

Privacy and Confidentiality

This policy outlines how we protect and handle personal and health information in accordance with relevant privacy legislation. GVK Group acknowledge an individual's right to privacy while recognising that personal information is required to be collected, maintained and administered in order to provide quality people and risk management solutions.

GVK Group is dedicated to upholding the Australian Privacy Act 1988, including the Australian Privacy Principles and the privacy and confidentiality of all internal information, including but not limited to employee records, business strategies, proprietary data, and sensitive communications.

GVK Group is committed to:

- Provide all individuals with access to information about the privacy of their personal information.
- Each individual has the right to opt out of consenting to and providing their personal details if they wish.
- Individuals have the right to request access to their personal records by requesting this with the GVK Group management team.
- Personal information will only be used by us and will not be shared outside the organisation without your permission unless required by law.
- Images or video footage of workers will not be used without consent and permission.

All employees are expected to:

- Respect the confidentiality of all internal information they encounter during the course of their employment.
- Handle confidential information with the utmost care and discretion.
- Use internal information only for legitimate business purposes and in accordance with company policies.
- Not disclose confidential information to external parties without proper authorisation.
- Take appropriate measures to prevent unauthorised access, disclosure, or misuse of confidential information.

Access Controls

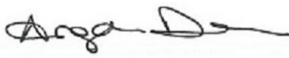
Access to confidential information will be restricted to authorised personnel on a need-to-know basis. Employees are required to use company-provided credentials and security protocols to access internal systems and information.

Data Security

We maintain robust security measures to protect internal information from unauthorised access, disclosure, alteration, or destruction. Employees are expected to comply with all security protocols, including password policies, encryption standards, and access controls.

Confidential Communications

All internal communications, whether verbal, written, or electronic, must be treated as confidential unless explicitly designated otherwise. Employees should exercise caution when discussing sensitive matters and use secure communication channels when necessary.



Angela Delic
Director