

RSS Privacy Policy

It is the policy of RSS Australia Pty Ltd to conduct its management of personal information such that it complies with the Australian Privacy Principles:

PERSONAL DATA

- Only necessary personal information will be collected and held.
- Staff personal information shall be kept in confidential paper and electronic files kept on premise or in secure cloud services.
- Purposes for which we collect, hold and disclose personal information for matters relating to staff employment, payment, notifications, communication with Government bodies such as the Australian Taxation Office and to form part of leave entitlement records.
- Each individual may access their own personal information held at RSS and may seek corrections to any information they believe is incorrect. Access to an individual's personal records will be via a request verbally or in writing/email to the responsible manager or the RSS Managing Director. Paper based records will be held in secured filing systems and online records will be held on the company's secured server protected by a secure password available only to the responsible manager.
- An individual may complain about a breach of the Australian Privacy Principles, through the RSS Disputes & Mediation procedure RSS-112 AD.
- Unless requested by a checked overseas Government body, your information will not be provided to an overseas entity.

PROFESSIONAL DATA

- Client and Supplier Data is treated as confidential and only disclosed to employees, contractors, Clients and Suppliers to the extent necessary to deliver the service RSS is providing.
- Client and Supplier Data is stored on physical media in a security controlled data centre and archive facility. Client and Supplier Data is removed from physical media through physical destruction prior to physical media disposal.
- RSS limits access to Client and Supplier Data to approved employees and subcontractors authorised based business need. When this authorisation is no longer required for a business need, access to this data is revoked.
- A secure network service including a firewall, encryption, password controlled access, antivirus and procedures are used to prevent unauthorised access to systems, application and devices.
- Data not intended for unauthorised viewing when transferred over public networks, is encrypted by cryptographic protocol such as HTTPS.

In order to support this policy, I will ensure that RSS Australia Pty Ltd will be aware of and comply with all relevant legislation and statutory requirements, industry standards and practices including the European Union General Data Protection Regulation (GDPR). I will provide adequate resources to meet these requirements.

Signed:



Date: 27 Mar 2023

Karl Procter
Director