IT Acceptable Use Policy

RGF Staffing

Table of contents

Introduction

All references in this document to “We”, “RGF”, or “the Company” means RGF Staffing APEJ, its related entities, and all its authorised agents and employees.

This document does not form part of your employment contract or other contract of engagement and may be changed by the Company at any time, with or without your consent.

Summary

RGF is committed to the appropriate and effective use of Information Technology resources (IT) . This policy sets out your obligations and the standard of behaviour expected when using RGF IT. Your use of RGF IT must not contravene any other RGF policy (e.g. Code of Conduct, Privacy, Anti-Bullying etc.) or law.

All Users of RGF IT are required to accept this policy, as a condition of use, prior to using any IT.

This policy sets out:

- Your responsibilities, and our expectations of you, when using RGF IT,
- Acceptable use of RGF or our clients’ IT,
- Acceptable use of mobile devices when “connected” to RGF IT or when used in any way related to RGF,
- Notice of RGF’s and clients’ computer surveillance activities,

Scope and Definitions

This policy covers any person using RGF IT equipment or systems (*“Users”*), meaning:

- **Employees** of RGF and its related entities, whether working for RGF or its clients, whether at an RGF workplace, a client workplace, working from home or other remote location;
- **Contractors or Suppliers** (or their representatives) who access RGF IT as part of an engagement with RGF; and
- **Others** who operate on RGF sites or access RGF IT (such as work experience students, interns, employees of a RGF client or supplier etc.).

The term *"RGF IT"* in this policy refers to and includes:

- **IT Equipment** including any computing and communications equipment such as phones, computers, printers etc. supplied by RGF or its clients, and your own IT equipment, when used for work purposes (i.e. BYOD).
- **IT Systems** include, but are not limited to the RFG network, software programs, Apps, email, instant messaging programs, internet access including social media and content sharing forums, intranet, web services, and any similar resources.
- **Confidential Information** (as fully defined in employment agreements) e.g.: information pertaining to our clients, candidates and employees (including contractual terms and commercially sensitive information), SOPs, training materials, intellectual property, strategy, design, plans and financial information etc. This includes information from third parties with a legal basis or reasonable expectation of privacy or confidentiality.

Provision & Use of IT Equipment & Systems

RGF IT provides Users with devices and physical & remote access to RGF IT resources. RGF IT also provides access to RGF IT resources for those who are approved to use their own devices/equipment (BYOD). *(If you require any information regarding IT access, please contact the RGF IT Service Desk on 1800 813 157 or rgfitservicedesk@rgfstaffing.com.au)*

RGF IT may also provide Users with tools to assist with work activities, including portable devices. These items remain RGF property and must be returned at the end of any engagement (or on request).

When using RGF IT, Users must:

1. engage in acceptable use of IT;
2. use RGF IT for legitimate work related purposes, that complies with our Code of Conduct and
3. ensure use of RGF IT is conducted in an honest, ethical, courteous and professional manner.

RGF protects users from malicious or inappropriate content, viruses etc. We use software that tracks and monitors usage and screens emails and web browsing for inappropriate use etc.

Acceptable Use Includes:

- Usage that complies with all federal and state legislation, such as: Privacy, Spam, Copyright, Anti-Discrimination, Intellectual Property and Workplace Health and Safety etc.

- Usage that is consistent with our policies including Code of Conduct, Workplace Diversity and Anti Bullying and your contract of employment or engagement;
- Respecting, protecting and upholding Copyright, Intellectual Property rights of RGF or any other person. Protecting Confidential Information.
- Using email and social media consistent with this policy; exercising proper care and judgement.
- Represents RGF, its clients and yourself professionally and honestly;
- Supports RGF and its clients in maintaining IT security;
- Accepting system updates or security protection updates when prompted;
- Using strong, secret passwords to access systems and for sensitive documents;
- Marking emails with ‘Private’, ‘Confidential’, ‘Commercial In Confidence’, ‘Private & Confidential’, ‘Do Not Forward’, ‘Sensitive’ etc. as appropriate;
- Taking appropriate care of any RGF IT equipment, including not leaving such items in vehicles or in unsecured locations and reporting any loss or damage immediately to RGF IT Service Desk and your manager;
- Limiting your personal use and ensuring it is always in a manner which does not interfere with your work and is not inappropriate or excessive;
- Reporting any inappropriate use of our IT to your manager or RGF representative. You must immediately delete any inappropriate material you receive, and report it to RGF IT.

Unacceptable Use Includes:

- Any use that is criminal, illegal or unlawful or in any way inconsistent with RGF policies (e.g. Code of Conduct, Workplace Health & Safety, Workplace Diversity, & Anti-Bullying)
- Creating, transmitting, attempting to access or otherwise dealing with any material or data which is sexually explicit, discriminatory, violent, obscene, indecent or which could reasonably be regarded as offensive or likely to cause harm or distress to another person;
- Creating, transmitting or otherwise dealing with defamatory material;
- Making derogatory comments about other Users, RGF’s clients, employees/contractors, or other representatives of clients;
- Causing damage (including reputational) to RGF, clients, Users, or representatives, or engaging in conduct which has the potential to do so;
- Use of an unprofessional or offensive photos, or depictions of you, on IT user profiles etc.;
- Transmitting or removing Confidential Information from RGF IT, including through use of USBs or other methods;
- Using IT while operating a vehicle or in any circumstance where it is unsafe to do so;

- Any use for private gain or personal commercial purposes;
- Downloading or using any content that may contravene Copyright or Intellectual Property, unless you have express permission to use this material;
- Unreasonable personal use of RGF IT.
- Any use that may compromise the security of RGF's or our client's IT equipment & systems, including:
    - Sharing passwords or creating basic, obvious, easily-accessible or discoverable passwords;
    - Making attempts to find out the password or gain unauthorised access to IT;
    - Using another RGF user's logon or passwords to access IT equipment or systems;
- Connecting, installing, or using any unauthorised hardware or other equipment or software with RGF's electronic equipment, or a client's;
- Attempting to subvert the security of any of RGF IT, attempting to subvert any restriction or control (for example, peer-to-peer, web authenticated proxy), or otherwise attempting to interfere with the operation of RGF IT;
- Attempting to download, create, or install any form of unauthorised or malicious software (for example, worms, viruses, sniffers);
- Attempting to download/install software without permission from RGF IT;
- Attempting to gain unauthorised access to or interfere with third party IT, including Internet sites, networks, computers or records;
- Removing any RGF IT from RGF's or a client's premises, without permission to do so (excludes BYOD).

If you have any questions about whether you can or should be downloading, accessing, or installing any software or information, please speak with your manager and/or contact the RGF IT Service Desk.

Use of Mobile Devices (Phones or Tablets)

Mobile Devices

RGF allows and encourages Employees to use their own mobile devices for work purposes. This prevents Employees from having to carry duplicate devices, enables individual freedom of choice (e.g. iOS or Android, features, upgrades etc.) and reduces the complexity of maintaining a fleet of mobile devices.
The use of any mobile device connected to the RGF IT systems is governed by this entire policy (and all relevant RGF policies).

Personal or private use of any technology: in the workplace, associated with, which impacts or may impact RGF, your work or the workplace, is most likely to be covered by RGF policies (e.g. Code of Conduct, Anti Bullying etc.)

Purchasing

If you wish to purchase a new mobile device, RGF may be able to assist.
Employees may elect to utilise salary sacrificing arrangements to purchase a mobile device. You will be required to complete and submit a declaration regarding work usage and may only purchase one device per year. Please refer to the Salary Sacrifice Guideline or People & Culture for further information regarding salary sacrificing.

Access

Users may only access RGF systems and data with the approval of RGF, which may be granted and revoked at any time. Access via a mobile device is only possible via our 'Mobile Device Management' (MDM) platform. This protects IT systems, company information as well as individual users.

Mobile Application Management (MAM)

RGF takes its data security, privacy and confidentiality obligations seriously; we handle and store volumes of confidential, commercial, personal and sensitive information.
We take additional measures, in conjunction with Users' own vigilance, to reduce the risk of:

- accidental data loss or breach
- malicious cyber-attacks, hacking
- consequence of device loss or theft
- fraud or theft

MAM connects Users with Microsoft 0365 Outlook and Office suite. MAM enables RGF to control which Users and devices can access RGF systems, as well as how they are used.
MAM enables you to completely segregate your work and personal activities and Apps on a device, whilst enabling you to move seamlessly from one to the other.
We enforce certain security practices, such as the use of at least a 4**-digit** password to access the application. We do not accept the "touch pattern" method as a substitute for a password. Finger print touch ID and facial recognition can be used as a substitute, provided your numeric password complies.
Access to corporate data must be through an approved app such as Microsoft Outlook, native apps are not supported and will be blocked. Jailbroken/rooted devices do not meet our security requirements and will be blocked.

Loss of a Device or Data

IMPORTANT: Users who lose a mobile device with company data should contact RGF IT Helpdesk **without delay**. IT will take immediate steps to protect RGF systems and data, via the MAM portal. This helps to protect you and the company from the consequence of data breach or loss.
If a device is stolen or lost entirely, RGF IT Helpdesk can remotely remove RGF systems and RGF data only. This is a crucial feature of our data protection program.
You may be charged for any damage that occurs as a result of misuse or carelessness.

Privacy

We are responsible for the private and confidential information of our clients, employees and candidates, including any sensitive information they may provide us. We take our obligations seriously; please reference the RGF Privacy Policy.
We therefore keep Company systems and data as secure as possible, including on mobile devices, to protect against data loss or privacy breaches.
We will not encroach on the privacy of Users of mobile devices via our MAM platform. We **cannot** and **will not** view personal information on your device. MAM **does not** allow RGF to see: your personal Apps, personal usage, browsing history, location, text messages or call history etc.
For full details regarding what RGF can and will view, control or delete using MAM, as well as the information we cannot and/or will not, please email SecureIT@rgfstaffing.com.au

Service Provider and Expenses

Employees should not be out-of-pocket by using a personal mobile service for work, but nor should Employees be reimbursed for their personal use or otherwise make a personal financial gain (note: Fringe Benefits Tax).
For more information, please reference the BYOD Mobile Handsets Policy.

International Travel – Calls, Texts and Data

International telecommunications charges can be hugely expensive, often uncapped. You should take care to manage these costs.
If you are required to travel overseas on RGF business, and:
You use a RGF SIM: please contact IT Helpdesk at least 48 hours ***prior*** to departure, to review roaming plans and pricing.
You use your own mobile or data service: to avoid any confusion or dispute, you should assume international calls, text and data ***will not*** be reimbursed by RGF, unless prior written approval is obtained. Better still, seek approval to pre-purchase daily capped service to cover cost of calls, data and text whilst international roaming.

RGF SIM holders who travel overseas for personal reasons should discuss with their manager whether international roaming is required for business and whether it will be provided at RGF's expense. Please reference the Travel & Expenses Policy.

Mobile Safety

For your own safety and the safety of others, you:

- must be aware of and follow the safe operating instructions associated with the mobile device,
- must follow normal safe working practices when using a mobile device, such as posture and rest breaks etc.,
- should remain attentive as a pedestrian, to avoid the serious risks caused by distraction,
- should get sufficient rest and 'down time', away from work demands and mobile devices.

RGF will not tolerate the **handling/touching** of mobile phone or a tablet by any Employee **operating a motor vehicle**; it is only acceptable to make or receive phone calls if this can be done without touching or handling the phone whatsoever. You must also obey the local road and traffic laws. Breach of this requirement, or any other safe work instruction, may be subject to investigation and disciplinary action, up to and including immediate dismissal.

Mobile Security

We deploy a range of measures to ensure the security of our IT systems, especially when accessed remotely. This protects the system, Users and the Company from various cyber risks, malicious acts, crime etc. See the Mobile Application Management (MAM) and Privacy sections for more information.
We have a shared responsibility to ensure the security and stability of our IT systems. You should take all reasonable measures to ensure the security of our systems and information.

Use of Clients' IT Equipment & Systems

If you work on a client site or use our client's IT, you should ensure that you have reviewed their policies. You are expected to comply with their policies, as well as our own. If the policies are inconsistent, you should comply with the stricter policy.

Clients' IT equipment must be used strictly for the Client's business use and ***not for any personal use*** *or RGF business use*, unless this has been expressly authorised by the client. If in doubt, you should not engage in any personal use.
If personal use is permitted by the client, you must ensure that such use fully complies with the client's policies and directions, does not impact on the performance of your duties, and is otherwise consistent with RGF's policies (including this Policy).

Blocking Access to Emails and Websites

RGF blocks access to various Internet sites. If a user attempts to access a blocked site, the user will be advised (usually immediately).

If you need to access a blocked website for work purposes, or you believe that a website should not be blocked, you will need to obtain email authorisation from your manager, before contacting RGF IT Helpdesk.

RGF may also block delivery of emails sent to or by Users. Usually an email will be sent to you to inform you that delivery has been prevented, but we are not obliged to provide such a notice.

Access to IT Equipment & Systems

When you are on Leave, RGF may restrict your access to RGF's IT.
Sometimes a manager may require access to a User's emails during Leave. Managers are encouraged to discuss and arrange forwarding of emails and access to files/folders with employees prior to the Leave commencing, where possible.
In most cases, an 'out of office' message will be sufficient. The person's manager can contact RGF IT Service Desk to set up an out of office message, when absence is unexpected.
If the person cannot be contacted, and access to the person's emails/computer system is essential and legitimate, People & Culture authorisation should be sought, for a fixed period of access, before asking RGF IT to arrange:

- Automatic forwarding of emails; or
- Direct access to the person's email/computer system

If a User has departed RGF, the manager may arrange to have that person's emails forwarded to them or another responsible person. Access to a former Employee's mailbox/calendar may be obtained by contacting RGF IT, this is subject to P&C approval.
All RGF-issued IT equipment must be returned on or before the final day of engagement to their manager. The Manager should contact the RGF IT Service Desk to arrange for the equipment to be re-allocated to another user or returned to IT. They can

also aid in retrieving equipment from employees that work remotely. Any equipment not returned to RGF IT will be charged to the managers PC.
RGF reserves the right to access, amend, and delete all files and other data (including emails) stored or recorded on its IT. This section does not limit RGF's rights regarding surveillance under the following section.

Computer Surveillance

Any material that is created, used, viewed, stored, transmitted, sent or received by you or any other User using RGFs IT (including if accessed via your personal device) may be accessed, modified, moved, monitored, logged, locked, deleted or backed-up by RGF.
Computer surveillance monitors or records the information input or output, or other use of a computer (including but not limited to the sending and receipt of emails and the accessing of internet websites).
Where legislation requires computer surveillance of 'workers' to be carried out in accordance with a policy on computer surveillance, this document constitutes that policy.
Notice of RGF's surveillance of the workplace, as required by legislation:

- RGF conducts computer surveillance, being surveillance of all RGF's IT hardware and software computer system and its use (including email and internet use);
- All Users are subject to computer surveillance;
- Computer surveillance is conducted using RGF's computer and technology systems and involves software designed to filter the use of web and email content and/or to monitor compliance with RGF's policies;
- Computer surveillance will be conducted by RGF on a continuous and ongoing basis; and,
- As part of the computer surveillance, RGF may also conduct forensic computer examinations randomly and/or to investigate a possible breach of policy.

Use of Surveillance Records

A RGF user must not use or disclose surveillance records without authority from RGF, which may be provided by Legal or People & Culture.
Surveillance records are to be stored in a secure location, and unwanted records are to be destroyed. Surveillance records are not to be used or disclosed except:

- To investigate a potential breach of: this policy, any RGF policy, Code of Conduct or the law; if it would be appropriate to take formal action against a person, should the breach be proven;
- When investigating system problems or potential security violations, and to maintain system security and integrity, and prevent, detect or minimise unacceptable use of RGF IT;

- For any other legitimate purpose related to the employment of RGF's employees or engagement of independent contractors, or any other purpose connected with RGF's business activities or functions;
- To a member or officer of a law enforcement agency for use for the detection, investigation or prosecution of an offence;
- For a purpose that is directly or indirectly related to the taking of civil or criminal proceedings; or
- Where it is reasonably believed to be necessary to avert an imminent threat of serious violence to persons or of substantial damage to property; or
- With the RGF user's permission;

If you are provided with access to a client's IT, your email and internet use may be monitored by the client on an intermittent and ongoing basis in accordance with a policy of the client.
Data obtained through surveillance may be used by RGF or the client for any of the above purposes, or as otherwise permitted by legislation. Data may be shared between RGF and the client for these purposes.
This policy constitutes notice to you of computer and other monitoring activities undertaken by the client for the purpose of any relevant legislation.
If a manager has concerns regarding excessive or inappropriate computer use, they should contact People & Culture to discuss the issue.

Consequences of Breaching this Policy

Any breach of this policy may result in disciplinary action up to and including termination of employment, or, for non-employees, other appropriate sanctions and action being taken by RGF.

Suspected breaches are investigated in accordance with relevant RGF's policies.
RGF may seek reimbursement from you for the cost of any private telephone calls, excessive internet usage or any other expense unreasonably incurred by you using RGF IT.

Review of this Policy

Revision of this Policy shall occur if any of the following circumstances arises or else, every two (2) years:

- there is an update to the Recruit Global ISMS,
- there is a change to applicable laws, regulations, standards, or controls

The delegated authority policy outlines who can propose changes and approve this policy.

Document Control

Version	Author	Changes	Date	Approver	Date Valid
1.0	CMG IT and P&C	CMG Policy	June 2014	P&C	June 2014
2.0	Michael Gavin	New RGF branding, removed Social Media, updated remote working and asset management	16/05/2023	CEO	Oct 2023

Related Polices

- Code of Conduct
- Workplace Diversity Policy
- Discipline and Misconduct Policy
- Privacy Policy
- Whistleblower Policy
- Data Breach Response Plan
- BYOD Mobile Handsets Policy
- Travel & Expenses Policy
- Flexible Work Arrangements Policy
- Overseas deployment policy
- Delegated Authority Policy

RGF Staffing APEJ
Level 13, 345 George St, Sydney, NSW 2000
T +61 (02) 9269 8666
info@rgfstaffing.com.au
www.rgfstaffing.com.au
ABN : 84 603 568 403