Royal Mail Group

Social Media

Guide for employees

This guide outlines the standards of behaviour expected from all employees when using social media as part of their job for Royal Mail and also for personal use where it impacts Royal Mail's business

Main topic areas

Getting help

Contact your manager if you have any queries about this guide.

Managers can obtain advice by:

Calling the HR Services Advice Centre on 0345 6060603 / 5456 7100

Managers working for Parcelforce Worldwide should call 0345 604 787 / 5456 4747

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

Social Media

Guide for employees

Purpose and scope

Royal Mail Group recognises that many of its employees use social networking sites both in a personal capacity and sometimes as part of their job if the role requires it. Social media tools play a positive role in everyday life, but can also be damaging to both businesses and individuals if used inappropriately.

The purpose of this guide is to provide guidance for employees (including consultants, contractors, agency workers and casual workers) and managers to help protect them and Royal Mail from the pitfalls of using social media.

It also provides details of the behaviours and standards expected of all Royal Mail Group employees whenever they use social media tools, either as part of their job at Royal Mail or in a personal capacity.

This should be read in conjunction with the Acceptable Use Policy, Our Business Standards and the social media information on the 'Think Secure' pages of myroyalmail.com - https://www.myroyalmail.com/thinksecure/social-media.

What is social media?

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

Some examples of social media tools are:

- Blogs
- Wikis e.g. Wikipedia
- Social networking sites e.g. Facebook, Twitter, YouTube, Bebo, Second Life, Instagram, WhatsApp and Snapchat
- Podcasts
- Message boards
- LinkedIn
- Workplace by Facebook (internal platform for RMG)

Risks of using social media

There are risks to both Royal Mail's business and individuals when using social media.

Royal Mail needs to make sure it is protected from:

- Internal, Confidential and Strictly Confidential company information being leaked externally
- Serious damage to Royal Mail's reputation, brand and business
- Potential claims for defamation, discrimination or harassment
- Legal action for breaches of copyright laws

Employees who use social media are personally at risk of:

- Claims for defamation, discrimination, harassment
- Conduct action under the Conduct Policy for breaches of the Acceptable Use or Stop Bullying and Harassment policies

- Identify theft
- Damage to personal property
- Personal harm

General advice for using social media in both work and personal lives

When using social media both in a business and personal capacity, employees should be mindful of the following:

- Employees are personally liable for what they communicate on social media. Any information will stay online for a long period of time and may reach a very wide and often unintended audience
- There is no such thing as a private social media site despite privacy settings. Once published online, the user's control is lost as comments can be forwarded or shared by other users

Employees should:

- When deciding to make a post online, consider whether the post could be used against them in the future
- Be familiar with Our Business Standards and how it impacts social media use
- Consider whether they would feel comfortable saying the same thing offline as they would online
- Make sure they follow the guidance provided in this document
- Let their manager know if they see content on social media that could be harmful to Royal Mail's business

Employees must ensure they:

- Avoid saying anything that might seriously damage Royal Mail's reputation and brand
- Do not put themselves or the business at risk when using social media

To help managers and employees be clear about what actions on social meda could seriously damage Royal Mail, a number of principles are set out below.

Shared principles for using social media in work and personal lives

The following principles apply to employees using social media in both a work and personal capacity:

- Employees must not use social media to make defamatory or discriminatory comments; neither should they use it to harass or bully
- Employees should not display behaviour online which may cause offence to other employees, customers or clients of Royal Mail Group, that could subsequently cause serious damage to the company
- Internal, Confidential and Strictly Confidential information about Royal Mail Group must never be disclosed on any social media sites. Disclosure of such information may amount to gross misconduct under the Royal Mail Group Conduct Policy. It may also be a criminal offence
- Employees must not make comments on behalf of Royal Mail Group without prior consent the Director of Strategy and Communications
- Employees must not take or distribute images (including videos) inside any Royal Mail Group sites. By disclosing such images, employees could put their colleagues; themselves and Royal Mail's business at risk Employees of Royal

Mail Group are bound by the Official Secrets Act or Personal Declaration, which would have been signed when starting employment. This is a contractual document which applies during and after employment with Royal Mail Group and so any information should not be disclosed without prior authorisation

- Information gained in the course of employment relating to other Royal Mail employees, clients, regulators, shareholders, partners or suppliers should not be published, unless their written approval has been given
- Copyright and fair usage restrictions (where some limited activities are allowed that don't infringe copyright law) should be respected and prior permission should be given to use copyright protection material. The unauthorised use of copyright may result in legal action
- If an employee is asked to make any comment on behalf of Royal Mail Group they must direct the request to the Managing Director of Corporate Affairs, Regulation, Marketing and Customer Experience rather than providing a response themselves
- Avoid making damaging or libellous comments about Royal Mail Group and its products. If an employee has concerns about serious wrongdoing within the business (such as fraud) they should refer to the Speak Up: Whistleblowing Policy. If they believe they have a genuine grievance, they should raise this with their manager or use the Grievance Policy

Key principles for personal use of social media

Royal Mail respects its employees' right to a private life. The company recognises that many employees use social media in their personal lives. While employees are not acting on behalf of Royal Mail during personal use of social media, they must be aware that they can seriously damage the company if they are recognised as being an employee or undertaking work for Royal Mail (see the section on Risks).

The Acceptable Use Policy does allow for reasonable and occasional personal use for email and internet, but social media sites should only be accessed outside of an employee's normal working hours or during their lunch break, so that it does not interfere with the efficient running of Royal Mail's business.

In addition to the General advice and Shared principles noted above:

- Employees are allowed to state that they work for Royal Mail, but their online profile (e.g. blog or Twitter name) must not contain Royal Mail Group's name
- Royal Mail Group brands or logos must not be used
- If employees discuss their work on social media sites (particularly Twitter or blogs), they are recommended to use an appropriate disclaimer along the lines of, 'The views I express here are mine alone and do not represent the views of Royal Mail Group'
- Be aware that any messages posted could be visible to other web users (e.g. Royal Mail employees, customers, suppliers who the employee is connected to), even if intended for a specific person or group of people. Employees are advised to check privacy settings regularly as sites such as Facebook have a tendency to adjust them when they make updates
- Employees should be security conscious by avoiding publishing their personal contact details where they can be accessed and used widely by people they did not intend to see them. By restricting the amount of personal information they can help protect themselves from identity theft, damage to their property, or personal harm. Social networking websites allow people to post detailed personal information such as date of birth, place of birth and favourite football

team, which can form the basis of security questions and passwords

- Employees are responsible for their comments and contributions. Before posting a comment, video or image, they should think about how they would justify their reason for publishing it, making sure it is in line with the Acceptable Use Policy

Key principles for use of social media for Royal Mail's work

Employees who use social media as part of their job at Royal Mail – e.g. Workplace by Facebook, RMG's internal social media platform, RMG's WhatsApp– can access social media sites in moderation during working hours as long as they adhere to the relevant guidelines and policies.

In addition to the General advice and Shared principles noted above, in any communications that employees make as part of their job at Royal Mail, they must:

- Make sure the communication has a purpose and benefit for Royal Mail
- Get permission from their manager and the either Beth Longcroft or Ian Lynch in the Corporate Affairs team before publishing a communication
- Consider the appropriate use of Royal Mail's internal social networks, ensuring the platform's primary purpose and values are adhered to – collaboration and cross-functional communication

Dealing with unacceptable behaviour

If an employee's behaviour is seen to either potentially harm their relationship with Royal Mail Group or the reputation of the business, their actions may be addressed under the Conduct Policy.

Breaches could lead to disciplinary action and in cases where the behaviour is serious enough to be considered gross misconduct this could lead to dismissal.

If the unacceptable behaviour is shown by contractors and agents it could result in the termination of a contract.

Any breach of the law may also result in criminal prosecution or civil action.

Where to go for further information

The Getting help box on the front page tells you where to find further information.

Guidance is also available on, the Policy and Information Site on PSP, the HR pages on the intranet (for non-PSP users) and the Think Secure section of myroyalmail.com.

For access to Information Security policies please go to: Group Policies intranet site.

Documents relating to this guide:

- Our Business Standards
- Acceptable Use Policy
- Acceptable Use – Inappropriate Use of Internet, Email and other Royal Mail Systems Guide for Employees
- Acceptable Use – Dealing with Conduct Issues Relating to Social Media Guide for Managers
- Systems Monitoring and Data Collection Policy
- Conduct Policy and guides
- Communications Policy
- External Digital Communications Policy
- Data Protection and Privacy Policy

Royal Mail Group

Dealing with Conduct Issues Involving Social Media

Guide for managers

This guide provides information for managers on how to deal with conduct cases relating to social media

Main topic areas

Getting help

Contact your manager if you have any queries about this guide.

Managers can obtain advice by:

Calling the HR Services Advice Centre on 0345 6060603 / 5456 7100

Managers working for Parcelforce Worldwide should call 0345 604 787 / 5456 4747

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

Dealing with Conduct Issues Involving Social Media

Guide for managers

Purpose

This guide details the process managers should use when dealing with employee conduct issues involving social media. Conduct issues will occur when employees use social media in a way that breaches the Acceptable Use Policy or Our Business Standards, causing serious damage to Royal Mail's business. This guide should be read in conjunction with the Acceptable Use Policy and Social Media Guide.

Use of social media

Employees should only access social media during work time where their job requires them to do so. There are a very limited number of employees whose role requires them to use social media as part of their job, e.g. the Communications team. Any personal use of social media sites should be kept to outside of normal working hours or during an employee's meal breaks, so that it does not interfere with the efficient running of Royal Mail's business. The exception to this is those with access to RMG's internal social networks such as Workplace by Facebook and the RMG WhatsApp group. Employees are permitted to using these in moderation during working hours, as long as they adhere to the relevant guidelines and policies.

When using social media in their own personal time, employees must ensure that their actions don't cause serious damage to Royal Mail's business and that they are in line with the Acceptable Use Policy and Social Media Guide for Employees.

The Social Media Guide sets out principles for using social media both in a personal capacity and when it is required for an employee's job.

If an employee disregards these standards, it may be classed as misconduct and will be dealt with under the Conduct Policy.

Using the Conduct Policy

Investigation

Before taking any action against the employee, the manager should carry out a full investigation. This process should be in line with the Conduct Policy.

It may be more difficult than with other forms of alleged misconduct because of the 'virtual' status and the fact that it may have happened outside the workplace. It is important that the manager does investigate and take action where required.

Managers should begin collecting evidence that may be referred to in any conduct process. This may include screenshots or print-outs of the offending material, records of any complaints received from customers or any evidence of damage caused by the posting

They should try to identify how widely the posting was communicated (i.e. whether there is unlimited access to the content or access is restricted)

They should ask the employee to remove the posting immediately.

Making a decision

When considering any potential conduct case, managers should act reasonably, taking into account the impact, or likely impact of any misuse of social media on the business. There must be evidence that the posting has had or likely to have a seriously damaging impact on Royal Mail's business. Conduct action may also be taken if the employee has potentially breached the Stop Bullying and Harassment or Equality of Opportunity policies.

Whether any formal conduct action is appropriate, and the level of that action, is likely to depend on the following factors:

- The nature of the posting
- Whether the employee's comments or conduct directly refers to the workplace
- If the employee's comments or conduct do not directly refer to the workplace, the extent to which the workplace may still be implicated by the posting
- How responsible the employee is for the posting. Did the employee post it themselves or did someone else post it and 'tag' the employee?
- How many people have viewed the posting or are likely to view it: how public the posting is?
- The employee's role within the business and their previous conduct record
- Whether the posting has any impact or is likely to have an impact on the employee's ability to perform their particular role
- Whether Internal, Confidential or Strictly Confidential Information relating to Royal Mail Group has been disclosed
- Be proportionate. Has there been any actual damage to Royal Mail's business or reputation and what evidence there is of this?
- Whether Royal Mail Group will become liable to any third parties for the content of the posting. This may occur if, for example, the posting breaches a confidentiality requirement, is defamatory or constitutes harassment of another employee
- Whether the posting can be undone or removed by the employee

The manager should also be aware of other similar cases and ensure consistency of treatment wherever possible.

Conduct that is considered to be a criminal act may also be investigated under the Crime and Investigation Policy.

Where to go for further information

The Getting help box on the front page tells you where to find further information.

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

The 'Think Secure' pages on Myroyalmail.com contain information on social media - https://www.myroyalmail.com/thinksecure/social-media.

The following policies and guides should are related to this document:

- Our Business Standards
- Acceptable Use Policy
- Systems Monitoring and Data Collection Policy
- Acceptable Use – Social Media Guide for Employees
- Acceptable Use – Inappropriate Use of Internet, Email and Other Royal Mail Systems Guide for Employees
- Conduct Policy and guides
- Stop Bullying and Harassment Policy and Guide
- Data Protection and Privacy Policy
- Crime and Investigation Policy
- Prosecution Policy

Royal Mail Group

IS02 - Group Acceptable Use Policy

Royal Mail Group provides a range of IT systems and mobile devices such as laptops, mobile phones, and personal digital assistants (PDA) as work tools for many of our people. This Policy sets out clear rules on how Royal Mail Group expects Staff to behave when using the Company's IT systems and Information (Including on personal devices).

Main topic areas

- Introduction to this Policy
- Purpose of this Policy
- Scope of this Policy
- How to comply with this Policy
- What happens if this Policy is breached?
- Further information
- Policy owner and review process

Getting help

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

Managers can obtain advice by contacting the Information Security Risk team (Compliance).

For web access go to: PSP

Owner: Chief Compliance Officer

Date: [May 2018]

Document Control Sheet

Date of Policy	Key Changes	Sections Affected	Date approved by Policy Owner	Date Uploaded Online
May 2018	Policy refresh by the Information Security Risk team (Compliance)	All	23/05/2018	24/05/2018
	Reviewed by Fiona Burgess – HR			
	Reviewed by Tracey Goulsbra – IT Audit & Controls			
	Reviewed by Simon Blanchard – Compliance			
	Reviewed by Dominic Batchelor – Legal			

A review of this Policy is carried out annually, as a minimum as part of the Policy review process. The approach, standard process and timetable in relation to the review of all Royal Mail policies is detailed in a Policy Review Guide which can be found on the guidelines sub-section of the policies section on the intranet.

Policy

Introduction to the Policy

Royal Mail Group defines 'Acceptable Use' as the use of its IT and communications systems to facilitate authorised business activities in line with other Royal Mail Group policies and procedures, or for limited personal purposes.

Within this Policy, 'Royal Mail Group Ltd' is referred to as 'Royal Mail Group' or RMG.

This Policy is effective from May 25th, 2018.

Purpose of the Policy

The important and positive role Royal Mail Group IT systems, the internet, intranet, sanctioned cloud services, and social media play in supporting the work and communication of RMG Staff (defined below), is widely recognised within the organisation. It is the purpose of this Policy to protect customers and raise awareness that misuse of the company's information and IT systems could affect the reputation of Royal Mail Group, our employees, agents, regulators, shareholders, and overall products and services, as well as potentially expose it or the Staff to legal liability.

Royal Mail Group has strict obligations as a listed company. Royal Mail Group information that is not generally available and which could have a significant effect on the value of Royal Mail Group shares must always be treated as 'Strictly Confidential' and disclosed only in accordance with RMG policies.

Details of the Information Classification Scheme of Royal Mail are noted in sub-section 7 in "How to comply with the Policy" section of this Policy (ref. Information classification).

Scope of the Policy

The policy applies to everyone at RMG including employees, contractors, consultants, subcontractors, casual workers and agency workers (herein, 'Staff') who use Royal Mail Group IT and communication systems.

This Policy applies to Staff whether they use equipment not provided by Royal Mail Group (such as personal computers), or equipment provided by Royal Mail Group, to access Royal Mail Group IT and communications systems.

This includes anyone who works on behalf of Royal Mail Group, accesses or uses Royal Mail Group's information, held electronically or on paper, and anyone who uses Royal Mail Group technology and services for business or for personal use. It also applies to people who use non-Royal Mail Group equipment to access Royal Mail Group systems and information.

Some Royal Mail Group systems and services require Staff to acknowledge this Policy before they can log on. Note however that this Policy applies even if there is no specific confirmation required by a system.

This Policy governs all IT resources and communication systems owned by or available at Royal Mail Group and use of such equipment, resources and systems including when accessed using an employee's own resources. Examples include email systems and accounts, internet and intranet access, social media (internal and external), telephones (including wired phones, mobile phones and smart phones), voicemail systems, SIM cards, tablets and/or PDAs, portable hard disks or USB sticks, laptops, printers, photocopiers or scanner, fax machines, all other associated computer, network and communications systems and hardware ('IT and communications systems').

This Policy does not form part of contracts of employment or engagement.

Royal Mail Group reserves the right to amend this Policy from time to time.

How to comply with the Policy

1. Use of IT Systems and Services

1.1 Staff may be assigned IT and communications equipment to support their work (some examples are provided in the defined policy scope above). Staff must ensure that their use of Royal Mail Group IT and communications systems is at all times in accordance with the law of the United Kingdom, and if they are using the systems outside the UK, also in accordance with the law of the place in which they use the services.

1.2 Staff must ensure that their use of Royal Mail Group IT and communications systems is in accordance with our Business Standards, with Royal Mail Group policies and procedures, and is 'Acceptable Use' as defined within this Policy.

1.3 Staff must not carry out any of the prohibited activities or uses listed in this Policy (ref. Sub-Section 9 - Prohibited uses of Equipment, Systems and Services). If Staff are unsure about whether or not something they intend to do complies with this Policy, they should ask their manager for advice.

1.4 Staff members should not upload RMG's Internal, Confidential or Strictly Confidential information to any unapproved application, including unapproved 'Cloud' based applications.

1.5 RMG IT equipment should not be connected to unsecured public Wi-Fi services. Staff should read our Business Standards, this Policy, and the other Royal Mail Group Information Security Policies that apply to them. Staff should also read the associated guides

applicable to them (see the ‘Further information’ section below).

2. IT Equipment assigned to Staff

2.1 Staff are expected to take care to safeguard any equipment that Royal Mail Group has assigned to them, both inside and outside of work, in particular by following the instructions and guides published on the intranet by RMG on securing equipment (see the ‘Further Guidance’ section below).

2.2 Staff must take reasonable steps to secure equipment from theft, for example by physically securing a laptop using an appropriate lock, or by locking the equipment in a secure cupboard or drawer when not in use.

2.3 Staff should ensure to keep their RMG IT equipment secure as if it were their own property, for example not leaving it where it is immediately visible through a window at home to an intruder.

2.4 Staff must not leave Royal Mail Group equipment unattended in a public place (e.g. restaurant, bar or public transport).

2.5 Staff must take reasonable steps to protect equipment from loss or damage (e.g. making use of protective carrying cases and bags supplied with the equipment).

2.6 Staff must report the loss or theft of any Royal Mail Group IT equipment as soon as possible to the IT Helpdesk, and co-operate with Royal Mail Group in any efforts to investigate the circumstances of the loss or theft, and with identifying the data or information that was stored on the lost or stolen equipment.

2.7 Royal Mail Group (or in some cases partner organisations working under contract with Royal Mail Group) owns such equipment, and retains ownership throughout the time it is assigned to an employee for use. Staff members have no rights in respect of such equipment or the data held within and must return it to Royal Mail Group on leaving Royal Mail Group or on demand by an individual authorised by Royal Mail Group.

2.8 RMG IT equipment should not be taken away from home or office, for example on holiday, unless an exception has been agreed with your Line Manager.

2.9 Staff should not attempt to circumvent any security controls on the RMG IT equipment that has been assigned to them.

3. IT Services provided to Staff

3.1 Staff may be assigned access to Royal Mail Group services to enable them to do their work, including, for example, an email

account on Royal Mail Group email servers or webmail, a logon account for a desktop or laptop, access to instant messenger, or access to the internet through a browser.

3.2 Staff must take all reasonable precautions to keep any account logon passwords, PINs, security devices and security details safe and to prevent others from using them. Services must also be used in line with the information security, and information governance policies.

3.3 If any password, PIN, security device or security details are lost or stolen, or Staff suspect that someone has used or tried to use them, they must report this immediately by calling the IT Helpdesk. Staff must also report to the IT Helpdesk information security incidents, such as unusual activity on their devices.

3.4 Staff are responsible for what is done on Royal Mail Group IT and communications systems using the accounts assigned to them. This includes anything done by someone else, if Staff members, in breach of this Policy, have allowed another person to use any passwords, PINs, security device or security details issued to them for their sole use. In cases where access to IT and communications systems has been through fraudulent, deceptive, or coercive means, the affected member of Staff may not be held responsible.

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

4. Personal use of provided Systems, Services and Equipment

4.1 Royal Mail Group IT and communications systems are provided principally for business purposes. Acceptable use includes reasonable and limited personal use in line with this Policy, and specifically subject to the conditions below.

4.2 Staff must agree any personal usage of IT and communications systems with their manager beforehand. Personal use will normally only be permitted during meal breaks or before or after working hours.

4.3 Personal use should be restricted to avoid interfering with their and any other member of Staff job responsibilities.

4.4 If Staff use Royal Mail Group IT and communications systems for personal use, Royal Mail Group will carry out monitoring of such use and create records of use in the same way it does for business use of the IT and communications systems. See the 'Systems Monitoring and Data Collection Policy' for further information.

4.5 Royal Mail may ask Staff to categorise recorded use of IT and communications systems either as personal use or as business use, to enable Royal Mail Group to determine the costs of business usage of its IT and communications systems.

4.6 Staff should not store personal data and items such as music or photographs on their RMG IT equipment. Royal Mail reserves the right to erase such data.

4.7 If personal use of Royal Mail Group equipment or other IT and communications systems causes an additional financial cost to Royal Mail Group (other than loss of the member of Staff's time referred to above), Staff may be asked to pay that additional cost to Royal Mail Group or direct to the organisation charging Royal Mail Group.

4.8 Royal Mail Group accepts no liability for any loss or detriment suffered by Staff through personal use of Royal Mail Group systems and services.

4.9 Royal Mail Group does not offer any guarantees of confidentiality or continued availability of any information Staff place on Royal Mail Group IT and communications systems while using them for personal purposes.

5. Email addresses and telephone numbers

5.1 Staff may be provided with an email address by Royal Mail Group for work purposes. Access to and use of such an email address, and/or the mailbox provided with it may be withdrawn at any time, and will be removed when they are no longer employed or engaged by Royal Mail Group.

5.2 Staff may be provided with landline or mobile telephone numbers by Royal Mail Group for work purposes. Use of these numbers 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 Royal Mail Group.

6. Social media

6.1 Unless acting on behalf of Royal Mail Group, Staff should only be accessing social media outside of their working hours or during meal breaks. The exceptions to this are those with access to RMG's

internal social networks and the RMG WhatsApp group, where Staff are permitted to use these in moderation during working hours as long as they adhere to the relevant guidelines and policies.

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

(a) Always treat social networking sites and activities as if they were publically accessible
(b) Do not disclose Royal Mail Group Internal, Confidential or Strictly Confidential information
(c) Never offer opinions or comments on behalf of Royal Mail Group without the prior approval of the Managing Director of Corporate Affairs, Regulation, Marketing and Customer Experience.
(d) Do not publish information relating to clients, partners or suppliers in a personal context
(e) Do not violate copyright, data protection and intellectual property rights
(f) Never cause offence or harass anyone
(g) Never use their Royal Mail Group email address as an identifier. The exception is RMG's internal social networks, where Staff will need to have a Royal Mail email address to gain access to the network.
(h) Never use Group brands or logos
(i) Post comments or upload images/videos on internal or external social media platforms that would damage Royal Mail's reputation

6.3 Where a member of Staff 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 group communication team.

6.4 Royal Mail Group expects all Staff to abide by the same standards of conduct and behaviour online as they would in all other dealings.

The Royal Mail Social Media Guide provides information that is more detailed.

7. Information classification

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

7.2 All Staff members have a duty to be aware of what information they

are accessing, using, distributing, and removing, and they must do everything they can to make sure such information goes to the right people and is secure, and that it is in line with this Policy.

7.3 Royal Mail Group expects Staff to protect information according to its classification, sensitivity, and potential business impact.

See the Information Security, and Information Governance policies on the Group Policies intranet site for further information.

8. Monitoring

8.1 Royal Mail Group systems and services generate records when they are used. Royal Mail may collect and analyse records made during Staff use of its systems. See the Systems Management Policy for details of what is monitored and why.

9. Prohibited uses of Equipment, Systems and Services

9.1 This section of this Policy gives some examples of prohibited and unacceptable uses of Royal Mail Group IT and communications systems. This list is not exhaustive.

9.2 Staff must not use any Royal Mail Group systems or services to:

(a) Download, view, possess, or transmit in any way material that:
  (i) Is illegal in the UK or in the country in which they are located, or operating;
  (ii) Is pornographic, offensive or obscene;
  (iii) Promotes or facilitates criminal or terrorist activities;
  (iv) Is discriminatory, or otherwise promotes or encourages intolerance, racism, sectarianism, hate crimes or violence;
  (v) Is, or is likely to be, defamatory, threatening, harassing, or abusive;
  (vi) Breaches copyright, or other intellectual property rights;
  (vii) Brings, or is likely to bring, Royal Mail Group or its Staff into disrepute;
  (viii) Staff know, or suspect of, being infected with a worm, virus, or any other form of malicious software

(b) Gain or attempt to gain unauthorised access to any computer systems for any purpose;

(c) Prevent access by other authorised users of Royal Mail Group IT and communications systems;

(d) Carry out any network or activity monitoring, unless properly authorised to do so for Royal Mail Group's business purposes;

(e) Intentionally alter or attempt to alter the intended operation of any computer (for example by downloading unauthorised software);
(f) Infringe the legal rights of others, including, but not limited to, privacy rights, copyrights, and intellectual property rights;
(g) Make statements that appear to represent Royal Mail Group's official views, or that make commitments on behalf of Royal Mail Group, unless they are properly authorised under other policies to do so;
(h) Carry out any non-Royal Mail Group business, trade or for-profit activities;
(i) Send or redistribute unsolicited emails ("spam") to external email addresses or to other Royal Mail Group Staff;
(j) Infringe any other Royal Mail Group policies that apply.

9.3 Staff must not:

(a) Give access to, or distribute Royal Mail Group information to anyone they are not properly authorised to;
(b) Deliberately alter, destroy or corrupt data or information stored in Royal Mail Group systems, unless they are properly authorised to do so;
(c) Send Royal Mail Group information internally or externally unless it meets the requirements of Information Security Classification Policy (available on the Group Policies intranet site);
(d) Use any account logon passwords, PINs, security devices or security details that have not been issued for their use;
(e) Share any account logon passwords, PINs, security devices and security details that have been issued for their sole use;
(f) Disable, bypass or circumvent any measures put in place by Royal Mail Group to maintain the safe and secure operations of its systems and services;
(g) Use any email address issued to them by Royal Mail Group to register for personal accounts or services (e.g. social media accounts, online shopping accounts, blogging accounts);
(h) Connect devices or equipment to Royal Mail Group IT and communications systems, unless properly authorised to do so for Royal Mail Group business purposes
(i) Auto-forward Royal Mail Group emails to personal email accounts.

10. Training and Awareness

10.1 All Staff should complete all relevant Information security and Privacy training or self-learning on relevant policies, procedures and

compliance responsibilities.

10.2 All Staff should ensure that they are aware of RMG's information security policies and procedures that they are required to follow.

What happens if the Policy is breached?

If Staff breach our Business Standards or this Policy, it is likely to be considered misconduct that may lead to disciplinary actions, or possibly gross misconduct, which could result in action under the Conduct Policy, up to, and including dismissal without notice (Check the 'Further information' section for more details), and can expose RMG or Staff to corporate or personal liabilities.

If Staff (other than employees) breaches our Business Standards or this Policy, this may result in Royal Mail Group re-considering its decision to engage them.

Further information

The 'Getting help' box on the front page of this Policy tells you how and where to find further information.

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;
- Conduct Policy.

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

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

This includes "Think Secure: How to guides for protecting information".

Other policies that employees should pay particular attention to include:

- Cloud Security Standard (ISDT01)
- Communications Policy
- Continuous Disclosure and Communications Policy

For access to the above policies, please go to the Group Policies intranet site, or to the Information Security policies intranet page.

Policy owner and review process	The Policy Owner is the Chief Compliance Officer and a review of this Policy is carried out annually, as a minimum. The approach to the review of all RMG policies are detailed in a Policy Review Guide, which can be found on the guidelines sub-section on the intranet.

Royal Mail Group

Inappropriate Use of Internet and Email and other Royal Mail Systems

Guide for employees

This guide outlines the behaviours and standards expected from all employees when using Royal Mail Group's information, IT systems and mobile devices (including personal devices)

Main topic areas

Getting help

Contact your manager if you have any queries about this guide.

Managers can obtain advice by:

Calling the HR Services Advice Centre on 0345 6060603 / 5456 7100

Managers working for Parcelforce Worldwide should call 0345 604 787 / 5456 4747

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

Inappropriate Use of Internet and Email and other Royal Mail Systems

Guide for employees

Introduction

Royal Mail Group provides employees access to various IT systems and mobile devices.

It is important that all employees read the Acceptable Use Policy, Our Business Standards and associated policies and guides, to understand that we all have a duty to follow its standards when using Royal Mail Group's information, IT systems, equipment and services for business or personal use, both on-site and remotely. The policy also applies to personal mobile devices or equipment/ computers which are owned by someone else (in an Internet cafe, for instance).

Failure to do so may be a breach of the Our Business Standards and Acceptable Use Policy. Such a breach is likely to be misconduct and possibly gross misconduct, and could result in conduct action up to and including dismissal, depending on the nature of the offence. Accessing or downloading certain material could also be a criminal offence.

This guide applies to all employees, contractors, consultants, subcontractors, casual workers and agency workers who use Royal Mail Group IT and communications systems and equipment.

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

Employees are responsible for the security of the Royal Mail equipment they use, especially when travelling.

When using Royal Mail computers, IT systems, Internet, email and mobile devices, employees should always ensure that:

- Remote connections to the Royal Mail Group network are made through Groups Virtual Private Network (VPN)
- Computer/laptops/mobile devices are switched off or locked when left unattended to prevent unauthorised users accessing Royal Mail systems
- They do not share their passwords or use another person's logon or password
- Only work-related music, videos, photographs or images are to be stored, transmitted, downloaded or uploaded to Royal Mail Group IT systems
- Group emails should not be used to raise queries or spread inappropriate messages. The appropriate helpdesk or contact should be used for queries and issues. Employees who receive inappropriate or erroneous group emails should not reply to all other recipients

Emails can be disclosed in legal proceedings in the same way as paper documents. Deleting an email from a user's inbox or archives does not mean that it can't be recovered.

Personal use:

- While Royal Mail Group internet, email, phones and other IT systems are primarily for business use, it is recognised that occasionally employees may need to send or receive a personal email, make a phone call or use the internet for personal activities. The Acceptable Use Policy does allow for reasonable and occasional personal use. This personal use should be

kept to a minimum, preferably before or after an employee's normal working hours or during their meal break, so that it does not interfere with the efficient running of Royal Mail's business

- Social media sites should not be accessed during normal working hours. The exception to this is those with access to RMG's internal social networks such as Workplace by Facebook and the RMG WhatsApp group. Staff are permitted to use these in moderation during working hours as long as they adhere to the relevant guidelines and policies
- 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
- Personal emails should be marked as 'personal' using the sensitivity tab under 'Properties'

The Acceptable Use Policy provides details of the prohibited and unacceptable uses of Royal Mail Group equipment, systems and services.

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.

Only employees who are authorised by Royal Mail Group can upload content to this site. They they must comply with the intranet rules noted in the Acceptable Use Policy, External Digital Communications Policy and the Communications Policy.

Information classification

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 (including inside information) that could harm our brand or expose Royal Mail Group to significant disadvantage should it fall in to the wrong hands. This includes, but is not confined to inside information, i.e. information that is precise, not generally available and which could have a significant effect on the price or

value of Royal Mail Group shares if it were made publicly available. Most people do not handle Strictly Confidential information. Examples: details of our commercial plans, strategic initiatives, capital raising initiatives, or unpublished financial results.

See the Information Security and Information Protection policies on the Group policies intranet site.

Monitoring

The content of Royal Mail's IT resources and communications systems is Royal Mail Group property. Therefore, employees should not expect guaranteed privacy when using these systems. Where Royal Mail systems have been used improperly or in breach of the law, the content of specific electronic transactions may be monitored by authorised individuals.

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.

See the Systems Monitoring and Data Collection Policy for details of what is monitored and why.

Inappropriate material

Employees must not search for, download, receive, store or send inappropriate material. Inappropriate material includes offensive material (such as distasteful jokes based on people's differences), sexually explicit images or abusive/exploitative images showing violence or degrading treatment.

Royal Mail Group will investigate seriously any allegations of this type of misconduct. In addition to contravening the Group's own policy, downloading and viewing sexually explicit images in the workplace may also constitute sexual harassment. The discovery of material of a sexual nature involving children or illegal pornography must be reported immediately to **Royal Mail Group Security on 020 7239 6655** or **postline 5474 6655** and material of this nature will be reported to the police.

Any allegations of misconduct in this area should be investigated following the appropriate standard disciplinary procedures (the Conduct Policy for Royal Mail Group employees). Each case must be considered on its own merits.

Extent of personal contribution to accessing inappropriate material

Computer records will help us to demonstrate and identify what actions people have taken when they have accessed or received inappropriate material.

This applies both to searching for and viewing inappropriate material as well as being the recipient of inappropriate material.

Users who mistakenly access an inappropriate internet site should click on the X icon in the top right corner of the browser screen to close internet explorer.

If an employee receives inappropriate material, they should inform the sender that they should not use business systems for this material and delete it from their system. The employee may also report the matter to their manager (or the sender's employer if outside the business) if they feel the material requires it.

Someone who receives material and sends it on to others will be held accountable for both their lack of judgement in effectively endorsing the material and the conscious decision to involve others.

The volume of material will also be considered: the more an individual searches, stores or sends, the more times they have exercised poor judgement about their willingness to uphold business values.

Individual's response to accessing inappropriate material

The degree of acceptance by the individual of their actions will help managers decide if they will be able to trust them in the future.

This involves the employee's:

- Degree of acceptance of wrongdoing
- Degree of commitment to correct behaviour
- Sincerity of both of these. However if cases are very severe or there have been a large volume of breaches sustained over a period of time, it will be difficult for people to successfully persuade the business that they are able to be trusted in the future

If employees try to frustrate, mislead, or deceive an investigation, they are accountable separately for this and the usual business standards of honesty and integrity apply. Ultimately, it is for the manager to decide whether an employee's honesty and integrity have been compromised to the extent that they have breached their contract and should be dismissed.

Where to go for further information

Please refer to the 'Getting help' for details of where to go for further information.

Please also refer to the Policy and Information site on PSP (HR pages of the intranet for non-PSP users) for further guidance relating to this guide:

- Our Business Standards
- Acceptable Use Policy
- Acceptable Use – Social Media Guide for Employees
- Acceptable Use – Dealing with Conduct Issues Relating to Social Media Manager Guide
- Conduct Policy and guides
- Stop Bullying and Harassment Policy and guide
- Information Security Policies
- Information Governance Policies
- Intellectual Property Policy
- Systems Monitoring and Data Collection Policy
- Data Protection and Privacy Policy
- Communications Policy
- External Digital Communications Policy