Russell Reynolds Associates

Internet and Electronic Tools Acceptable Use Policy

Updated June 19, 2019

Private and Confidential

Internet and Electronic Tools Acceptable Use Policy

I. INTRODUCTION

As an employee, intern, or contractor of Russell Reynolds Associates ("RRA" or the "Firm"), you have been given access to RRA electronic tools and messaging to assist you in performing your business duties. The purpose of this Internet and Electronic Tool Acceptable Use Policy ("AUP") is to provide you with notice of the Firm's administration and monitoring of its electronic tools and messaging and to establish the minimum standards for use of such tools.

Please review this AUP carefully. You are responsible for knowing and understanding its content and for exercising good judgment in your use of the Firm's electronic resources.

II. APPLICATION AND RELATIONSHIP WITH LOCAL LAWS

This AUP addresses RRA's "Electronic Tools" (any electronic system that RRA provides or pays for, such as email, voicemail, video conferencing, collaboration platforms, file sharing platforms and instant messaging, including the computer systems, devices and other hardware on which such programs run, including, but not limited to, computer desktops/laptops and portable storage devices) and the "Internet" (when it is accessed using RRA facilities and/or network). All employees, interns, contractors and other staff of RRA (collectively, "personnel") who use the Electronic Tools and the Internet (collectively, the "Systems") are bound by this AUP. Any provision of this AUP that conflicts with stricter restrictions imposed by applicable local law should be read in favor of that law.

This AUP also aligns with the Information Security Management Systems (ISMS) standards published by the International Organization for Standardization ("ISO") and the International Electrotechnical Commission ("IEC"). As a Firm, we operate an Information Security Management system ("ISMS") that conforms to requirements of ISO/IEC 27001:2013 and are also ISO certified.

This AUP does not create any rights for RRA personnel or any rights outside the scope of RRA's obligations under applicable law. This AUP is confidential and internal to RRA and shall not create any rights or entitlements of any third parties.

Your use of the Systems constitutes consent to all terms and conditions of this AUP. Violations of this AUP may result in disciplinary action up to and including immediate termination of employment or assignment.

III. GUIDING PRINCIPLES

The following principles should guide your use of the Systems:

- Only use the Systems that you are authorized to access and the resources you need to perform your role at the Firm.

- Adhere to the Firm's password policy or the statements in this AUP to protect your passwords and to secure resources against unauthorized use or access.
- You are individually responsible for appropriate use of all resources assigned to you, including the computer, network resources, software and hardware.
- Do not provide resources or other forms of assistance to allow any unauthorized person to access Firm Systems or information.
- The Firm is bound by contractual and licensing agreements with regard to third-party resources. You are expected to comply with all such agreements when using such resources.
- Do not attempt to access or provide resources to access restricted portions of the Firm's Systems without appropriate authorization by the system owner or administrator.
- Comply with the policies and guidelines for any specific set of resources to which you have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.
- Do not engage in deliberate activity to degrade the performance of the Systems deprive an authorized user access to Firm the Systems; obtain extra resources beyond those allocated; or circumvent Firm computer security measures.
- Do not attempt to bypass or delay any security control or software/system updates unless you have been specifically authorized to do so by IS Security. All requested updates should be completed within one business day of notice.

IV. BUSINESS USAGE

RRA has provided you with the Systems solely for conducting Firm business. Only minimal use of these Systems for personal reasons is permitted. Accordingly, excessive personal use of these Systems, use that violates internal Firm policies and/or the law, or use that is in furtherance of any illegal activity, is strictly prohibited. You may use RRA's Systems for reasonable and limited personal use so long as your personal use does not:

- interfere with or in any way impair job performance and/or productivity,
- disproportionately utilizes (or monopolizes) RRA resources,
- suggest or imply that RRA in any way endorses or supports any views expressed in personal email or other electronic communications,
- appears unprofessional or reflects negatively on RRA, its clients or other business partners,
- impede or interfere with the normal processing of our Systems including, but not limited to, email, servers, security, or network traffic,
- hide or misrepresent the sender of a message,
- result in message distribution to dedicated RRA lists or forums which would violate their intended use, or
- result in additional costs or fees to RRA that would otherwise not be incurred.

To avoid any potential misunderstandings, users must clearly state that the communications they make are made in a personal capacity and are not to be attributed to RRA.

V. APPLICATION OF RRA POLICIES

RRA's internal policies, including but not limited to RRA's Equal Employment Opportunity and Harassment Free Workplace Policy, apply when using the Systems. Accordingly, under no circumstances should you use the Systems to transmit, download, upload, display, store, initiate, receive, access or open material that is unlawful in any manner, inappropriate, intimidating, hostile, pornographic or obscene, defamatory, fraudulent, or offensive (including but not limited to offensive material concerning sex, race, color, national origin, religion, age, sexual orientation, disability or other characteristics protected by local law). Should you receive any material that you believe violates Firm policies, consult your Area/Country Manager or Global Human Capital immediately.

VI. GENERAL CONSIDERATIONS

Confidentiality of emails and the Internet cannot be assured, even where there are password protections. Internal and external email messages are considered business records and may be subject to discovery in the event of litigation. Moreover, it is easy for recipients to forward and alter your emails and voicemails. In addition, transmissions over the Internet are never 100% secure or error free. Therefore, when creating or transmitting a message electronically, ask yourself, "Would I be content to post the contents of this email on a bulletin for all to see?"

Do not use the Systems to circumvent Firm policies or the law. When you use Firm Systems to communicate electronically or send an email over the Internet for business purposes, you are viewed as a representative of RRA. Therefore, you are expected to use the same care and judgment in an electronic communication as you would use for letters or other memoranda written on RRA letterhead.

Do not send messages which hide or mischaracterize your identity and avoid making statements that do not reflect favorably on you or RRA, or that could expose RRA to legal liability.

RRA allows you to bring your own personal electronic devices (e.g. tablets, mobile devices) into RRA facilities and use them as an RRA work-related resource. In such cases, however, due to potential security concerns, if requested, those non-RRA Electronic Tools will be provided only restricted access to the Systems. Please refrain from using unsecured wi-fi networks and copying data from RRA app on mobile devices to public apps (e.g., from Beacon mobile to One Note). Any access related questions or concerns can be addressed through the RRA Help Desk.

When your employment with RRA ends, you must arrange to make available any email records relating to your work. Any electronic devices provided to you by RRA must be returned by the last day of your employment.

VII. INTELLECTUAL PROPERTY

It is the Firm's policy that all information obtained and created during ordinary business is the Firm's property. It is strictly prohibited for any personnel to use the Systems to communicate or exchange information belonging to the Firm for personal benefit.

You are expected to protect the confidentiality of knowledge developed by the Firm and take all reasonable steps to limit exposure of the Firm's critical assets of knowledge and information to external groups or individuals. For example, encrypt or mark an email "Confidential" when it contains confidential, sensitive, or proprietary information.

No email or other files related to the business of RRA may be copied, saved, sent, or otherwise taken from RRA's premises for any reason other than to facilitate your work for RRA. Additionally, you may not store the Firm's property electronically on non-RRA cloud servers, such as Evernote, for any reason.

You may not use public cloud storage websites (e.g., Dropbox, Google Drive, Box, Personal OneDrive) to store or transmit RRA business information. If a client explicitly asks to use their corporate version, you may do so via the web version of the product. We do not allow local installation of non-RRA approved client software.

You must comply with copyright law and applicable licenses when using our Systems. Accessing sites that facilitate the violation of intellectual property rights is strictly prohibited (e.g., megaupload and rapidshare).

VIII. EMAIL

Except for relevant information transferred to clients in the normal course of business, do not transmit RRA confidential information outside of RRA or to any individual who is not an RRA employee unless the intended recipient has signed a Non-Disclosure Agreement in a form approved by the Legal Department and the information is appropriately protected during transmission.

Do not use third party email applications such as Gmail, Yahoo! or Hotmail for business or work-related communications, reproducing or sharing copyrighted materials, or disseminating sensitive information or confidential information pertaining to RRA. Wherever applicable, it is a best practice to encrypt email and documents when sending to clients to protect RRA intellectual property.

IX. SPECIAL CONSIDERATIONS FOR INTERNET USAGE

Access to the Internet is not anonymous. Sites that you visit using Firm resources are identified as having been visited by Russell Reynolds Associates. RRA may log and disclose the sites accessed using its resources to protect its interest.

Usage of the Internet to canvass broad, untargeted audiences for sourcing ideas relating to assignments for which RRA has been retained is expressly prohibited. Likewise, because RRA has a targeted marketing program, personnel may not use electronic media, such as the Internet, to communicate information about individuals at the Firm to broad, untargeted audiences (including competitors). However, it is permitted for an associate to communicate with a source via individual email when that source has already been identified by the Firm and expressed a preference to communicate with the associate electronically.

Creating or participating in websites or home pages for individual offices, sectors/practices or associates, or using the Internet to advertise positions for which RRA has been retained (or otherwise to obtain candidates) is expressly prohibited without the express written authorization of the appropriate Regional Coordinator and the Sector Leader.

You may not publish any confidential information or any content that is related to RRA or your work on Internet-facing or otherwise publicly accessible computer systems (e.g., websites) on behalf of RRA without approval from your supervisor.

Any use of social media (e.g. Facebook, Twitter) with RRA Electronic Tools or that implicates RRA in any way must comply with RRA's Social Media Policy.

The following examples are intended to illustrate the preceding general guidelines, but not limit their generality. These guidelines apply to both work-related and personal use of our Systems.

- Do not make representations on RRA's behalf or attribute opinions to RRA on the Internet unless specifically authorized and approved by the RRA Marketing Department.
- Do not post, distribute, store, or forward material that is offensive, abusive, obscene, defamatory, disparaging or threatening. Examples include: hate-material, personal attacks, racial or ethnic slurs or jokes, profanity, and any material that contributes to a hostile work environment or violates RRA policies and/or applicable laws.
- Do not post, distribute, store, or forward material that may be construed as offensive or in violation of RRA's Code of Conduct. Examples include pornography or any material of a sexual, racial, ageist or other inappropriate nature that contributes to a hostile work environment or violates RRA policies and/or applicable laws.
- Do not illegally redistribute copyrighted material on the Internet (e.g., music, video files, news articles, publications). Redistribution includes, but is not limited to, reproducing, emailing, posting, distributing, displaying, storing, selling, publishing, broadcasting, and photocopying protected material inside or outside RRA.
- Do not participate in scams (schemes to make money fast), SPAM (unsolicited mailing or postings), chain letters, solicitations (except for authorized RRA services in the ordinary course of your job duties), or illegal activities.
- Do not seek or gain unauthorized access to any Systems (whether the system belongs to RRA) by hacking, exploitation or otherwise. This prohibition includes unauthorized network and system mapping or port-scans of any Systems.

- Do not post RRA confidential information outside of RRA Systems unless expressly authorized.
- Do not comment on pending legal actions involving RRA, or its clients or competitors on the Internet unless expressly authorized.
- Do not use personal Internet Service Provider (ISP) connections to connect RRA laptops to the RRA network, except with secure connection methods expressly approved of by the IS Department.
- Do not allow visitors to have unsupervised access to the RRA internal network. The RRA internal network is only available to visitors to conduct RRA business. Visitors may use the guest network with the required password for internet access.
- Do not attempt to visit inappropriate websites using the Systems, such as those related to pornography or online gambling.
- Do not endorse RRA products or services, or those of RRA's clients, on the Internet or other electronic media (including email, social networking sites, and blogs) without authorization from the RRA Marketing Department. This restriction does not apply to re-tweets or reposting of official RRA tweets or posts.
- Do not engage in commercial or non-commercial activities using the Systems that do not further RRA business, including operating an outside business, soliciting for personal gain, charitable or political contributions, gambling and/or online auctions.
- Do not otherwise violate the law and or regulation of any federal, state or local jurisdiction in which RRA operates.

X. SPECIAL CONSIDERATIONS FOR ELECTRONIC DEVICES

Keep portable devices secure. You must take reasonable care to store and transport laptops, smart phones, and tablets whether on or off business premises, or as directed by the IS Department. You must limit the amount of RRA confidential information, personal data, or data assets you download to, or save on, portable storage devices to what is necessary to complete your work-related tasks/assignments. You must delete such information from portable storage devices when it is no longer necessary. Notify the IS Department immediately if any portable devices are lost or stolen. The IS Department will remotely remove RRA information from the device if notified it has been lost or stolen or upon termination of your employment or assignment.

The technology platform used at RRA allows access from various mobile devices to RRA email, contacts, calendar and other RRA applications. The information below outlines key points for those personnel wishing to set up email, contacts or calendar and application functions on such devices. It is imperative that the points below are understood and agreed by the personnel before setup commences.

- IS will provide individuals with the steps required to set up RRA email, contacts and calendar on the device.
- Personnel should back up personal files on the device on a regular basis. Where possible, the most recent version of software should be on the device from the manufacturer.

- Upon termination of employment or assignment, devices with RRA applications will be "wiped" and ALL RRA DATA on the device will be deleted.
- To protect the integrity of the RRA data held on the device, RRA will enforce password protections on the device. If the password feature is not supported by the device, RRA applications will not be activated. The password feature must always be maintained on the electronic device.
- Personnel must report to the IS Helpdesk immediately if a device is lost or stolen. If the lost or stolen device has been set up to receive RRA data, the device's access to RRA applications will be removed immediately and a "wipe" command will be sent to the device that will delete ALL RRA DATA on the device.
- Personnel must install and activate the Lookout Work app.
- RRA does not provide technical support for non-RRA devices. Personnel should deal directly with the hardware manufacturer or retailer.
- Installation of non-standard RRA software on an RRA owned electronic device is prohibited.

XI. MONITORING USE OF RRA SYSTEMS

The Systems and the resources to access the Systems are the property of RRA, unless restricted by applicable law. Likewise, you have no expectation of privacy when using these Systems unless specifically granted to you under applicable law. Accordingly, RRA, in its sole discretion, may restrict your ability to use one or more of its Systems without prior notice and may monitor, review, retrieve, access, delete, record, log, and disclose to any third party any matters, information, electronic documents or communications stored in or related to the Systems, the use and contents thereof, and the sites accessed on the Internet.

RRA may choose to monitor its Systems for any reason permitted by applicable law, including without limitation: (i) preventing illicit, illegal, or defamatory acts; (ii) ensuring the security and safety of the Firm's personnel, facilities, and networks; (iii) protecting the interests of the Firm; (iv) ensuring compliance with internal policies and the law, and investigating and detecting breaches of the same; (v) ensuring the security and/or good working of the computer systems network, including control of the costs related thereto, as well as the physical protection of the Firm's installations; (vi) ensuring respect in good faith of the rules of use of the System, computers, networks, and other RRA facilities; and (vii) establishing the existence of the facts and legal claims or defences relevant to the Firm. Always make sure that anybody outside the RRA organization with whom you may be communicating - clients, suppliers, sources, your friends, family, etc. - are aware that if they are communicating with you through RRA's Systems, their communications may be monitored, recorded, tracked, filtered and otherwise processed.

RRA reserves the right, but has no duty, to so monitor without permission or notification to any personnel unless required by applicable law. Therefore, you should avoid storing electronic documents or communications of a non-work-related nature within RRA's Systems.

To the extent permitted by applicable law, RRA may take immediate disciplinary action based on the results of its monitoring, including immediate termination of employment or assignment.

Use of passwords, marking messages as "private", or other security measures do not in any way diminish RRA's rights to access or monitor materials on its Systems, or expand any privacy rights of personnel in the messages and files on the system. Indeed, please note that even electronic documents or communications that are not work-related may be subject to the monitoring and access described in this policy in RRA's sole discretion, and your personal use of the Systems will be construed as consent thereto, if applicable law permits it. RRA may also override any applicable passwords or codes to inspect, investigate, or search personnel's files and messages. Deleting messages or files will not truly eliminate the messages from the System because messages are stored on a central back-up system in the normal course of data management for as long as necessary to protect RRA's legal, contractual, and business interests. You should be aware that independently of any targeted monitoring actions, RRA routinely keeps logs of erased files, network, instant messaging, email and Internet activity allowing RRA, in its sole discretion, to recreate files, messages, and web browser sessions even after network sessions have ended or a file has been closed or deleted. RRA reserves the right to delete any unauthorized programs or files.

XII. PERSONAL DATA

Electronic documents and communications created, received or transferred via the Systems may include data that personally identifies you, such as name, address, username, IP address, job title, websites accessed, email content, etc. RRA processes such data to provide you and the company with IS resources and support, as well as the reasons specified in (i) through (vii) in "Monitoring Use of RRA Systems". This personal data, and the document or communication of which it is a part, may be shared between different departments of RRA (including IS, Legal and HR), both within and outside of your country, on a need-to-know basis for legitimate business reasons. It may also be transferred to outside third parties such as (i) information technology service providers (for the purposes of providing users with the Systems), (ii) external advisors (law firms, auditors, etc.), or (iii) public authorities (for instance, during investigations of mergers or acquisitions or criminal investigations). All third-party transfers are subject to mandatory data privacy regulations and appropriate safeguards, as may be required by law, such as data transfer agreements. We take reasonable steps to protect your personal data from loss, misuse, and unauthorized access, disclosure, alteration, and destruction.

Depending on the jurisdiction in which you reside, you may be entitled to request from RRA information regarding personal data relating to you that is processed or make corrections in case of incorrect personal data or personal data that is processed incorrectly. Please review the Staff and Applicant Privacy Notice for additional details or contact privacy@russellreynolds.com with any questions.

XIII. RECORDS RETENTION

RRA has implemented appropriate limited retention periods for information collected through monitoring and stored under this AUP. These retention periods are in accordance with applicable legal requirements

and RRA's business needs, having regard for the nature of the information collected and the purposes of such collection. In any event, the information collected through monitoring will not be held any longer than required by law or necessary for the pursuance of RRA's legitimate organizational, technical and security interests

XIV. SECURITY

Networked computers have automatic virus checking software and firewalls. Nevertheless, security cannot be absolutely guaranteed. Therefore, if you have any suspicions about the safety of a file, delete it without opening it. Do not open emails or instant messages from unknown sources. If you become aware of a virus warning or suspect something is wrong in any way, contact the IS Helpdesk immediately - do not commence warning other internal and external bodies or individuals. If the system is compromised, the IS Client Services team will issue the usual warning email with any specific instructions.

If you lose your mobile device that is registered with RRA or you lose your laptop, contact IS Client Services immediately so proper action can be taken to protect the intellectual property of the Firm.

Do not write down or divulge your password to anyone. Nobody from RRA will ask for your password. If, for any reason, IS support staff needs to sign in to your system as you, they will change your password and you will have to change it upon next log in. It is your responsibility to safeguard any password or user ID you use to access the Systems and to notify the IS Client Services if you ever suspect that your password or user ID has been compromised. If someone calls you claiming to be personnel of RRA who needs your password, verify their identification by asking where they can be reached. If you are in doubt, call the RRA Chief Information Officer to confirm whether the individual is authorized to receive your password.

XV. ADMINISTRATION

This AUP is subject to change at the discretion of RRA without notice. You will be informed of any changes that have been implemented and, from time to time, will be required to acknowledge and consent to this AUP. Your use of the Systems constitutes consent to all terms and conditions of this AUP.

Violations of this AUP should be reported to Human Capital or the Legal Department. Violations of this policy may result in disciplinary action up to and including immediate termination of employment or assignment.

Please contact Eric Allen, General Counsel (212-716-7094 or eric.allen@russellreynolds.com) or Matthew Herman, Associate General Counsel (212-590-0486 or matthew.herman@russellreynolds.com) with any questions about this AUP.