Reward Gateway Acceptable Use and IT Policy

Classification – Confidential

May 2018 – Version 2.5

RewardGateway
the employee engagement people

265 Tottenham Court Road
London
W1T 7RQ
UK

Table of contents

Document purpose

This document describes how we should use our business information systems, including the Internet, Intranet, and all other related computer equipment – and there's a lot of it! Software, operating systems, storage media (USB and hard drives), network accounts, email, web services, remote access services, telephone systems, and other 'virtual' services which are provided by Reward Gateway.

We all need to be careful and exercise common sense. Inappropriate use of any of our system exposes Reward Gateway to risks including virus attacks and potentially, legal issues.

We will respect your privacy, including when you use company equipment.

Technology, in particular instant messaging and social media has completely changed the way we communicate in our personal and professional lives. The old ways of thinking and working are no longer valid.

We believe in an individual's right to privacy and we don't think that employment with us should limit that. Unless required by law or by a formal investigation agreed by our Group Director of Product & Client Success in Leadership, we will not interfere, snoop, pry or read the communications of any employee even when made during work time or on work equipment.

All email and instant chat conversations sent and received through your Reward Gateway account are backed up and retained for 7 years, even if you delete them. So whilst we would not unduly pry, if you wish to have complete confidentiality for your personal communications then use an alternative account or messaging system.

Software usage

Software, including any 'shareware', shall not be installed on Reward Gateway computers without IT approval.

Do not download or install any software if unsure of its origin or security.

This isn't intended to prevent anyone from using and sharing new tech, but we use many different systems and the intention is to protect us against illegal or malicious downloads.

Please, ensure you download routine updates to the standard software on Macs and PCs when prompted. In addition, IT will facilitate the patch process by using remote management tools.

Computer usage

You're personally responsible for protecting your laptop against theft. As well as the secure storage of information stored in the laptop based on IT support's instructions.

Storage of personal data or credit card information on the laptop is strictly prohibited.

If you lose or have your laptop stolen, please, tell IT support and your Line manager immediately. Also, reporting it in our Information Security Event system.

Your computer needs to be in good working order too. If it isn't, tell IT and they can sort it out. The use of own equipment for daily work is not allowed unless compliant with BYOD policy.

Email communication

Be sensible when using email. Think about what you're sending. Would a face to face conversation or a telephone call be better? Perhaps even a video call or instant message?

Before you write an email, think for a moment:

- Would you be happy for it to be made public and what would our customers think if they saw your email? We've all sent something to the wrong person, so check you've put the right person in the 'To' box before pressing 'Send' – and don't 'Reply to all' unless necessary.
- The IT Administrators have access to all employees' email boxes. They will only use this access if absolutely necessary. For example, as part of an HR or legal investigation, or if someone takes sudden unplanned leave and a work situation requires your manager to access information.
- If we ever have to look at someone's behaviour because it's deemed/or has been complained about – email content can also be taken into account. If you're unsure about how your email will be perceived then don't send it.

Also, be careful with any emails from unknown senders claiming to own an RG trademark in Mongolia...or anything similarly bizarre! We filter a lot into spam, which you can see in your Gmail, but sometimes, the odd email will get through. Report them to the InfoSec team and mark them as spam within Gmail.

Think about the security level of the message.

Email should never be used to send or receive confidential information or Personal/Employee data. We have and use **Secure File Uploader** in Reward Manager for this.

And there are no exceptions to this rule.

If any data classified as 'Confidential' needs to be transferred via email, for instance, if the recipient doesn't have access to Reward Manager, then it must be sent as an encrypted attachment or encrypted via Wetransfer application and the password sent to the recipient by phone/SMS. Do not send the password by email.

Acceptable internet usage

Internet access is provided for business purposes. Personal use is OK so long as it doesn't expose a risk to the integrity of the systems, place unusually high demands on storage, or conflict with any other Reward Gateway policy or procedure. Please do not store all of your music, photographs, and videos on your laptop. This may cause issues with the memory. If you don't know how to store your personal pieces in the cloud then IT can help you.

Remember that while working in the office you must ensure you are connected to **Foxpass** WiFi network. The usage of other WiFi networks is prohibited.

Passwords

Passwords are the first line of information protection. This is why they are one of the most important aspects of information security. A poorly chosen password may have disastrous consequences for the organisation.

General rules that must be followed:

- Employees must not disclose their passwords or allow any other person to use their password (no matter if it's a colleague, friend or business partner).
- OKTA is our first choice for password management and application access.
- If an employee suspects a password has been compromised, this must be reported as a security event to the InfoSec team, and the password immediately changed.
- Unique passwords must be used for each system and application.
- Previously used passwords must not be reused.
- Passwords can be stored only in applications design for the purpose (i.e. OKTA, KeepassX, Vault). The store in documents or notes in electronic and paper format is not allowed.
- Passwords used in the business must:

- Have at least 12 alphanumeric characters (OKTA password must be at least 16);
- Have both upper and lower case characters (e.g., a-z, A-Z);
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./);
- Not be a word in any language, slang, dialect, jargon, etc.; and
- Not be based on personal information, names of family, previous names, place of birth, etc.

Local password managers must only be used for non-web applications that are not supported by OKTA. On Windows you can facilitate password management by using KeePassX software (www.keepassx.org). On Mac, you can use "Vault" which is built-in.

Working off-site and flexible working

We welcome flexible working and working from home, or somewhere that's not an RG space. Anyone who has chosen to work outside of the office must consider the following:

- All rules related to data protection are the same as if you were working in the office.
- Not all functionality that is accessible in the office is available from other remote locations. For example, access to some configuration screens and member's records.
- Any company material must not be made accessible to others.

Reward Gateway is not liable for loss, destruction, or injury that may occur if you've chosen to work somewhere else other than an RG office.

Physical access control

Reward Gateway's premises are accessible only with personal key fobs which are issued to each employee. Please do not lose, lend or share fobs.

If you lose or have your fob stolen, please, tell the Office Manager immediately and log it through Reward Gateway's Information Security Event system.

Visitors must sign in and out of the offices. The Visitors Book is maintained by the Office Manager. It is also the responsibility of the RG host to ensure the visitor signs in and is escorted at all times.

Since the office in Bulgaria is slightly bigger, we require visitors to wear identification badges.

The Office Manager has the responsibility to deal with shipments and deliveries and escort the delivery personnel. Ask your local Office Manager for more details.

Removable media

Removable media (USB devices, DVD/CD, memory cards) although not forbidden, should be avoided as much as possible and should be considered only if alternatives are not available.

Usage of removable media on the locked down terminals (Google Chromebooks) and employees' laptops (Mac or PC) is administratively restricted.

The following rules are mandatory for all employees and exceptions are not allowed:

- Storage/transfer of personal data or credit card information on removable media is strictly prohibited.
- If removable media is used to transfer/store data classified as 'Strictly Confidential', it must be approved by the Head of Information Security in Infrastructure. Data must also be encrypted according to Reward Gateway's Encryption Policy requirements.
- All data classified as 'Confidential' must be encrypted when written on removable media.
- Loss of removable media needs to be urgently logged as security incident.

Personal phones and tablets

Our Bring Your Own Device (BYOD) policy is available to those who want to use their own personal devices for business purposes.

Deleting files from your computer

You have to sync all business data processed locally on your computer with Google Drive and Reward Manager to make it available to your colleagues and track changes. Once you are done, please delete the files from your local hard drive.

If you put a file in the 'Trash' on your PC or Mac then it can still be recovered – even after you have emptied your deleted items folder. This is because the computer marks the file as deleted but it doesn't actually erase the file and remove it from the hard drive.

To ensure that confidential data is fully erased:

- On PCs, PGP Shredder must be used. In particular, you should use it to ensure that any old content is wiped. Also, delete any file that contains sensitive data. PCs hard drives are encrypted and once a file is deleted it cannot be restored.
- On Macs, you will either have a secure shredder in your dashboard or you'll have the option to Empty Trash when you empty your trash bin. This removes the file fully from the hard drive. If you don't get this option then contact IT support. Macs hard drives are encrypted and once a file is deleted it cannot be restored.
- No action is needed on Chromebooks because their hard drives are encrypted and once the file is deleted from the Downloads folder it cannot be restored.

Monitoring

Users should be aware that the data they transmit or create on Reward Gateway systems is deemed to be the property of Reward Gateway and is subject to monitoring. Reward Gateway retains the right to access data, electronic messages, internet usage, etc. at anytime, with or without user consent or knowledge. Users should not expect that information stored on Reward Gateway's information systems will be treated as private.

Revision history

Rev	Date	Author	Description	Approved	Date
0.1	08.06.2010	Andy Seaton	Initial draft.	Will Tracz	27.08.2010
1.0	20.08.2015	Ivan Dichev	Formatting and sections update.	Richard Hurd-Wood	20.08.2015
2.0	10.05.2016	Ivan Dichev	Update on ‘Physical access control’ and ‘Removable media’.	Richard Hurd-Wood	15.05.2016
2.1	07.07.2016	Ivan Dichev Tracy Mellor	Improvement of language expressions and rework of some sections.	Richard Hurd-Wood	20.07.2016
2.2	22.11.2016	Asen Varsanov	Revised section ‘Computer usage’.	Richard Hurd-Wood	28.11.2016
2.3	01.03.2017	Liam Jones	Rebrand and general clean.	Will Tracz	03.03.2017

2.4	17.05.2017	Ivan Dichev	Update on Monitoring	Will Tracz	18.05.2017
2.5	29.05.2018	Asen Varsanov	Complete review and update.	Adam Altounyan	29.05.2018