



CORP POL-0015

Fraud, Waste, and Abuse (FWA) Policy

December 2023

Version 1.0



TABLE OF CONTENTS

Table of Contents.....	i
1. Introduction.....	1
1.1 Purpose	1
1.2 Audience	1
1.3 Responsibility.....	1
1.4 Scope.....	1
1.5 Terms and Definitions	1
1.6 Training and Awareness.....	2
1.7 Confidentiality Statement.....	2
2. General FWA Policy and Reporting.....	3
2.1 General Policy	3
2.2 Reporting FWA (i.e., Whistleblower Policy)	3
3. Specific Policies Related to FWA.....	4
3.1 Conflict of Interest.....	4
3.2 Anti-Bribery and Anti-Corruption Policy	5
3.3 Modern Anti-Slavery Statement and Policy.....	6
3.4 Insider Trading Conduct.....	7
Appendix A: Revision History	9



1. INTRODUCTION

Integrity is at the core of Ready Computing (“Company”) and all of its business operations. We take all matters of FWA very seriously, as a means to staunchly defend our Company's reputation. Although Ready Computing has 100% confidence that it has hired and employs a workforce that believes in, and practices, the same values described in our *Corporate Culture Policy*, and in order to show our due diligence, we have developed a series of interconnected programs and policies supported by documented procedures, processes, and controls to produce evidence-based records that we regularly audit to ensure that fraud, waste, and/or abuse are not occurring..

1.1 Purpose

The purpose of this Policy is to define the FWA requirements that all Personnel must follow.

1.2 Audience

This Policy applies to all Personnel.

1.3 Responsibility

All Company Personnel are expected to read, understand, and comply with the information contained within this Policy and complete any training required. All Company Personnel are equally responsible for the prevention, detection, and reporting of FWA. Company Personnel are required to avoid any activities that could lead to, or imply, a violation of this Policy.

If anyone has reason to believe or suspect that an instance of FWA has occurred, or will occur in the future, you must refer to [2.2 Reporting FWA](#) and follow the requirements therein.

1.4 Scope

Some Company Personnel are located outside of U.S. where this information may be duplicated, or supersede what has been written in this Policy. When this may be the case, Personnel are instructed to follow the most applicable Policy for their locale, and use this Policy as supplemental.

1.5 Terms and Definitions

Term	Definition
Abuse	Excessive or improper use of a thing, or to use something in a manner contrary to the natural or legal rules for its use (in financial or non-financial ways).
Bribery	Is a form of Fraud and is defined as the act of offering, giving, promising, asking, agreeing, receiving, accepting, or soliciting something of value or of an advantage to induce or influence an action or decision.



	Specific forms of Bribery include Facilitation Payments/Kickbacks, defined as "payments made to a government official with the intent of expediting or facilitating an administrative process."
Fraud	Wrongful or criminal deception with intent to result in financial or personal gain (e.g., misrepresenting facts, making false statements, forgery, or concealing information).
Waste	Thoughtless or careless expenditure or mismanagement of resources (e.g., time, money, etc.) to the detriment (or potential detriment) of another. Incurring unnecessary costs from inefficient or ineffective practices, systems, or controls.

Table 1: Terms and Definitions Table

1.6 Training and Awareness

The Company makes a reasonable effort to train all Personnel and those who conduct business with Ready Computing through various means.

For Ready Computing Personnel, the Company:

- Has a Learning Management System (LMS) through which it assigns e-learnings.
- Provides this Documentation in a virtual location that is accessible to all Personnel
- Communicate the release and subsequent updates made to this Policy, at least, annually.
- Conducts optional training via a virtual meeting platform.

For those that conduct business with Ready Computing, the Company:

- Requires formal acceptance of Company Policy through flow-downs in legal contracts.

1.7 Confidentiality Statement

The information contained within this document is intended for either internal or external use but is confidential in nature. Any review, retransmission, dissemination, or other use of the information in this document by persons or entities other than approved Company Personnel is strictly prohibited. Any unintended recipient of this document is expected to immediately contact the Company and destroy any copies of this document.



2. GENERAL FWA POLICY AND REPORTING

2.1 General Policy

Engaging in any form of fraud, waste, or abuse is strictly prohibited. Any Company Personnel who have knowledge of FWA, or who has good reason to suspect that such conduct has occurred, must immediately report the activity or suspicion following the guidance in the next section.

2.2 Reporting FWA (i.e., Whistleblower Policy)

The following must be used for all forms of FWA defined throughout this Policy.

2.2.1 Reporting FWA Internally

- Any member of Executive Leadership (i.e., CEO, CFO, COO, etc.)
- Jake Pugh, General Counsel and Compliance Officer: jake.pugh@readycomputing.com
- Legal Department: legal@readycomputing.com
- Human Resources: HR@readycomputing.com

2.2.2 Reporting FWA Externally

Company Personnel should make every effort to do their due diligence to internally report FWA or suspicion of it. That said, and under extreme circumstances, Company Personnel may also report it externally to:

- Any international governmental body relevant to your location.
- The Department of Homeland Security and/or Health and Human Services
 - www.oig.dhs.gov / 1-800-323-8603 Toll-Free
 - www.oig.hhs.gov/report-fraud / 1-800-HHS-TIPS
- A member of Congress or a representative of a committee of Congress
- The Department of Justice or other law enforcement agency; a court or grand jury

2.2.3 Anti-Retaliation

Anyone reporting FWA will not be retaliated against in any manner. In addition, you will not be subject to discipline for reporting a threat or cooperating in an investigation.

- If you initiate, participate, are involved in retaliation, or obstruct an investigation into conduct prohibited by this Policy, you will be subject to discipline up to and including termination.
- If you believe you have been retaliated against, immediately report it to the HR Department.

2.2.4 Additional Resources

Refer to the [Company Intranet](#) for more information.



3. SPECIFIC POLICIES RELATED TO FWA

3.1 Conflict of Interest

There are two types of Conflict of Interest relevant to Ready Computing:

- Personal Conflicts of Interest
- Organizational Conflicts of Interest

3.1.1 Personal Conflict of Interest

Personnel have a legal duty of good faith and loyalty to the Company and should always act in the best interest of the Company. To avoid potential conflicts of interest, Personnel should avoid activities that could reasonably put them in a conflicting situation. A personal conflict of interest occurs when the Personnel's financial or personal interest, or interests of a family member interferes with, or even appears to interfere with, the Company's legitimate business interests or with the Personnel's ability to perform work-related duties objectively and effectively. If ever in doubt, Personnel should use any of the communication mechanisms provided in section [2.2 Reporting FWA](#).

3.1.2 Organizational Conflict of Interest in Government Contract Work

An organizational conflict of interest may occur when the Company's past or current projects, relationships, or knowledge of non-public information gives the Company bias or an unfair competitive advantage. As a result of the other projects, relationships, or knowledge, the Company may be in danger of being unable to provide the government with objective advice, assistance, or performance of work. Therefore, Personnel involved in a government proposal and/or project are expected to immediately report any recognized, existing, or potential organizational conflicts of interest using any communication mechanisms provided in section [2.2 Reporting FWA](#).

Hiring Government Personnel

Special concerns apply to hiring or retaining former and current government Personnel. Additionally, special constraints apply to communication concerning the employment of procurement officials. Therefore, the Company and Personnel shall:

- Not conduct any discussions regarding, or make any offer of, future employment without first clearing such action with the Company's Founder and CEO, Chief Financial Officer (CFO), and/or Legal Department; nor
- Add a former government Personnel onto a federal contract project without first clearing such action with the Company's Founder and CEO, CFO, and/or Legal Department.

3.2 Anti-Bribery and Anti-Corruption Policy

Ready Computing has a zero-tolerance policy regarding bribery and corruption. It is committed to acting with integrity in all its business dealings and relationships and implementing and enforcing effective systems to prevent bribery and corruption.

Note: This Policy does not form any part of a Company Personnel's contract. The Company may amend it at any time to improve its effectiveness in combatting bribery and corruption.

3.2.1 Compliance with Laws

The Company and Company Personnel must obey all applicable laws and regulations that affect the Company's business. This Policy covers laws relating to anti-bribery and corruption in the U.K., including the Bribery Act 2010 ("UKBA"), and all associated laws and regulations in the U.S. Personnel are responsible for:

- Having a general understanding of laws governing Personnel's areas of responsibility.
- Seeking guidance prior to taking action if there is any doubt concerning the application of a law or regulation.
- Reporting any instance of, or suspicion of, anything related to this Policy.

3.2.2 Reporting Bribery and/or Corruption

The following sections provide a non-exhaustive list of things to establish commonality. Please note, that using reasonable judgment is best, but if you are ever faced with a circumstance in which you have a question, need to report [Bribery](#) or corruption, or have suspicion of [Bribery](#) or corruption, please reach out to any of the following departments using any of the communication mechanisms provided in section [2.2 Reporting FWA](#).

Gifts and Hospitality

Normal and appropriate gestures of hospitality and goodwill (whether given to or received from third parties) are acceptable so long as a gift meets the following requirements:

- It is **NOT** given to any recipient who works for any governmental body.
- It is not defined as anything in the section [1.3 Terms and Definitions](#).
- It is not made with the suggestion that a return favor is expected (i.e., "quid pro quo").
- It is given in the name of the Company, not in an individual's name.
- It does not include cash or a cash equivalent (e.g., a voucher or gift certificate).
- It is appropriate for the circumstances (e.g., giving small gifts around Christmas).
- It is given or received openly, not secretly.
- It is not selectively given to a key, influential person.



- It is not above a 100 (£ or USD).
- In circumstances where it may be considered inappropriate to decline the offer of a gift, as determined by the Legal Department and/or HR Department.

Important Note: The Finance Department will keep detailed and accurate records and will have internal controls in place to declare and keep a written record of gifts and/or hospitality.

3.2.3 Facilitation Payments and Kickbacks

Accepting or making any form of facilitation payment or kickback of any nature is prohibited.

3.2.4 Political Contributions

The Company will never make any form of political donation.

3.2.5 Charitable Contributions

The Company encourages the act of donating to charities — whether through services, knowledge, time, or direct financial contributions (cash or otherwise) — and agrees to disclose all charitable contributions it makes. Company Personnel must be careful to ensure that charitable contributions made by or on behalf of the Company are not used to facilitate and conceal acts of [Bribery](#). The Company will ensure that all charitable donations made are legal and ethical under local laws and practices, and that donations are not offered or made without the Company approval.

3.2.6 Special/Extreme Circumstances

The Company recognizes that Company Personnel may face a situation where avoiding a facilitation payment or kickback may put their safety or that of their family at risk. Under these circumstances, Personnel must:

1. Keep any amount to a reasonable minimum.
2. Ask for a receipt detailing the amount and reason for the payment.
3. Create a record concerning the payment.
4. Report this incident as defined in section [2.2 Reporting FWA](#).

3.3 Modern Anti-Slavery Statement and Policy

The Company is opposed to all forms of human trafficking, slavery, servitude, forced or compulsory labor, and any other trafficking-related activities as outlined in this Policy and is committed to fully complying with all applicable international human rights standards, labor, and employment laws, rules, and regulations. Ready Computing achieves this through:

- Training and awareness via its *Corporate Culture Policy*.
- Monitoring operations and supply chain via an *Enterprise Risk Management (ERM) Policy*.
- Regular review of laws and regulations that apply to this topic.

- Documented participation in the UK Slavery Registry.

3.3.1 Supply Chain Accountability

As a condition of doing business with Ready Computing, all third parties must operate with the same principles established in this Policy. This applies to all third parties that provide goods or services to our organization and entities that the Company partners or subcontracts with. Within these third parties, this applies to all entities working on their behalf. All third parties are responsible for providing their subcontractors with these principles and ensuring they follow them.

All levels of a Company's supply chain must:

- Have effective controls to ensure that applicable law, regulation, and policy related to Modern Anti-Slavery and Human Trafficking is followed.
- Not retaliate against anyone who, in good faith, reports potential misconduct.
- Cooperate in audits, investigations, and reviews.
- Promptly report potential violations to Ready Computing.

3.4 Insider Trading Conduct

Anyone with knowledge of material, nonpublic information about a company may be considered an "Insider" for purposes of laws and statutes which prohibit or restrict insider trading ("Insider Trading Laws"). It is a violation of Company policy, and may be a violation of Insider Trading Laws, for any Personnel to:

- Trade in any securities while aware of "material nonpublic information" concerning any company, or
- Communicate, "tip", or disclose material nonpublic information to outsiders so that they may trade securities of any company, based on that information.

To prevent even the appearance of improper insider trading or tipping, it is important that all Personnel read, understand, and comply with this section of the Code of Ethics policy.

3.4.1 Material Information

"Material Information" can be considered to be any information pertaining to a company that reasonable financial personnel would consider to be important in making any decision related to investments (i.e., buy or sell a company's securities). Below are some examples of "Material Information" that Company Personnel may encounter while performing their duties.

Note: This is a non-exhaustive list.

- A significant cybersecurity incident experienced that has not yet been made public.
- Potential mergers and acquisitions or the sale of company assets or subsidiaries.

- New major contracts, orders, suppliers, customers, or finance sources, or the loss thereof.
- Major discoveries or significant changes or developments in products or product lines, research, or technologies.
- Significant changes in management.
- Actual or potential exposure to major litigation, or the resolution of such litigation.
- Significant changes in sales volumes, market share, production scheduling, or pricing.

3.4.2 “Nonpublic” Information

Information is typically considered “nonpublic” until it has been widely disseminated to the public. This can occur through any major news service. Additional provisions state that ‘the market’ should also have sufficient time to digest any information from a major news source.

3.4.3 Inquiries

Please direct all inquiries regarding insider trading to:

- The Legal Department: legal@readycomputing.com
- The Compliance and Risk Management Department: quality@readycomputing.com.

3.4.4 Penalty and Consequences

Penalties and consequences of prohibited insider trading or tipping can be severe. Violation of this Policy by any Personnel may result in disciplinary action by the Company, up to and including immediate termination for cause. Moreover, persons violating insider trading or tipping rules may also be subject to legal consequences.

APPENDIX A: REVISION HISTORY

Date	Version	Name	Description	Status
12/12/2023	0.1	Anthony Simonetta	Initial Draft that merges all existing standalone Policies into one Policy	Draft
12/13/2023	0.2	Amber Dager	Accepted redlines, reviewed and made updates.	Revised
12/14/2023	0.3	Tricia Moorehead	Accepted redlines, reviewed and made updates	Revised
12/18/2023	0.4	Olivia Reyes Anthony Simonetta	Accepted redlines, updated document, and added some additional text where needed. Approved. Added Insider Trading and consulted with Olivia.	Revised Approved
12/19/2023	1.0	Anthony Simonetta	Finalized and published for distribution and accessibility.	Final

Table 2: Revision History Table

