Angard
Acceptable Use Policy

Angard Staffing employees who are placed on assignments with Royal Mail will have access to a range of IT systems and mobile devices such as laptops and personal digital assistants (PDA) as work tools. This policy sets out some clear rules on how Angard Staffing expects employees to behave when using the company's and Royal Mail's information and IT systems.

Main topic areas

- Overview
- Policy statement
- Use of computers, IT systems, Internet, email and mobile phones
- Personal use/Use of Royal Mail systems generally
- Using the internet appropriately
- Internet access
- Social media
- Email, spam and viruses
- Understanding our information
- Keeping our information secure
- Monitoring
- Copy right infringement
- Non-compliance
- Where to go for further information
- Related documents
- Glossary
- Review

Getting help

Please contact the Angard Helpline Number 0333 240 8502 or email angard.employee@reedglobal.com.

For web access go to: www.angardstaffing.co.uk.

Overview

This policy applies to Angard Staffing **(Angard)** employees who are accessing Royal Mail Group Ltd **(Royal Mail)** Systems.

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

This policy does not form part of contracts of employment.

This policy is effective from 1st April 2014.

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 Angard's and/or Royal Mail's information and IT systems, it can impact on the reputation of Angard, the Royal Mail, our employees and agents, our products and services.

It is important that you read this policy and understand that we all have a duty to follow the rules and standards outlined when using Royal Mail's information and IT systems for business 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). For the avoidance of doubt, as an Angard employee, you are not permitted to use Royal Mail systems for personal use.

Failure to observe any aspect of this policy may lead to disciplinary action being taken against you. Such action could include summary dismissal (in the most serious cases) or suspension of email or internet facilities.

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

Royal Mail provides computers, mobile phones and a range of portable equipment as work tools for many of its people. As an Angard employee you may be given access to Royal Mail systems and equipment when on an assignment to Royal Mail.

The security of information and IT systems is essential to Royal Mail's success. Anyone who uses Royal Mail .equipment must know how to keep these secure by following the requirements in this Acceptable Use Policy.

Remember to use the internet safely and sensibly, be social media wise and report incidents immediately.

Royal Mail and Angard do not permit:

- Downloading, installing or using unauthorised or banned software or modifying company-provided hardware or software;
- Accessing, storing, sending, posting or publishing gambling , pornographic, indecent, illegal, offensive, threatening or insulting material, or chain or "spam" emails;
- Accessing or forwarding documents or emails that allow computer viruses to infect our network;
- Use of Royal Mail or personal equipment in such a way that it interferes with productivity;
- Sending confidential or Strictly Confidential information by email, instant messaging, or the Internet without adequate security;
- Sharing of computer user IDs log in details and passwords.

Always ensure that:

- Remote connections to the Royal Mail network are made through the Royal Mail Virtual Private Network (VPN)

- Only business related music, videos, photographs or images are to be stored, transmitted, downloaded or uploaded to Royal Mail IT systems.

Personal use/use of Royal Mail systems generally

As an Angard employee you are not permitted to make personal use of Royal Mail information and IT systems and equipment.

Neither Angard nor Royal Mail is responsible for the recovery of any non-business data on its systems and this data may be deleted at any time.

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

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

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 of Royal Mail, including those who do not have access to a computer at work.

Security

Any attempt (whether successful or not) to gain unauthorised access to, or to tamper with, any computer system or software or installation will be regarded as gross misconduct. This includes the malicious deletion or alteration of documents created by you or others in the course of your duties. You may also be liable to prosecution under the Computer Misuse Act 1990, even where no damage results from your action.

Your password is confidential and should be kept as such. When leaving the office, you must log out of the system to prevent unauthorised access through your terminal. This also enables the virus checks on your computer to be updated. Unauthorised use of a password without good reason will also be treated as gross misconduct.

Screensavers and Software Installation

You may not install any software onto Angard's or Royal Mail's computers or systems. Such action may lead to disciplinary action up to and including summary dismissal in serious cases.

You may not use screensavers which include any obscene, pornographic or otherwise offensive (within the meaning of our Equality and Fairness Policy) material. Such use will lead to disciplinary action up to and including summary dismissal in serious cases.

Internet Access

You must not use Angard's or Royal Mail's internet facilities to visit, bookmark or download material from obscene, pornographic or otherwise offensive (within the meaning of our Equality and Fairness Policy) websites on the Internet. This could infringe copyright, incur expense for the firm or expose it to criminal penalties or liability for harassment or defamation. Such use constitutes misconduct and will lead to disciplinary action which, in serious cases that are viewed as gross misconduct, may result in summary dismissal.

You will not be permitted to use the internet for personal use during any assignment to Royal Mail.

Social media

Angard 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 Angard's or Royal Mail's reputation and brand.

You must therefore carefully consider the content of their posts and any reference to Angard or Royal Mail in such messages and comments before making them. Further information on this is contained in our Social Media Policy.

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

Angard 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 you use instant messaging as part of your job, they must only use the Royal Mail approved instant messaging facilities – Microsoft Office Communicator. You must not use alternative, non-approved systems for business conversations.

Royal Mail approved instant messaging services should only be used:

- With the same etiquette expected of any other form of business communication, i.e. appropriate:

    (i) tone and language;
    (ii) content and subject matter;
    (iii) relevance and related business information;
    (iv) 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 you do not recognise the source of an incoming email you 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 you receive any suspicious content, you must report it to the Angard Helpline Number 0333 240 8502 or email angard.employee@reedglobal.com. You must also delete offensive or commercial messages promoting or advertising goods, services or opinions.

You should remember that email messages do not cease to exist when you delete them from your terminal. They remain on Royal Mail's hardware and can be retrieved if required by Royal Mail or the courts. The content of emails may be relevant to legal action against Angard or Royal Mail and therefore emails may have to be disclosed. Messages sent on the email systems for business purposes should therefore accord, in both the form and content of language used, to the high professional standards

applied by Angard and Royal Mail to all other written forms of communication. Where appropriate, hard copies of outgoing and incoming emails should be retained, as should confirmation (if this is available) that important outgoing messages have been received and opened by the intended recipient. Care should be taken to avoid entering into binding contractual relations inadvertently, making negligent statements or breaching any confidentiality obligations.
When using email you should ensure that:

- Email and instant messaging is not used to communicate confidential or strictly confidential information;
- All email messages are concise. General messages to a wide group should only be sent where necessary;
- 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;
- 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, provided it 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.

Virus checks

Screensavers, wallpaper and programmes other than Word and Excel documents must not be downloaded from the Internet.

Our information

Information is a valuable asset for Royal Mail 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 expects employees to protect information according to its classification. Angard employees who are placed on Assignments with Royal Mail will need to be aware of these classifications. Each classification defines a clear set of instructions for the appropriate storage, distribution and disposal of information. The 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 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 internet. 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'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 to significant disadvantage should it fall in to the wrong hands. Most people do not handle Strictly Confidential information. Example: unpublished financial results.

We must manage our information, and that of Royal Mail, correctly and ensure that:

- Information related to any person, whether a colleague or a customer, is used appropriately;
- Appropriate authorisations are complied with: 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;
- Out of Office auto reply messages do not include personal contact information;
- Only business-related music, videos, photographs and images are stored, transmitted, downloaded or uploaded to Royal Mail IT systems.

If you receive an email or other message which is not intended for you, you should redirect it as appropriate. If the message contains confidential information, you have a responsibility not to act on or disclose that information.

When working with any Royal Mail 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 you must:

- Only share it with employees of Royal Mail or other Angard employees 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'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 you 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 landlines and mobile numbers are also recorded and retained.

Royal Mail reserves the right to monitor communications in order to determine the existence of facts, detect unauthorised use of its system and to ascertain the standards which ought to be achieved by employees using its system. Monitoring information may be passed to Angard as your employer. Where Royal Mail IT systems have been used improperly or in breach of the law, or if we need to assist the authorities, we will extend this monitoring to the content of specific electronic transactions. Only authorised individuals can access this information.

If your data has been accessed in your absence, unless this is to comply with the law or assist the authorities, you will be notified on their return of the reasons for the access. You will also be told who had access to the information and what was disclosed.

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

Copyright Infringement

You must take care to ensure that you do not breach copyright or incur expense to Angard or Royal Mail when copying, downloading or sending material to third parties which you have received by email or visited on the Internet.

Non-compliance

Failure to comply with this policy may prevent future use of Royal Mail IT systems and may result in investigation and disciplinary action under our Disciplinary 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 the Angard Helpline Number 0333 240 8502 and email angard.employee@reedglobal.com any breaches of this policy or any unauthorised use they are aware of. This includes inappropriate postings about Angard and Royal Mail, their employees, customers, partners or suppliers on the Internet or intranet.

Where to go for further information

Please contact the Angard Helpline Number 0333 240 8502 or email angard.employee@reedglobal.com.

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

Related documents

Angard's Social Media Policy on the company internet or available from the Angard Helpline.

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 information security classification scheme consists of four levels: PUBLIC, INTERNAL, CONFIDENTIAL, STRICTILY CONFIDENTIAL.

Instant messaging

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 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.

Review

Angard will carry out reviews of this policy from time-to-time and may need to update to make sure it reflects business need.