Royal Mail Group

Acceptable Use of I.T. Policy

Using our devices and networks safely and securely.

Policy Owner: Director of Information Governance and DPO

Date: June 2020

Overview and Policy Statement

At Royal Mail Group (RMG), we provide individuals with access to computer and telephone hardware and software, corporate networks, systems, devices and information, which we collectively describe as "**RMG Systems and Technology**" to facilitate authorised business activities. Individuals may also use such devices to a limited extent for personal purposes. Any individual who is given access to RMG Systems and Technology, or to RMG's information held electronically or on paper through being a RMG employee, casual, agent, professional interim, agency worker, contract staff, consultant, officer or any other representative, is described in this policy as a '**user**'.

When accessing RMG Systems and Technology to facilitate authorised business activities, or for limited personal purposes, the following Acceptable Use Principles should be followed.

Our Responsibilities for General use of RMG Systems and Technology

We must:

- Use them in accordance with the law of the United Kingdom at all times and, if using systems outside the UK, in accordance with local law.
- **Use strong, unique and secret passwords** to access RMG Systems and Technology, in line with the, **taking care to keep them safe and undisclosed**.
- Keep user logon details. PINs, security devices and security details strictly confidential – keep them safe and prevent others from using them. For more information, please see the Information Security and Information Governance policies.
- Be aware of phishing scams, know how to detect them on your RMG device, what to do if you receive or click on one, and how to report it.
- Use RMG's approved transfer encryption tools (Office365 Protection and MoveIT) when sharing RMG Internal, Confidential or Strictly Confidential information with authorised external parties such as customers and third parties.

Responsibilities

We must not:

- Connect RMG IT equipment to any public Wi-Fi services (e.g. coffee shops, hotels, airports etc.). Only connect RMG IT equipment to RMG Wi-Fi, password-protected domestic Wi-Fi or to RMG individually assigned mobile devices by tethering.
- Share logon details and passwords, or use another user's logon details or password.
- Upload any of RMG's Internal, Confidential or Strictly Confidential information to a device not issued by RMG.
- Send any RMG business related information to your own or a colleagues personal email account (e.g. Gmail, Hotmail etc).
- Share any RMG Internal, Confidential or Strictly Confidential information with customers or third parties without the use of approved transfer encryption tools. Should MoveIT and Office365 Protection not be appropriate, it is the responsibility of the Information Owner to work with Technology team to find a suitable solution.
- Use personal or special category personal data or commercially sensitive data in an unapproved technology.
- Gain or attempt to gain unauthorised access to any RMG Systems and Technology for any purpose or prevent access by other authorised users.
- Send or redistribute unsolicited emails ("spam") to external email addresses or to other RMG staff; forward RMG emails to personal email accounts or use any email address issued by RMG to register for personal accounts or services (e.g. social media accounts, online shopping accounts, blogging accounts).
- Use access to RMG Systems and Technology to make unauthorised public statements that might affect public perception of RMG.

Keeping RMG IT equipment safe and secure

We must:

- Take care to safeguard any equipment assigned by RMG whether inside or outside the workplace.
- Ensure that you connect your RMG laptop/ desktop computer to the RMG network at least once per month so it can receive the most current security patches and anti-virus software. PDAs must be returned to docking stations for recharging and system updates when not in use.
- Ensure that the equipment is locked or switched off when you are not present, even temporarily, (e.g. CTRL-ATL-DEL and ENTER) to prevent unauthorised access to information and devices.
- Notify the IT Helpdesk immediately on 0345 6082555 if any RMG equipment is lost or stolen.
- Follow the Leavers Guide on PSP and complete the Leavers Checklist which mandates the return of RMG IT Equipment on the users Last Day of Service (LDOS).

We must not:

- Leave RMG equipment unattended in a public place (e.g. restaurant, bar, public transport, in view inside a vehicle) or expose it to unnecessary risk of theft, loss or damage.
- Share logon details and passwords, or use another user's logon details or password.

Personal Use of RMG Systems and Technology

We must:

- Use RMG Systems and Technology principally for business purposes.
- Agree any personal usage of RMG Systems and Technology with line management beforehand. Personal use will normally only be permitted during meal breaks or before or after working hours.
- Carefully consider the content of our posts on social media sites and any reference to RMG in such messages and comments before making them. For more information, please see the Royal Mail Social Media Guide.

We must not:

- Carry out any non-RMG business, trade or for-profit activities using RMG Systems and Technology.
- Allow personal use to interfere with our roles and responsibilities.
- Store non-RMG information and items such as music or photographs on RMG IT equipment. RMG reserves the right to erase such data.
- Use social media in a manner incompatible with our duties to RMG.
- Use RMG IT and communications systems if this could result in an additional financial cost to RMG. Individuals may be asked to pay additional costs to RMG or direct to the organisation charging RMG if considered 'unacceptable use'. Examples include use of access to mobile data networks to stream or download content unsuitable for business purposes.

RMG's rights and responsibilities over user access to RMG Systems and Technology

Acceptable Use Principles are based on laws relating to communications, computing and data protection. Every user has a responsibility to use RMG systems in line with this policy. This includes use of RMG's systems as accessed through the user's own resources (e.g. domestic Wi-Fi).

In the event any use of RMG Systems and Technology presents an imminent threat to other users or to RMG's technology infrastructure, or poses a likely violation of the law or RMG policy, RMG may, without giving notice, take whatever steps it considers necessary to manage the threat and/or preserve and access data. Those measures might include changing passwords, removing access rights, disabling or impounding devices, or disconnecting specific equipment or entire network segments from RMG voice and data networks.

Users may be provided with an email address, landline or mobile telephone number by RMG for work purposes.

Access to and use of such an email address, and/or the mailbox provided with it and the use of the number and any network services such as voicemail provided with it may be withdrawn at any time, and will be removed when they are no longer employed or engaged by RMG.

The content of RMG's Systems and Technology is Royal Mail property. RMG systems and services generate records when they are used. RMG may collect, monitor and analyse records made during use of its systems, including emails sent for business and personal purposes (e.g. Data Loss Prevention activity). Network or activity monitoring must only be carried out by those authorised to do so.

Therefore, users should not expect guaranteed privacy when using these systems.

Where RMG Systems and Technology have been used improperly or in breach of the law, the content of specific electronic transactions may be monitored by authorised individuals. If a user is concerned about personal privacy, they are advised not to use RMG Systems and Technology for personal correspondence or to store personally sensitive data. Further information is available in the RMG Information Security Policy.

Users should seek advice from their manager if unsure about whether or not something complies with this policy.

Managers should refer to the following guidance if they are made aware of employees circumventing this policy; Dealing with Conduct Issues Involving Social Media Guide for managers; Inappropriate Use of Royal Mail Systems Guide; Stop Bullying and Harassment Policy and Guide, or contact the Data Protection Office for advice.

Users are permitted to use RMG's IT and communications systems for limited, incidental personal use subject to this policy.

Further guidance and documents

Guidance is also available on the Policy and Information site on PSP and the HR pages on the intranet (non-PSP users) including:

Acceptable Use – Inappropriate Use of Royal Mail Systems Guide

Acceptable Use – Social Media Guide for employees

Acceptable Use – Dealing with Conduct Issues Involving Social Media Guide for managers

Our Business Standards

Stop Bullying and Harassment Policy and Guide

RMG Information Security Policy

RMG Information Security Classification Policy

RMG Data Protection and Privacy Policy

Information Leavers Guide - PSP

For more details on how to protect our information, please go to the Think Secure section of myroyalmail.com/ThinkSecure.

ISS03 - Information Security - Data Backup and Restoration Standard

ISS04 - Information Security - Asset Management Standard

ISS05 - Information Security -Classification Standard

ISS06 - Information Security - Incident Management Standard

ISS08 - Information Security - Mobile Security Standard

ISS13 - Information Security – Identity and Access Management Standard

Reporting Concerns

If you see something, say something.

Everyone should be able to raise concerns without fear of retaliation.

You can talk to your line manager or you can Speak Up by calling the confidential helpline on **0800 090 3154** or using the on-line web-based service at; https://royalmail.gan-compliance.com/p/speakup. We will take action.

Scope of Policy

This Policy applies to Royal Mail Limited and its wholly or majority owned subsidiary companies registered in the United Kingdom. Individuals include employees, casuals, agents, professional interims, agency workers, contract staff, consultants, officers and any other representative. This Policy does not form part of any employee's contract of employment and we may amend this policy at any time.

Breach of this Policy

Users are responsible for the actions taken when using the RMG accounts assigned to them. This includes anything done by someone else, if the user has allowed another person to use any passwords, PINs, security device or security details issued to them for their sole use (which would not follow the principles of this policy). In cases where access to IT and communications systems has been through fraudulent, deceptive, or coercive means, the affected user will not be held responsible.

Anyone found in breach of this Policy may be subject to disciplinary action up to and including dismissal. Breach of this policy could expose RMG or individuals to corporate or personal liabilities.

Where a business partner granted access to any RMG system, network, device or account fails to comply with this Policy, RMG may seek to terminate that business relationship.

Getting help with this Policy

This policy is owned by the Director of Information Governance and DPO.

For advice on this document or applicable standards, contact Group Compliance and Ethics on:

- 020 7449 8302 or e-mail them at
- group.compliance@royalmail.com

Contact your line manager if you have any queries about this Policy.

Managers can look at the security guidance on the Think Secure section of the Royal Mail Intranet, or obtain advice by contacting the Information Assurance Team (Compliance).

Thinksecure@royalmail.com

For Conduct Policy queries, contact HR Advice and Support.

For web access go to: PSP

Policy Governance

Policy Reference number:	ISO2/POD/COMP/ POL/012
Version Number:	004.2
Policy Owner:	Director of Information and Governance and DPO
Policy Effective from:	June 2020
Last Review Date:	June 2020
Next Review Date:	June 2021
Approved by:	Chief Risk & Governance Officer
Approval date:	June 2020

To request changes or updates to this document, e-mail policy.governance@royalmail.com.

This document is classified: RMG – CONFIDENTIAL