POL00137308

Information Security and Assurance Group

IS03 - Acceptable Use Policy

Document Control

Overview

Owner:	CIO	**Enquiry point:**	Head of Information Security
Version:	1.2	**Effective from:**	7th June 2013
Last updated:	30th May 2013	**Last review date:**	6th June 2013
Review period:	Annually or major change		

Revision History

Version	Date	Author	Changes
1.2	30/05/2013	Duncan Godfrey	Updates with comments from stakeholders. Issued for ISPRC.
1.1	22/04/2013	Mark Pearce	Consistency corrections
1.0	03/04/2013	Duncan Godfrey	Updated with external review comments from Post Office Legal department. For approval.
0.4	13/02/2013	Duncan Godfrey	Minor formatting and grammar changes. Ready for approval by ISPRC.
0.3	28/12/2012	Mark Pearce	Review.
0.2	27/12/2012	Duncan Godfrey	New IS policy. Added comments from Mark Pearce and Dave King
0.1	21/12/2012	Duncan Godfrey	Reformatted from original HR release

1 Purpose and Statement

POL00137308

The purpose of this policy is to present what is acceptable use of Post Office® Information Systems.

All employees of Post Office® are responsible for using Post Office® information resources responsibly and securely. The resources are primarily provided to support business activities.

This policy does not form part of employees' contracts and may be amended at any time.

2 Goals

The goals of this policy are:

- Communicate what is acceptable behaviour when using Post Office® Information Systems.
- Communicate the repercussions for failing to follow this policy.
- Manage the impact of the risks associated with inappropriate use of Post Office® Information Systems, including: confidentiality breaches, legal claims, reputational damage, and adverse impact to the availability and/or integrity of Post Office® Information Systems and loss of revenue.

3 Scope

The policy applies to all Post Office® people and agents, contractors, suppliers and consultants of Post Office®.

4 Roles and Responsibilities

4.1 Information Security and Assurance Group

The Information Security and Assurance Group (ISAG) will review this policy at least annually and update accordingly to reflect changes to business objectives or risks.

4.2 Users

It is the responsibility of each user irrespective of their terms of employment or engagement to adhere to this policy.

All managers are directly responsible for implementing Post Office® policies within their business areas and for their staff's adherence to them.

5 Policy Statement

The use of Post Office® Information Systems is governed by its Information Security and company policies and it is the responsibility of the user to keep abreast of and comply with these policies at all times.

5.1 General System Use

POL00137308

Post Office® Information Systems and all the information contained within are the property of Post Office®. Users are provided access to these systems for appropriate business use only.

Users may only use resources for which they have authorisation. Users may only use their individual accounts and must not use another individual's account to access Post Office® Information Systems.

Users are individually responsible for the resources assigned to them and are accountable to Post Office® for the use of such resources.

It is the responsibility of the user to protect their passwords or any other credentials. Do not write down, display or disclose your user identity or password, or any other access code to any other individual.

Non-Post Office® owned devices must not be directly connected to Post Office® Information Systems (See IS16 Secure Mobile Device policy).

5.2 Misuse of Post Office Resources

Users must not intentionally attempt to alter the configuration of any Post Office® Information System or interfere with any security control (for example anti-virus). Users must not conduct any monitoring of Post Office® Information Systems unless this has been defined as part of their role and the necessary impact assessments have been undertaken.

Users must not take any actions to anonymise their use of Post Office® Information Systems.

Users shall not conduct any illegal or malicious activities using Post Office® Information Systems. This includes installing any tools that could support such an activity.

5.3 Email and Instant Messaging Acceptable Use

Email and Instant Messaging (IM) are tools for conducting Post Office® business and shall not be used for any other non-Post Office® related business activity. All emails and IMs are archived and retained as permanent records and are subject to disclosure to outside parties including regulatory and legal authorities.

Users must not forward business emails to their own non-Post Office® accounts. All email remains the property of Post Office® and must only be accessed via authorised channels.

The Email or IM facilities specifically must not be used for:

- Sending any message that others could consider indecent, offensive, threatening, insulting or derogatory
- Sending any messages that could be considered as bullying or harassing other employees, Post Office® customers or any other third party;
- Sending a false and/or defamatory statement about any person or organisation;
- Sending discriminatory material;

POL00137308

- Distributing, disseminating or storing images, video, text or other materials that might be considered indecent, pornographic, obscene or illegal
- Creating or distributing chain letters or unsolicited advertisements (SPAM)
- Any other material that is likely to create any liability (whether criminal or civil, whether for you or us).

Any conduct listed above is likely to be seen as gross misconduct and investigated under our disciplinary procedure. Any such action will be treated very seriously and is likely to lead to the summary dismissal of the user concerned (where the user is an employee) or termination of the user's contract (where the user is not an employee).

Only Post Office® approved IM facilities shall be used for business use.

5.4 Web Acceptable Use

Access to the web has been provide to support business activities and must primarily be used for this purpose. A certain amount of personal use is permitted (see section 5.8) but users must not:

- Access any content relating to: gambling, illegal drugs, pornography, criminal skills, hate speech or any other indecent, obscene or offensive material
- Send offensive, bullying, harassing or discriminatory material or material which is derogatory to others
- Post or otherwise transmit false or derogatory material
- Access pirated material which infringes copyright
- Access any material that is likely to create any liability (whether criminal or civil, whether for you or us).

Any conduct listed above is likely to be seen as gross misconduct and investigated under our disciplinary procedure. Any such action will be treated very seriously and is likely to lead to the summary dismissal of the user concerned (where the user is an employee) or termination of the user's contract (where the user is not an employee).

All web access is monitored and archived; this record will be audited for compliance with this policy.

5.5 Use of external File backup and Synchronisation Service

External file backup services (such as Dropbox and Gdrive) must not be used for storing Post Office® information. Access to these services will be restricted.

5.6 Authorised Software and Copyright Material

Users may only use the software provided to them by the Post Office® IT service. No unauthorised software is permitted on Post Office® Information Systems.

All users must comply with all intellectual property laws including copyright law. Any material which has a copyright must not be used on Post Office® Information Systems without the correct licence. This includes: videos, audio files and any protected documents (such as restricted PDFs).

POL00137308

5.7 Use of social media

Post Office® recognises that many of our people enjoy using social networking sites in their own time. Comments we publish on these sites may reach a surprisingly wide audience, and so we must all protect our brand and avoid doing anything that might bring the reputation of Post Office® into disrepute.

Everyone must be aware that information gained about Post Office® as a result of your work for the business must never be discussed or shared on social media sites.

5.8 Personal use of Post Office resources

While Post Office® Information Systems are intended for business use only, our policy does allow for reasonable and occasional personal use. Any personal use must be kept to a minimum and should not interfere with an employee's business responsibilities and the resources they are using.

Personal use remains a privilege and activity conducted on Post Office® Information Systems is still owned by the Post Office®. The Post Office® is not responsible for the recovery of any non-business data on Post Office® Information Systems and this data may be deleted at any time.

5.9 Reporting Incidents

It is the responsibility of the User to report any security incident or suspicious activity to the IT Service Desk. Advice can be sought from the ISAG.

5.10 Monitoring

Post Office® Information Systems will be monitored and audited for compliance with this policy. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

Where we have a reasonable suspicion that Post Office® Information Systems have been used improperly or in breach of the law, or if we need to assist the legal authorities or are otherwise required to do so by law, we will extend this monitoring to the content of specific electronic transactions. Only authorised individuals can access this information.

If an employee is concerned about personal privacy, they are advised not to use Post Office® Information Systems and equipment for personal correspondence or to store personally sensitive or confidential data.

6 Exceptions

As per the standard policy process, a policy exception must be applied for by contacting the ISAG. These exceptions will be challenged and reviewed by the ISAG on an annual basis. Evidence must be retained for both the exception and the annual review.

7 Violations

POL00137308

Any failure to comply with this policy will be seen as a violation of the policy and may be dealt with as set out under Enforcement below.

8 Enforcement

The ISAG will regularly assess for compliance against this policy. Additionally, all Post Office® people have a responsibility to report any concerns that there may have been a violation of the policy. Any violation of this policy will be investigated and is likely to be dealt with under our disciplinary procedures. In particular, any serious breach of this policy is likely to be seen as gross misconduct and could lead to the summary dismissal of the user (where the user is an employee) or termination of the user's contract (where the user is not an employee).

9 References

This document has the following references:

- UK Data Protection Act 1998
- The Computer Misuse Act 1990 (http://www.legislation.gov.uk/ukpga/1990/18/contents)

APPENDIX A: Glossary

	Definition
Acceptable Use	The rules on the use of Post Office® Information Systems in a way which protects the reputation of Post Office® and the integrity of its Information Systems and equipment.
Instant Messaging (IM)	A system for real-time electronic messaging on the Internet or over networks. The approved Instant Messaging tool in Post Office® is Microsoft Office Communicator.
Post Office® Information Systems	Broadly defined and includes but is not limited to: computer networks, Internet facilities, Instant Messaging systems, tablets, laptops, desktops, Personal Digital Assistants (PDA), podcasts, forums, blogs, message boards, social communication websites, newsgroups, remote access facilities and all communications through such systems.

POL00137308