Royal Mail Group

Acceptable Use Policy

Royal Mail Group provides a range of IT systems and mobile devices such as laptops and personal digital assistants (PDA) as work tools for many of our people. This policy sets out some clear rules on how Royal Mail Group expects employees to behave when using the company's information and IT systems.

Main topic areas

Getting help

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

Line managers can obtain advice by:

Calling the HR Services Advice Centre on 0845 6060603 / 5456 7100

Managers working for Parcelforce Worldwide should call 0845 6042787 / 5456 4747

Calling Group Compliance on 0207 4498301 / 5461 8301

For web access go to: https://www.psp.royalmailgroup.com

Acceptable Use Policy

Overview

The policy applies to everyone in Royal Mail Group Ltd including contractors, consultants, subcontractors and agency workers.

This includes others who work on behalf of Royal Mail Group, access or use, Royal Mail Groups information (held electronically or on paper) and technology services for business or personal use. It also applies to people who use non-Royal Mail Group equipment to access Royal Mail Group systems and information.

Within this policy ‘Royal Mail Group Ltd’ will be referred to as ‘Royal Mail Group’.

This policy is effective from 28 April 2012.

This policy does not form part of contracts of employment. Royal Mail Group reserves the right to amend this policy from time to time.

Policy statement

We all recognise the important and positive role IT systems, the Internet, intranet and social media play for work and communication. However we must also be aware that whenever we use the company’s information and IT systems, it can impact the reputation of Royal Mail Group, our employees and agents, our products and services.

It is important that everyone reads this policy and understands that we all have a duty to follow the rules and standards outlined when using Royal Mail Group’s information and IT systems for business or personal use both on-site and remotely, and also when using personal equipment/computers or equipment/ computers which are owned by someone else (in an Internet cafe, for instance).

Use of computers, IT systems, Internet, email and mobile phones

The work tools we provide to many of our employees include a range of IT systems and mobile devices such as computers, mobile phones, laptops and PDAs. These devices must not be left unattended and must always be secured when not in use.

While company policy allows some reasonable personal use of them in an employee’s own time, it does not permit:

- Downloading, installing or using unauthorised or banned software
- Unauthorised modification of computer provided hardware, software or other services
- Accessing, storing, sending, posting or publishing:
    - Pornographic, sexually explicit or other indecent, illegal or offensive material
    - Materials promoting violence, hatred, terrorism or the intolerance of others
    - Gambling, threatening or insulting material, or chain or spam emails
- Sending confidential information via email, instant messaging or via the Internet without adequate security
- Using another person’s computer or email identity or account, or accessing their files and print-outs without their authorisation
- Accessing, copying, modifying, removing or distributing company information, copyrighted or licensed materials without authorisation

Always ensure that:

- Remote connections to the Royal Mail Group network are made through Groups Virtual Private Network (VPN)
- Only business related music, videos, photographs or images are to be stored, transmitted, downloaded or uploaded to Royal Mail Group IT systems

Personal use

While Royal Mail Group IT systems are intended for business purposes, our policy does allow for reasonable and occasional personal use. This must be kept to a minimum and should not interfere with an employee's business responsibilities and the resources they are using (such as time, disc space and bandwidth).

Royal Mail Group is not responsible for the recovery of any non-business data on our systems and this data may be deleted at any time.

When using Royal Mail Group IT systems, employees must always exercise sound judgment and consider whether a communication could harm them or the organisation.

Employees must also avoid using Royal Mail Group systems to communicate personal information that might cause distress or embarrassment if viewed by unintended recipients.

Using the intranet appropriately

The Royal Mail Group Intranet

The Royal Mail Group Intranet is provided as a source of information for our employees. They may read, download or otherwise use the information on the intranet for the purpose of carrying out their role with Royal Mail Group.

Any information on the Intranet which relates to the internal operations of Royal Mail Group must not be shared externally.

Employees who are authorised by Royal Mail Group to upload content to the intranet must:

- Only upload information classified as internal and within the scope of their job role
- Take care to ensure that information uploaded is true and accurate
- Not upload content that is unlawful, harassing, defamatory, abusive, threatening, harmful, obscene, racially offensive or may be considered objectionable to those who may view it
- Take care not to upload information that infringes the rights of any third parties

Myroyalmail.com

Myroyalmail.com is an open access site. Anyone with internet access can view it. It is provided as a source of information for employees, including those who do not have access to a computer at work. Employees who are authorised by Royal Mail Group to upload content to myroyalmail.com must comply with the intranet rules listed above. In addition, no commercially sensitive or confidential information should be uploaded to myroyalmail.com unless it is behind a secure area not visible by any external third parties.

Social media

Royal Mail Group recognises that many of our employees use social networking sites. When comments are published on these sites they may reach a surprisingly wide and unintended audience, and so we must ensure that we avoid saying anything that might harm the Group's reputation and brand.

Employees must carefully consider the content of their posts and any reference to Royal Mail Group in such messages and comments before making them. They must also ensure that they:

- Do not disclose Royal Mail Group internal, confidential or secret information
- Never offer opinions or comments on behalf of Royal Mail Group without the prior approval of the Director of Communications
- Do not publish information relating to clients, partners or suppliers in a personal context
- Do not violate copyright, data protection and intellectual property rights
- Never cause offence or harass any one
- Never use their Royal Mail Group email address as an identifier
- Never alter Group brands or logos in any way
- Always treat social networking sites and activities as if they were publically accessible

Where an employee is asked to make any comment about Royal Mail Group in an external published form, such as newspaper, radio, television or a website, they must direct the request to the Director of Communications.

Royal Mail Group expects all employees to abide by the same standards of conduct and behaviour on line as they would in all other dealings.

Instant messaging

When employees use instant messaging as part of their job, they must only use the Royal Mail Group approved instant messaging facilities – Microsoft Office Communicator. They must not use alternative, non-approved systems for business conversations.

Royal Mail Group approved instant messaging services should only be used:

- With the same etiquette expected of any other form of business communication, i.e. appropriate:
  - tone and language
  - content and subject matter
  - relevance and related business information
  - clarity and brevity
- For business purposes
- For communicating non-confidential or non-sensitive information

Email, spam and viruses

Unsolicited emails (spam) and malicious code-like viruses, trojans, worms and spyware can cause a serious threat to the integrity of our IT systems and information. If employees do not recognise the source of an incoming email they must:

- Not save or open attachments
- Not click on embedded links to websites. Be particularly suspicious of links which direct them to a website and ask them to enter an ID, password or other personal information

- Not respond to emails seeking personal or financial details

If employees receive any suspicious content, they must report it to the IT Helpdesk. They must also delete offensive or commercial messages promoting or advertising goods, services or opinions.

When using email employees should ensure that:

- Email and instant messaging is not used to communicate confidential or strictly confidential information
- Auto-forwarding of company emails is not set up to external or personal email accounts or accounts of individuals no longer employed by Royal Mail Group
- Out of Office auto reply messages do not include personal contact information
- Employees who receive an email or other message, which is not intended for them, and is not deemed by the recipient as 'inappropriate' and the sender's email identity deemed 'trust-worthy', then the user should inform the sender of the email of the error and not redirect the email to anyone else

Our information

Information is a valuable asset for the Group and takes many forms. It exists in different types of media (including music) and can be distributed through a wide variety of channels.

We all have a duty to be aware of what information we are accessing, using, distributing and removing, and we must do everything we can to make sure it goes to the right people and is secure, and that it is in line with this policy.

Classification

Royal Mail Group expects employees to protect information according to its classification. Each classification defines a clear set of instructions for the appropriate storage, distribution and disposal of information. Our classification scheme has four levels; Public, Internal, Confidential, and Strictly Confidential.

PUBLIC – Information which is intended for public use, or which would have minimal impact on Royal Mail Group if lost or stolen. Examples; brochures or leaflets, information published on royalmail.com

INTERNAL – Information for internal use only and not intended for public release. Examples; group-wide communications, meetings, material on the intranet. The default classification is Internal.

CONFIDENTIAL: Information that has been assessed to be of a sensitive nature and likely to cause damage to Royal Mail Group's reputation following unauthorised disclosure. Examples; HR and payroll records, customer data

STRICTLY CONFIDENTIAL: Very sensitive information that could harm our brand or expose Royal Mail Group to significant disadvantage should it fall in to the wrong hands. Most people do not handle Strictly Confidential information. Examples: unpublished financial results.

We must manage our information correctly and ensure that:

- Information related to any person, whether a colleague or a customer, is used appropriately
- Using another person’s computer or email identity or account, or accessing their files and print-outs is not permitted without their authorisation

- Auto-forwarding of company emails is not set up to external or personal email accounts or accounts of individuals no longer employed by Royal Mail Group
- Out of Office auto reply messages do not include personal contact information
- Only business-related music, videos, photographs and images are to be stored, transmitted, downloaded or uploaded to Royal Mail Group IT systems
- Employees who receive an email or other message which is not intended for them should redirect it as appropriate. If the message contains confidential information, they have a responsibility not to act on or disclose that information

When working with any Royal Mail Group information ensure that:

- A screen saver is activated (Windows <L> or <CTRL><ALT><DEL>, Enter) when leaving a computer unattended so that data on the screen is not visible by others

For information classified Internal employees must;

- Only share it with colleagues and third parties who are authorised to receive it
- Be vigilant when sending information via email. Check beforehand that the recipient details are correct
- Lock it away in a secure place and never leave it unattended
- Only use Royal Mail Group's approved instant messaging facilities and internal mail to share non confidential information. Do not use consumer-grade systems to share it e.g. Gmail email or messenger
- Ensure information related to any person, whether a colleague or a customer, is used appropriately and with their explicit consent
- Be sensitive to discussing it in public areas where you can be overheard.

For Confidential and Strictly Confidential information employees must also:

- Be authorised to email, copy distribute or upload it
- Encrypt it when storing on a computer, sending by email or storing to a removable disk, CD, DVD, memory stick or other external storage device
- Dispose of it in the appropriate manner, shred it or place it in a confidential waste bin.

Monitoring

Although online presence is not actively monitored, the volume of network traffic and Internet use is, along with Internet sites visited. Email communications are also recorded and retained. Telephone numbers called and the duration of calls from Royal Mail Group landlines and mobile numbers are also recorded and retained.

Where Royal Mail Group IT systems have been used improperly or in breach of the law, or if we need to assist the legal authorities, we will extend this monitoring to the content of specific electronic transactions. Only authorised individuals can access this information.

If an employee's data has been accessed in their absence – unless this is to comply with the law or assist the legal authorities – they will be notified on their return of the reasons for the access. They will also be told who had access to the information and what was disclosed.

If an employee is concerned about personal privacy, they are advised not to use Royal Mail Group IT systems and equipment for personal correspondence or to store personally sensitive data.

Non-compliance

Failure to comply with this policy may prevent future use of Royal Mail Group IT systems and may result in investigation and disciplinary action under our Conduct Policy.

Serious breaches may lead to dismissal for gross misconduct for employees or termination of contract for contractors and agents. Any breach of the law may also result in criminal prosecution or civil action.

Individuals have a responsibility to report to their line manager any breaches of this policy or any unauthorised use they are aware of. This includes inappropriate postings about Royal Mail Group, its employees, customers, partners or suppliers on the Internet or intranet.

Where to go for further information

The ‘Getting help’ box on the front page of this policy tells you where to find further information.

Guidance is also available on the *HR pages* on the intranet and the *Policy and Information site* on PSP.

In the event of any inconsistency between this policy and the supporting documentation the terms of this policy take precedence.

Forms

There are no forms applicable to this policy.

Related documents

For more details on how to protect our information and access our Information Security Policies, please go to the Information Security Knowledge Zone at:

http://iplatform.intranet.point/infosecurity

Glossary

Computer virus

A small software programme that can copy itself and is designed to spread from one computer to another and interfere with its operation; otherwise known as malware.

Email

A method of exchanging electronic messages across the Internet or other computer networks.

Encryption

The process of converting information into a format that cannot be easily understood by unauthorised people.

Information classification

Criteria used to decide which level of classification is appropriate based on the purpose and sensitivity of the information.

The Royal Mail Group information security classification scheme consists of four levels: PUBLIC, INTERNAL, CONFIDENTIAL, STRICTILY CONFIDENTIAL

Instant messaging

A system for real-time electronic messaging on the Internet or over networks.

IT system

Broadly defined and includes but is not limited to: computer networks, Internet facilities, instant messaging systems, laptops, desktops, Personal Digital Assistants, podcasts, forums, blogs, message boards, social communication websites, newsgroups, remote access facilities and all communications through such systems.

Personal Digital Assistant (PDA)

Blackberries, smart phones and other similar equipment used by Royal Mail Group employees.

Removable media

Computer storage which can be removed from the computer without having to power off. Includes USB flash drives, optical discs, Blue-ray discs, DVDs, CDs, memory cards, floppy discs, magnetic tapes and paper data storage.

Social Media

Social media is the term used to describe forms of electronic communication through which users create online communities to share information, ideas, personal messages and other content.