. Any disciplinary action will be proportionate to the seriousness of the breach, consistent with applicable work health and safety obligations, employment legislation, and principles of procedural fairness.

Stockwell International may take disciplinary action against any person who engages in, or is responsible for, a breach of this policy.

Disciplinary action may include, but is not limited to, one or more of the following:

(a) a requirement to undertake additional training, counselling, or education
(b) a verbal or written warning
(c) termination of employment or contract, in cases of serious misconduct or repeated breaches

Signed: _____ Date: _____/_____/_____

David Stockwell (CEO)