Postmaster support policy

Network monitoring and branch assurance support

Version 4.1

Post Office is determined to reset its relationship with postmasters and has introduced policies that set out guidelines on how Post Office should support postmasters, specifically for use across twelve areas.

The policies stand on their own but should be reviewed in conjunction with each other. Support teams should have an awareness of all twelve policies and how they link together.

The twelve Postmaster Support Policies are listed in section 3.2 of this policy and can be found on the hub, here.

Contents page

1 Definitions

1.1 Definitions

1. **Branch Assurance Visit** – This is a comprehensive assessment of the current trading position of a Post Office[1] branch, and includes the verification of reported levels of cash, foreign currency (if applicable), stock items and discuss any highlighted operational issues to check if mandatory business conformance are operating as intended.

2. **Rationale Document (RD)** - this document sets out the rationale behind a decision to undertake a Branch Assurance Visit, along with relevant supporting data, and is provided to a postmaster to explain the reason behind the visit.

3. **Branch Assurance Reporting Tool (BART)** – This is a data capture form used to record the difference between the actual volume and value of cash, stock and currency in branch and the volumes and values as shown on Horizon.

4. **Script** - This is a script for the Lead Branch Assurance Advisor to follow to ensure the main points are communicated.

5. **Discrepancy** - Any difference between (i) the actual cash and stock position of a branch and (ii) the cash and stock position shown on Horizon as derived from transactions input by branch staff into the branch's terminals.

6. **Established Gain** - An event that causes a positive Discrepancy (i.e. the situation where the branch has more cash and/or stock than the derived figures for cash and/or stock on Horizon), which has been investigated by Post Office, or agreed by the postmaster, and found to be a genuine gain to Post Office which was caused by the negligence, carelessness or error of the postmaster and/or their assistants.

7. **Established Loss** - An event that causes a negative Discrepancy (i.e. the situation where the branch has less cash and/or stock than the derived figures for cash and/or stock on Horizon), which has been investigated by Post Office, or agreed by the postmaster, and found to be a genuine loss to Post Office which was caused by the negligence, carelessness or error of the postmaster and/or their assistants.

8. **Operational Excellence visits (Support visits)**– This is a supportive, face to face visit that is conducted to encourage accurate accounting and encourage operational robustness.

[1] In this policy, “Post Office” means Post Office Limited.

2 Overview

2.1 Introduction

The Central Operations Director and the Retail Operations Director have joint accountability to the Board of Directors for the design and implementation of controls and to manage risk, assure levels of cash and stock and reduce discrepancies and losses in the network[2]. Risk in the network is an agenda item for the Audit, Risk and Compliance Committee and the Post Office board is updated as required.

This policy is a non-contractual document provided for information. It does not form part of the contract between any postmaster[3] and Post Office.

2.2 Purpose

This Policy has been established to set the minimum operating standards relating to the management of Network Monitoring and Branch Assurance support throughout the Post Office network.

Network Monitoring and Branch Assurance support activity helps to ensure the accuracy of branch accounting records, relating to cash and stock. It also helps to assure that the integrity of cash and stock in the Post Office network is maintained. Network Monitoring is in place to identify branches where the integrity and accuracy of cash and stock, for that branch, could be at risk. This monitoring can then lead to a number of intervention activities (including Branch Assurance support) which are designed to identify the risks and help the branch resolve any associated issues.

This policy explains how branches will be supported with any potential issues identified through Network Monitoring and how Post Office will help those branches maintain accurate records of cash and stock through their branch accounting. Monitoring branch compliance with accounting processes helps to identify any issues earlier and makes investigating the root cause of any issues easier for both branches and Post Office.

It is one of a set of policies which provide a clear risk and governance framework and facilitate an effective system of internal controls for the management of risk across Post Office. Compliance with these policies is essential to Post Office in meeting its business objectives and to balance the needs of postmasters, customers, clients, and other stakeholders including our shareholder.

As many postmasters are limited companies or partnerships (and as individual postmasters may appoint managers to operate a branch on their behalf) any steps that need to be taken by a postmaster under this policy can be taken by someone authorised to act on that postmaster's behalf (such as a director, partner or manager).

[2] In this policy, “network” means branches not directly managed by Post Office

[3] In this policy, “postmaster” refers to a limited company, partnership, limited liability partnership, other entity or individual that contracts with Post Office for the operation of a Post Office® branch.

2.3 Core principles

Under agreements between postmasters and Post Office, postmasters provide products and services to customers on behalf of Post Office. The cash and stock used to effect those transactions is owned and funded by Post Office, unless the branch is self-funded.

Post Office has an obligation to its customers and clients to ensure that all branches are providing a quality of service and adhering to agreed standards. Post Office is committed to supporting its postmasters in this process.

- Branch activity is monitored, particularly in relation to accounting of cash and stock, and data insights will be used to identify branches that are experiencing issues and to identify potential risks to the cash and stock in a branch.
- Support is offered to branches identified through Network Monitoring to help resolve any issues related to branch accounting and mitigate risk in the branch. Wherever possible, this support will be offered remotely in order to minimise disruption to the operation of a branch. On-site support will be addressed by the Training team.
- Where Post Office cannot determine whether the branch's cash and stock records are accurate, Branch Assurance support will physically attend a branch to carry out a full count of cash and stock assets. Post Office will provide support to the postmaster when carrying out the visit.

The guidelines will ensure these practices are carried out in good faith and apply principles of fairness, transparency, and professionalism (being the underpinning behaviours of Post Office).

2.4 Application

This Policy is applicable to all Post Office employees[4] who perform Network Monitoring and Branch Assurance activities and defines the minimum standards to control financial loss, postmaster impact, regulatory breaches and reputational damage in line with the Post Office's Risk Appetite.

2.5 The risk

There are a number of risks that the Network Monitoring and Branch Assurance team help mitigate.

Discrepancies in cash and stock in the network can cause difficulties for postmasters and customers. Issues identified through Network Monitoring and/or Branch Assurance support may indicate that local branch accounting systems and processes are not robust, although it is recognised that there may be other reasons for discrepancies, including Post Office's accounting system. Some Discrepancies, once investigated, or agreed by the postmaster, may become Established Losses or Established Gains.

[4] In this Policy "employee" means permanent staff, temporary including agency staff, contractors, consultants and anyone else working for or on behalf of Post Office and, for clarity, does not include postmasters or postmasters' staff.

The risks in this area include:

- There is a risk that we may become non-compliant if the correct processes and procedures are not followed
- There is a risk the Branch Assurance team are providing incorrect advice & guidance
- There is a risk that Branch Assurance visits have an inconsistent approach
- There is a risk there may be lack of co-operation with postmasters during a Branch Assurance visit
- There is a risk that branches are not performing accounting procedures in a timely manner
- There is a risk that excess cash and or stock is not being managed effectively in branch
- There is a risk that source data may become corrupted when accessed through tools

Section 3.5 sets out the required operational standards that the Post Office has implemented to control these risks.

3 Risk appetite and required operational standards

3.1 Risk appetite

Risk appetite is the extent to which the Post Office will accept that a risk might happen in pursuit of day-to-day business transactions. It therefore defines the boundaries of activity and levels of exposure that Post Office is willing and able to tolerate.

Post Office takes its legal and regulatory responsibilities seriously and consequently has:

- **Averse risk appetite** to risks around service and support provided to postmasters**.**
- **Averse risk appetite** to being non-compliant with our statutory and regulatory obligations.
- **Averse risk appetite** for financial crime to occur within any part of the Post Office or network..
- **Averse risk appetite** in relation to unethical behaviour by Post Office employees.
- **Averse risk appetite** to risks around disputes and litigation.
- **Averse risk appetite** towards risks around our core operational processes that impact postmasters.
- **Cautious risk appetite** towards the risk of service interruptions that would considerably reduce branch availability across the network resulting in the inability to serve customers.

Post Office acknowledges however that in certain scenarios even after extensive controls have been implemented a risk may still sit outside the agreed Risk Appetite/Risk Tolerance. Risks outside of Appetite/Tolerance may be presented to the relevant governance forums for escalation/agreement of the risk position.

If a risk is identified which is outside of agreed policy a risk exception note will be required, details of which can be found here.

3.2 Policy framework

This policy is part of a framework of postmaster support policies that has been established to set the minimum operating standards relating to the management of postmaster contract risks throughout the business and network in line with Post Office's risk appetite. The framework includes the following policies:

- Postmaster Onboarding
- Postmaster Training
- Postmaster Complaint Handling
- Network Monitoring and Branch Assurance Support (this policy)

- Network Cash and Stock Management
- Network Transaction Corrections
- Postmaster Account Support
- Postmaster Accounting Dispute Resolution
- Postmaster Contract Performance
- Postmaster Contract Suspension
- Postmaster Contract Termination
- Postmaster Contract Termination Decision Review

3.3 Who must comply?

Compliance with this Policy is mandatory for all Post Office employees who perform network monitoring and Branch Assurance activities.

Where non-compliance with this policy by Post Office employees is identified by Post Office, Post Office will carry out an investigation. Where it is identified that an instance of non-compliance is caused through wilful disregard or negligence, this this will be investigated in accordance with the Group Investigations Policy.

3.4 Roles and responsibilities

- **Audit, Risk and Compliance Committee** – is the Committee of the Post Office Limited Board which reviews and approves Postmaster Support policies
- **Risk and Compliance Committee** - is the standing committee of the Strategic Executive Group who review and approve Postmaster Support policies for recommendation to the Audit, Risk and Compliance Committee.
- **Retail Engagement Director** – is the policy owner, who must comply with the governance responsiblities set out at section 6.1.
- **Head of Network Monitoring and Reconciliation** – is accountable for the deployment of this policy and the support of the team that manages Network Monitoring. This role is also responsible for regularly reviewing the effectiveness of this policy and for drafting any amendments that may be required.
- **Head of Operational Excellence** - is accountable for the deployment of this policy and the support of the team that manages Branch Assurance Support. This role is also responsible for regularly reviewing the effectiveness of this policy and for drafting any amendments that may be required.
- **Operations Manager, Network Monitoring and Support** – is responsible for assuring the effectiveness of the processes, tools and activies of the Network Monitoring team.

- **Central Operations Insight Manager** – is responsible for updating the risk model that sits behind the Network Monitoring report
- **Network Monitoring Team Manager** – will lead a team of Network Monitoring Advisors in identifying branches with potential accounting issues using a risk based data model.
- **Network Monitoring Advisors** – will carry out desk-based reviews into branch accounts using branch data to identify potential accounting issues. They will work with Branch Assurance Advisors, postmasters and other internal and external teams to review any identified issues, explain potential areas of concern, and agree with the postmaster solutions to any issues found ways to remedy the situation.
- **Branch Assurance Manager -** will lead a team of Branch Assurance Advisors (North and South) in deploying Branch Assurance support activity, including making phone calls and visiting Post Office branches in accordance with the standards set out in this policy. Branch Assurance Team Leaders, supported by the Branch Assurance Manager, are responsible for the quality assurance of these activities.
- **Branch Assurance Advisors -** will plan for and deploy Branch Assurance support activity. During the visit they will verify assets in a Post Office branch and produce a factual, detailed and accurate account of the visit (including areas identified for improvement) to provide to the postmaster.
- **Operational Support** – this is the team, reporting into the Head of Operational Excellence, that are responsible for scheduling visits to branches, updating the Branch Assurance Advisors on their schedule and providing points of contact. All cases are administered on MS Dynamics 365.

3.5 Policy required operational standards

A required operational standard defines the level of control that must be in place to manage inherent risks so that they remain within the defined Risk Appetite statements. This section of the policy also sets out the Business Area(s) responsible for managing that risk through their controls, and all employees must ensure that they comply with the policy requirements. There must be mechanisms in place within each business unit to demonstrate compliance. The policy required operational standard can cover a range of control types, i.e., directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk and the required policy operational standard in consideration of the stated risk appetite. The subsequent pages define the terms used in greater detail:

Risk area	Description of risk(s)	Required operational standard	Business owners	Control	Frequency
Non-Compliance of Postmaster facing teams	We may become non-compliant if correct processes and procedures are not followed.	**Preventive control**: The Network Monitoring and Branch Assurance Support policy is reviewed every twelve months, at least, or before if any material changes are required. Any amendments made to the policy are approved by RCC and ARC before the new version is published and circulated to the business. Once approved, policy training will be delivered to colleagues and include details about any updates or amendments that have been made.	Head of Network Monitoring and Reconciliation / Head of Operational Excellence	Governance & Training	As required (reviewed at least annually)
		Detective control: Data is used to identify branches who are not following the correct processes and procedures, who may require further support or monitoring.	Head of Network Monitoring and Reconciliation	Exception reporting	Daily

Risk area	Description of risk(s)	Required operational standard	Business owners	Control	Frequency
		Detective control: Network Monitoring Support Advisors will have four cases quality assured each month by the Network Monitoring Manager.	Head of Network Monitoring and Reconciliation	Performance management	Monthly
Consistent completion of Branch Assurance Visits	The Branch Assurance team are providing incorrect advice & guidance	**Detective control:** Branch Assurance Advisors will have a minimum of one Branch Assurance visit quality assured by the Branch Assurance Team Leader, per quarter.	Head of Operational Excellence	Observed Branch Assurance Visit	Quarterly
	Branch Assurance visits have an inconsistent approach Lack of co-operation with postmasters during a Branch Assurance visit	**Detective control:** The Branch Assurance Manager will review all Quality Assurance Review feedback with the Branch Assurance Team Leaders and the reviews will be spot checked by the Head of Contract Management & Deployment.	Head of Operational Excellence	Quality assurance feedback check and review.	Quarterly
		Preventive control: The Branch Assurance Chapters, which details the ways of working and process to follow for the different types of support call/visit or branch assurance visit required, are reviewed to make sure they are up to date and correct.	Head of Operational Excellence	Annual review of Branch Assurance Chapters	As required (reviewed at least annually)

Risk area	Description of risk(s)	Required operational standard	Business owners	Control	Frequency
Non-compliance of branch obligations	Branches are not performing accounting procedures in a timely manner	**Detective control:** A report is created to show branches that have not produced a branch trading statement in the last 60 days. Network Monitoring will contact the branch to offer support.	Head of Network Monitoring and Reconciliation	Monitoring branches who haven't rolled over in 60 Days	Daily
		Detective control: Where cash and stock accounting issues are identified, the Network Monitoring Team will notify the Business Support Managers, in the first 6 months of the term of a postmaster's contract, and the Area Managers thereafter, to advise them the postmaster may require extra support.	Head of Network Monitoring and Reconciliation	Notifying the Business Support Manager	Upon identification of an exception
Excess cash and stock	Excess cash and or stock is not being managed effectively in branch	**Detective control:** Surplus cash escalations will be reviewed, and any other risk factors will be considered. The actions taken, dependent on the findings, can be a combination of a phone call, visit, training, or support, or requesting a Branch Assurance visit in order to verify the cash at the branch.	Head of Network Monitoring and Reconciliation	Identification of branches with excess cash and stock	Weekly
		Detective control: Where a support visit or Branch Assurance Visit identifies excess cash or stock, the Branch Assurance Advisors will support the postmaster in creating a return of the excess to the Cash Centre or Swindon Stock Centre.	Head of Operational Excellence	Return of excess cash & stock	During a Support Visit or Branch Assurance visit

Risk area	Description of risk(s)	Required operational standard	Business owners	Control	Frequency
Data integrity	Source data may become corrupted when accessed through tools	**Detective control:** All flagged branch issues identified by the data tools are validated against the source data before proceeding.	Head of Network Monitoring and Reconciliation	Validation of presented data against source data	Weekly

4 Procedures

4.1 Network Monitoring

The Network Monitoring team carry out network monitoring using a risk-based model. The model ranks the branches in order of risk so that the team can ascertain which branches are the most 'at risk' and review them as a priority. The team also carry out reviews based on local knowledge received from internal teams.

The scoring rankings in the model are re-calculated on a weekly basis and the Central Operations Data team refresh the data used by the model on a weekly basis. The model can be used to 'search' for an individual branch, and it allows the advisor to 'deep dive' and review potential trends and patterns in the data with respect to that branch. The advisor can build a picture from the data to aid understanding of the accounting systems and processes at the branch before raising any issues or concerns with the relevant postmaster.

Where an accounting issue is identified, the Network Monitoring team will, wherever possible and appropriate, contact the postmaster with a view to helping the postmaster to rectify that issue. This support may be provided through a telephone call from the Network Monitoring team, which will include signposting to the NFSP, the arrangement of a Support Call or Visit by a member of the Branch Assurance Support team and, occasionally, through an Branch Assurance Visit. A combination of these support options may be deployed.

The Network Monitoring team will produce a Rationale Document at this stage of the review in circumstances where a Branch Assurance Visit is required. This document is sent to the relevant Branch Assurance Advisor, and the branch, in advance of the visit.

The Network Monitoring team will open a case on the case management system (Microsoft Dynamics 365) for each desktop review. They will populate the case with any all actions that are taken in relation to that case, including phone calls made to the postmaster and the record and results of any visits made.

4.2 Scheduling supportive visits and branch assurance visits

The Operational Support team are responsible for scheduling calls, visits and Branch Assurance Visits to branches on behalf of the Branch Assurance team. They will schedule these activities at the earliest opportunity based on the priority of the activity and the resources required to carry out the activity. At least two Branch Assurance Advisors will be scheduled to attend a full visit.

In order to complete a full verification, it is necessary to close a Post Office branch for the duration of the visit. As a result, it is essential in order to expedite the process and cause minimum disruption to postmaster and their customers that Post Office use the optimum number of Branch Assurance Advisors. Factors that may inform the number of Branch Assurance Advisors required, for a full verification visit, are the cash holdings in the branch at the time of the visit, whether the branch has an ATM machine and whether the branch holds foreign currency.

In the case of Support Visits and Branch Assurance Visits (including closure visits and transfer visits), unless there are exceptional circumstances, the Operational Support team will attempt to arrange a suitable time and date with the postmaster in advance.

4.3 Carrying out a branch assurance visit

A lead Branch Assurance Advisor will attend each visit. Lead Branch Assurance Advisors are responsible for preparing for the visit, managing the visit and completing the final Branch Assurance report. The lead Branch Assurance Advisor will liaise with the postmaster or the postmaster's representative throughout the visit. They will engage in a discussion with the postmaster or representative using the Script. As a minimum, the lead Branch Assurance Advisor will go through the Rationale Document with the postmaster or representative

The lead Branch Assurance Advisor will explain why the Branch Assurance Reporting Tool (BART) is used as a verification tool. They will: (i) talk through the relevant event history; (ii) establish where all the assets are held in branch; (iii) explain why they need to access the Horizon Online system at the branch; and (iv) encourage questions throughout the process.

The lead Branch Assurance Advisor will provide regular updates throughout the visit and perform the closing meeting, during which they will explain the result and findings, in doing so following the Script. The lead Branch Assurance Advisor will delegate necessary tasks to the other Branch Assurance Advisors in attendance, making the most efficient use of resources to ensure that there is minimum disruption to the branch and its customers.

The lead Branch Assurance Advisor will print various reports from the Horizon Online system so that the team can understand the value of the cash, stock and foreign currency being held in branch. These reports are detailed in the Branch Assurance Chapter 02, available on the Knowledge Centre. The lead Branch Assurance Advisor will conduct a physical count of the same and will manually record both sets of figures. They will repeat this process for each stock unit and then calculate the totals for the branch. A second Branch Assurance Advisor will repeat this process and check the figures generated, and the Branch Assurance team will invite the postmaster or representative to check the figures independently.

The Branch Assurance Advisors will prepare any excess cash and or stock or obsolete stock for despatch from the branch once it has been counted and verified.

The figures from the cash and stock count sheets will be transferred onto the Branch Assurance Reporting Tool at the visit. A final copy of the report will be emailed to the postmaster/branch. The lead Branch Assurance Advisor will retain the manual records of the cash and stock counts for a period of 60 days.

The Branch Assurance Advisors will advise of any discrepancy found at the visit with the postmaster or representative and will use their ID to move the discrepancy into the centralised holding account. They will signpost the postmaster or representative to the Branch Support Centre (BSC) who will assist in the resolution of the discrepancy. National Federation of Subpostmasters support will be also signposted.

In the event where there is an admittance of theft or misuse of Post Office Funds, for example using Post Office funds for private use or processing deposits into bank accounts without accepting cash at the time of the transaction, the Branch Assurance Advisor will contact a Contract Advisor. The purpose of this contact is for the Contract Advisor to make an assessment of the situation and, in line with the Postmaster Contract Suspension Policy, determine whether there is a requirement to suspend the agreement. If suspension is not deemed appropriate the Contract Advisor may be required to ensure that any further activity (including support for the postmaster) is undertaken.

4.4 Closure branch assurance visits

The Operational Support team will schedule a date for the closure visit to take place. A closure visit is carried out when a postmaster contract is terminated by either party. The outgoing postmaster will be contacted by the Branch Assurance Advisor no more than 5 working days after they have notified Post Office of the planned closure. The Branch Assurance Advisor will check if there are any unresolved accounting issues and, if there are, they will work with the postmaster or its representative to aim to have these rectified by the time of closure. Branch Assurance Advisors will ask the outgoing postmaster to reduce the holdings of cash and stock at the branch and return any excess cash and stock to Post Office prior to the date of closure.

All cash and stock will be prepared, by the branch, for despatch on the day of the visit for its subsequent despatch from the branch and a full final balance of the accounts will be completed. The Branch Assurance Advisors will use their ID to move the discrepancy into the centralised holding account and the postmaster/representative can instigate a review into the discrepancy by contacting the Branch Support Centre. Additional support will be offered by the National Federation of Subpostmasters (NFSP), and their contact details will be provided by the lead Branch Assurance advisor.

4.5 Post security incident branch assurance visits

In the event of a security incident, such as a robbery or burglary, a Branch Assurance Advisor will conduct a security incident Branch Assurance visit at the branch if the loss is valued at more than £5000.

Post security incident Branch Assurance visits will be scheduled as soon as is practicable following the incident to ensure that the postmaster is properly supported. The visit's purpose is to ascertain the cash and stock holdings in the branch immediately after the incident. The Branch Assurance process is the same as a full Branch Assurance Visit, but any discrepancies recorded at these visits will be posted to the Robbery & Burglary suspense account.

4.6 Reference materials

All written materials relevant to Branch Assurance Visits, including the instructions on how to complete a visit and relevant scripts, are stored in the Knowledge Centre SharePoint which is accessible to all Branch Assurance Advisors and Managers. These are reviewed annually as a minimum.

POL00448252

4.7 Quality assurance

The Branch Assurance Team Leaders are responsible for quality assuring Branch Assurance activities.

Each Branch Assurance Advisor will have a minimum of one Branch Assurance Visit quality assured by the Branch Assurance Team Leader, per quarter.

The Network Monitoring Team Managers perform monthly monitoring of phone call activity between postmasters and the Network Monitoring team. In addition to this, the RD and the Dynamics case are quality checked monthly. A sample of cases are selected for review by the Assurance & Complex Investigations team for second line assurance.

The Head of Operational Excellence is responsible for ensuring that the Branch Assurance Manager ensures the Quality Assurance Review (QAR) exercise is completed by the Branch Assurance Team Leaders.

When observing a Branch Assurance Visit, the Branch Assurance Team Leader will attend in person and will review the manner in which the visit is carried out, including engagement with the postmaster and adherence to the process. They will then complete an observational Quality Assurance Review form and use it to provide feedback to the Branch Assurance Advisor as soon as possible after the visit. The Branch Assurance Team Leader will also check the visit paperwork, such as the count sheets and report generated figures. The Branch Assurance Manager will spot-check feedback with the Branch Assurance Team Leaders.

4.8 Reporting

Post Office create reports to show how the Post Office network is performing against agreed cash and stock accounting practices. The reports which are generated daily include:

- Number of branches making daily cash declarations;
- Number of branches completing regular branch accounting;
- Number of branches not up to date with branch accounting deadlines; and
- Amount of cash in the network.

In addition, reporting is carried out on a monthly basis to give visibility of team performance. The reports which are generated monthly include:

- Number of branches monitored within a period;
- Number of branches contacted by phone;
- Number of supportive visits conducted;
- Number of Branch Assurance Visits completed by type; and
- Value and volume of discrepancies recorded at Branch Assurance Visits.

The Branch Assurance team host a weekly meeting with relevant stakeholders across the business to discuss branch assurance visit activity. This will include:

- Branch Assurance visits completed, rescheduled and repeat visits
- Branch Assurance visit details including potential value at risk, the trigger and findings

- Lead times from scheduling and performing a Branch Assurance visit
- Identification of postmaster support required
- Postmaster feedback

5 Where to go for help

5.1 Additional policies

This Policy is one of a set of policies. The full set of policies can be found on the SharePoint Hub under Postmaster Support Policies.

5.2 How to raise a concern

Any postmaster, any postmaster's staff or any Post Office employee who suspects that there is a breach of this Policy should report this without any undue delay.

If a postmaster or the postmaster's staff are unable to raise the matter with the area manager of the relevant branch or if a Post Office employee is unable to speak to her or his line manager, any person can bring it to Post Office's attention independently and can use the Speak Up channels for this purpose. Any person can raise concerns anonymously, although disclosing as much information as possible helps ensure Post Office can conduct a thorough investigation.

For more details about how and where to raise concerns, please refer to the current Speak Up Policy which can be found on The Hub under Post Office Key Policies, accessed here, or report online at: http://speakup.postoffice.co.uk or call the Speak Up Line on GRO

Please note that a postmaster may also contact the National Federation of SubPostmasters (NFSP) for help and support, by contacting their helpline on GRO or by emailing admin GRO

5.3 Who to contact for more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact the Retail Engagement Director, Tracy Marshall, by emailing GRO

6 Governance

6.1 Governance responsibilities

The Policy sponsor, the Group Chief Retail Officer of Post Office, takes responsibility for policies covering their areas.

The Policy Owner is the Retail Engagement Director who is responsible for ensuring that the content is up to date and is capable of being executed. As part of the review process, they need to ensure that the minimum controls articulated in the policy are working or to identify any gaps and provide an action plan for remediation

Additionally, the Retail Engagement Director, with input from the Central Operations Director and the Retail Operations Director, is responsible for providing appropriate and timely reporting to the Risk and Compliance Committee and the Audit, Risk and Compliance Committee as required.

The Audit, Risk and Compliance Committee are responsible for approving the Policy and overseeing compliance.

The Board is responsible for setting Post Office's risk appetite.

7 Document control

7.1 Document control record

Summary

GE policy sponsor	Standard owner	Standard implementer	Standard approver
Martin Roberts (Group Chief Retail Officer)	Tracy Marshall (Retail Engagement Director)	Network Monitoring – Alison J Clark (Head of Network Monitoring and Reconciliation) Branch Assurance Support – Mike Lowe (Head of Operational Excellence)	R&CC/ARC
Version	**Document review period**	**Policy – effective date**	**Policy location**
4.1	Annual	07/2024	Postmaster Support Policies on SharePoint Hub

Revision history

Version	Date	Changes	Updated by
0.1	1st October 2020	Draft Version	Jo Milton
0.2	8th October 2020	Revised draft	Jo Milton
0.3	8th December 2020	Revised draft – updated definitions and job roles	Jo Milton
0.4	15th December 2020	Footnotes added	Jo Milton
1.0	26th January 2021	Final Version approved by ARC	Jo Milton
1.1	29th March 2021	Annual review 2.3, 2.5, 3.4, 4.5, 4.6, 4.7, 4.9 expansion on existing content Section 3 -Added in Risk Appetite Statements 3.1, added in Policy Framework 3.2, added in “Who must comply” 3.3, added in Minimum Control Standards 3.5 Alignment to other postmaster support policies	Jo Milton
1.2	26th April 2021	Text amendments following internal and external legal review	Jo Milton

1.3	4th May 2021	Risk appetite amendment	Jo Milton
1.4	13th May 2021	Replacement of “settled centrally” language Rewording of section 4.4 (penultimate para)	Jo Milton
1.5	25th May 2021	Added linked policy statement to front page Added reference to the Group Investigations Policy to section 3.3 Who Must Comply? Updated link to section 5.1 Added footnotes to link to other policies referred to in this policy.	Jo Milton
1.6	25th February 2022	**Annual Review** Revision of job role names throughout 2.1 Addition of section stating that a postmaster may authorise someone to act on their/its behalf 3.1 Updated risk appetite statements to include Operational statements 3.4 Added Operations Manager to job role responsibilities 5.2 Added reference to NFSP	Jo Milton
2.0	1st April 2022	Amended version number following approval	Jo Milton
2.1	4th July 2022	2.1, 3.4, 5.3, 6.1, 7.1 – updated owner and sponsor Font updated to Nunito Sans	Jo Milton
2.2	4th October 2022	**Annual Review** Policy name amended to Network Monitoring and Branch Assurance Support Policy Throughout - Updated ‘Audit’ to ‘Branch Assurance’ and SPEAR visit to Support visit 2.5 and 3.5 - Addition of new risk “Consistent completion of Branch Assurance Visits” and related controls 5.2 ‘Whistleblowing’ changed to ‘Speak Up’	David Southall
3.0	5th December 2022	Updated to full version number following approval at ARC	Jo Milton
3.1	19th June 2023	Updated owner	Jo Milton
3.2	8th December 2023	Updated owner and implementer 1.1 Clarified Establish Loss/Gain definitions 3.1 Amended risk exception statement 3.2 Updated framework policy name – Contract Termination Decisions Review 3.4 added Service & Supports Insights Manager 4.3 Update to process for scheduling a visit	Jo Milton
3.3	25th March 2024	**Annual Review** Throughout: Removal of reference to unannounced visits and updating of ‘investigation’ to ‘review’ 1.1 Updated definitions 2.5 Removal of contractual discrepancy text. Risks amended to reflect ServiceNow 3.5 Minimum Control Standards changed to Policy Required Operational Standards 4.2 Removal of non-suspension monitoring section	Mike Lowe/Alison Clark

		4.3 Amended the circumstances when a Branch Assurance Advisor would contact a Contract Advisor. 4.7 Amendments to reflect new QA process and postmaster CSAT 4.8 Addition of reports for weekly stakeholder meetings 5.2 Addition of Speak Up and NFSP contact details	
4.0	21st May 2024	Updated to full version number following approval at ARC	Jo Milton
4.1	24th July 2024	Updated Casework team to Operational Support team throughout 1.1 Remove definitions of Local, Main and SPSO branches 4.2 Amended to clarify that a visit will be arranged with the postmaster unless in exceptional circumstances. 4.3 and 4.4 Amended “Smart ID” to “ID” for simplicity 4.5 Security incident visit trigger increased from £1000 to £5000 (approved at RC July24)	Jo Milton

7.2 Oversight committee

Oversight Committee: Risk and Compliance Committee and Audit, Risk and Compliance Committee

Committee	Date approved
POL R&CC	7th May 2024
POL ARC	22nd May 2024

Next review: 31 MAY 2025

7.3 Company details

Post Office Limited and Post Office Management Services Limited are registered in England and Wales. Registered numbers 2154540 and 08459718 respectively. Registered Office: Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ.

Post Office Management Services Limited is authorised and regulated by the Financial Conduct Authority (FCA), FRN 630318. Its Information Commissioners Office registration number is ZA090585.

Post Office Limited is authorised and regulated by Her Majesty’s Revenue and Customs (HMRC), REF 12137104. Its Information Commissioners Office registration number is Z4866081.

VAT registration number GB 172 6705 02. Registered office: Finsbury Dials, 20 Finsbury Street, London, England EC2Y 9AQ

POL00448252

POST
OFFICE