

	Use of AI Tools Policy	Risk and IT
	Version 2.0	7 pages
<b>Target Audience</b>	<ul style="list-style-type: none"> <li>All Employees</li> </ul>	
<b>Contact Person</b>	<ul style="list-style-type: none"> <li>Group Risk &amp; Compliance Manager</li> <li>CIO</li> </ul>	
<b>Policy Owner:</b>	<ul style="list-style-type: none"> <li>Risk and IT Departments</li> </ul>	
<b>Related Standards:</b>	<b>Related guidance documents:</b> <ul style="list-style-type: none"> <li>RGF Staffing HQ – AI Utilisation Policy</li> <li>RGFS ANZ Code of Conduct &amp; Values</li> <li>RGFS ANZ IT Facilities &amp; System Use Policy</li> <li>RGFS ANZ Information Security &amp; Governance Policy</li> </ul>	
<b>Effective Date:</b>	<b>Updated as per:</b>	<b>Modification:</b>
Oct 2025	Updated with CIO, HQ and Vivir input	Updated
<b>Approved by:</b>	<b>Approved on:</b>	
Managing Director Managed Services	<b>Oct 2025</b>	

**Please Note:**

**Document uncontrolled if printed or downloaded. Controlled version is available within the Bridge/Vivir Learning.**

## 1. Purpose

The purpose of this policy is to encourage whilst guiding the use of Artificial Intelligence (AI) tools for the group, in-line with RGF Staffing Head Quarters and Recruit Holdings requirements.

## 2. SCOPE

For the purposes of this policy, RGF Staffing ANZ will herewith be referred to as 'the Group'. This policy applies to all entities and brands of the Group, and their employees (including directors, officers, employee, subcontractors, representatives, agents and others (collectively you). This policy applies to the use of an AI tool used in a work/business capacity.

## 3. PRINCIPLES

High Risk AI systems are defined, under the EU AI Act, as the following:

- a) AI systems intended to be used for the recruitment or selection of natural persons, in particular to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates
- b) AI systems intended to be used to make decisions affecting terms of work-related relationships, the promotion or termination of work-related contractual relationships, to allocate tasks based on individual behaviour or personal traits or characteristics or to monitor and evaluate the performance and behaviour of persons in such relationships.

The Group will ensure the following when utilising AI tools:

- We will strive to not cause or contribute to discrimination and/or violation of human rights based on class, race, colour, sex, language, religion, gender, age, political or other opinion, national or social origin, nationality, property, sexual orientation, gender identity, disability, birth, or other status.
- that testing of all high-risk AI tool(s) is performed regularly by the tool Vendor, in order to document that there is no bias and to ensure that outcomes are not disproportionately skewed in favour of a particular group and that this testing is evidenced by the Vendor through their Bias Statement.

## 4. Legal & Compliance

The Group's use of AI tools must be compliant with the local legislation on Artificial Intelligence, across the jurisdictions in which the use of the tool will impact. This includes compliance to local Privacy and Anti-Discrimination legislation.

## 5. Transparency .

The Group must be transparent about our use of AI tools, providing workers and employees with information about their interactions with AI systems involved in the hiring process and explaining how these systems arrive at their decisions.

In this policy, **High Risk AI systems** are defined in alignment with the EU AI Act, as the following:

- a) AI systems intended to be used for the recruitment or selection of natural persons, in particular to place targeted job advertisements, to analyze and filter job applications, and to evaluate candidates;
- b) AI systems intended to be used to make decisions affecting terms of work-related relationships, the promotion or termination of work-related contractual relationships, to allocate tasks based on individual behaviour or personal traits or characteristics or to monitor and evaluate the performance and behaviour of persons in such relationships.

## 6. Responsibilities

The **Managing Director / Head of Department** responsible for the brand/department has the ultimate accountability/responsibility to:

- a) Approve AI results (output is consistent with Bias Statement provided),
- b) Ensure no breach has occurred (including of IP and copyright)
- c) To raise any AI related concerns to the Risk Team
- d) To ensure AI tools are run through the IT Vendor Questionnaire and if PII is included, through the Privacy Impact Assessment
- e) Implement mechanisms and safeguards, (e.g. human oversight) to identify and address risks that may arise from:
  - i. uses outside the intended purpose,
  - ii. intentional / unintentional misuse, or
  - iii. bias in the algorithmic processes.

The **Chief Information Officer** has the ultimate authority to:

- Determine that an AI tool is considered a **High-Risk AI system**.
- Order cessation of use of a particular AI tool on the basis of data or other security risks to the Group

## 7. General Rules

### Limitations and Conditions for Use

1. AI tool accounts must use a Company email address for the log-in credentials and, where PII is involved, Multifactor Authentication is required.
2. Testing must be undertaken and documented by the Vendor in their Bias Statement, in each of the following cases to ensure no bias / result skewing:
  - *class, birth, or other status,*
  - *race, colour,*
  - *sex, gender, sexual orientation, gender identity,*
  - *language, religion*
  - *age,*
  - *political or other opinion,*
  - *national or social origin, nationality,*
  - *property,*
  - *disability*
3. In the event workers, clients or prospective workers enquire about the use of AI systems involved in the hiring process, these requests should be directed to the IT

Service Desk for review and response.

4. Artificial Intelligence (AI) technologies must not be used to provide direct clinical care under any circumstances. This includes, but is not limited to, the summarisation, interpretation, or modification of clinical notes, assessments, or client health records. All clinical decisions and documentation must be completed and reviewed by appropriately qualified allied health professionals in accordance with regulatory standards and organisational policies.

### **Conditions related to Generative AI (GenAI) use (e.g. ChatGPT)**

#### **1. Using GenAI for day-to-day tasks**

- GenAI may be used to obtain answers that will NOT be shown directly to customers/clients.
- Users are to create an account using work email address.
- All activity on GenAI must be for work/commercial purposes only.
- General searches only, just like Googling.
- Must turn Chat History & Training **off** in the GenAI settings when using it.
- **MUST NOT** input any Personally Identifiable Information or information you would not put into a search engine.

#### **Examples of acceptable use:**

- Researching (as an alternative to search engine searching)
- Creating samples (drafting email newsletters, ads, or materials)
- Developing code samples.

Use of GenAI via Microsoft 365 via CoPilot **is** permitted and is an approved use of GenAI.

However, if you are using MS 365 Co-Pilot and utilizing the output commercially, please notify the risk team who is required to notify the RGF Staffing HQ Global Risk Department.

#### **Prohibited usage:**

**MUST NOT** input any personal information, employee data, and the like or any confidential data even for the above listed purposes.

- Input of the following is prohibited:
  - personal information,
  - employee data,
  - confidential data including resumes/CVs/.
  - financial information
  - client data
- Developing meeting minutes,
- Generating queries by inputting data definitions,
- Input of strategy material
- Input of code for tuning, etc.

If a brand / department wants to integrate GenAI into applications, they must consult the Risk and IT Teams prior to implementation. (Approval is required from RGF Staffing HQ).

## 2. Using GenAI for customers/clients

Using GenAI to obtain answers that will be shown directly to customers/clients or any other third parties is subject to the conditions for day-to-day use AND must also have thorough content review and approval by the responsible or manager of the Brand/Department, prior to release.

If the Manager is unsure of the content/sensitivity, consult the Risk Management/Legal team.

Where the Risk/Legal team is unsure, these cases are to be raised to RGF Staffing HQ Risk Management Department.

## 8. PRIVACY & PROPRIETARY INFORMATION

It is important that your use of AI tools complies to privacy legislation and regulations and our Group policies at all times.

The following should be considered, when using AI tools:

- Exercise judgement and discretion at all times;
- Work on the assumption that anything used in a prompt may be viewed, forwarded, or transmitted to recipients that do not have consent to access the information.
- Do not disclose any trade secret type information, for example, don't enter source code into prompts.
- If you are unsure, pause, re-read and think about it before you submit a prompt and check with your manager if you are still not sure whether it complies to this and our other policies.

In particular, **never** enter the following information into an AI prompt:

- TFN (Tax file number), passport number, driver's license number, AGSC ID or any other Government Identifier
- personal health and medical information about anyone
- passwords, passcodes, and other confidential information
- financial and commercially sensitive data and intellectual property, client information, contract information, financial information, source code etc.

Prior to using an AI tool, you must review the associated Usage, Privacy and Security Policies of the vendor and their Bias Statement. If you are unsure whether your use or the tool itself complies with this Policy, please liaise with our Risk or Legal team for further guidance.

## 9. Non-Compliance to this Policy

If you think that you or someone else may have accidentally breached this policy, it is important to alert the IT and Risk teams, so that appropriate investigations can be undertaken to ensure data security.

Deliberate non-compliance to this policy may result in discipline action up to and including termination of employment.