POL00447923

GROUP POLICY

Cooperation with Law Enforcement Agencies and Addressing Suspected Criminal Misconduct

Version – V0.3

POL00447923

POL00447923

1. Overview

1.1. Introduction by the Policy Owner

The General Counsel has overall accountability to the Board of Directors for the design and implementation of controls relating to cooperation with Law Enforcement Agencies and the manner in which Post Office addresses suspected criminal misconduct. Cooperation with Law Enforcement Agencies and addressing criminal misconduct is an agenda item for the Audit and Risk Committee and the Post Office Board is updated as required.

1.2. Purpose

Post Office receives a large number of requests to assist Law Enforcement Agencies in the prevention, detection, investigation and potential prosecution of alleged offences. It also has legal obligations to provide information to Law Enforcement Agencies (e.g. through suspicious activity reports) and may also wish voluntarily to notify Law Enforcement Agencies if it suspects that it, its Employees, Operators or Customers have been the victim of crime.

This Policy has been established to set the minimum operating standards relating to cooperation with Law Enforcement Agencies and the manner in which Post Office will address suspected criminal misconduct.[1] It is one of a set of policies which provide a clear risk and governance framework and an effective system of internal control for the management of risk across the Post Office. Compliance with these policies supports the Post Office in meeting its business objectives and to balance the needs of shareholders, employees[2] and other stakeholders.

1.3. Core Principles

Post Office's approach to cooperating with Law Enforcement Agencies is based upon the following core principles:

- Post Office is committed to supporting Law Enforcement Agencies in the prevention, detection, investigation and potential prosecution of alleged offences;
- Post Office will as far as possible cooperate with Law Enforcement Agencies and voluntarily provide information and evidence on request;
- Post Office is committed to ensuring that prosecutions are fair and that Prosecution Teams are made aware of, and provided with, Disclosable Material in Post Office's possession;
- Post Office will manage the risks associated with providing such cooperation, by ensuring that appropriate controls are in place in relation to the provision of information.

In accordance with these principles, and subject to the controls described in section 2.4 below, Post Office:

- will make a Victim Crime Report to the police where suspected criminal misconduct is identified in its business operations;
- will not conduct private prosecutions (Post Office's shareholder must be consulted and approval obtained from the Post Office Board if any deviation from this is contemplated);
- will provide information to Law Enforcement Agencies to assist the prevention, detection, investigation and potential prosecution of crime:

[1]In this Policy "Post Office" and "Group" means Post Office Limited, Post Office Management Services Limited and Payzone Bill Payments Limited.

[2]In this Policy "employee" means permanent staff, temporary including agency staff, contractors, consultants and anyone else working for or on behalf of Post Office.

POL00447923

- voluntarily for intelligence purposes, accompanied by an Advisory Note if required to describe any known issue/s which might affect the reliability of the information;
- voluntarily for use as evidence, where it is classified by Legal and Compliance as 'low risk data' for the purpose of this policy (see Appendix 1);
- voluntarily for use as evidence, if approved by Post Office Legal or any Nominated Criminal Law Advisors acting for Post Office; or
- as required by a Mandatory Order or otherwise approved by the Post Office Board.

1.4. Application

This Policy is applicable to all areas within the Post Office and defines the minimum standards to control financial loss, customer impact, regulatory breaches and reputational damage in line with Post Office's Risk Appetite.

In exceptional circumstances, where risk sits outside of Post Office's accepted Risk Appetite a Risk Exception can be granted. For further information in relation to the risk exception process please contact the Central Risk team.

For definitions please see section 3.1.

The risk to Post Office in relation to cooperation with Law Enforcement Agencies and the manner in which it addresses suspected criminal misconduct is reviewed by the Board annually.

1.5. The Risks

Post Office is frequently asked to provide data and other information to support Law Enforcement Agencies and prosecutors in Criminal Investigations and prosecutions. This may arise either when Post Office is a victim of crime or when it holds data which is relevant to other suspected criminal misconduct. Post Office also has legal obligations to provide data in some circumstances, for example suspicious activity reports.

Provision of appropriate and reliable information to Law Enforcement Agencies promotes the administration of justice. Compliance with this policy will ensure:

- Suspected criminal misconduct is subject to proper review before it is reported to a Law Enforcement Agency;
- Proper consideration is given to information that may be provided to Law Enforcement Agencies and Prosecution Teams, to assist them in complying with their duties of disclosure;
- Any issues with the reliability of provided information are identified and dealt with appropriately;
- Post Office is able to identify and verify information provided to Law Enforcement Agencies at a later date.

1.6. Legislation

There are a number of relevant legal and regulatory requirements which are applicable, including (but not limited to):

- Criminal Procedure and Investigations Act 1996
- Proceeds of Crime Act 2002
- Terrorism Act 2000
- The Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017
- Crime and Courts Act 2013

In addition, Post Office can be legally required to provide information if it is served with a compulsory order from a Court or Law Enforcement Agency (e.g. under Schedule 1 of the Police and Criminal Evidence Act 1984, or section 2 of the Criminal Procedure (Attendance of Witnesses) Act 1965).

POL00447923

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

A Risk Appetite is the extent to which the Group will accept that a risk might happen in pursuit of day to day businesses transactions. It therefore defines the boundaries of activity and levels of exposure that the Group is willing and able to tolerate.

The Group takes its legal and regulatory responsibilities seriously and consequently has[3]:

- **Tolerant risk appetite** for Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality.
- **Averse risk appetite** for litigation in relation to high profile cases/issues.
- **Averse risk appetite** for litigation in relation to Financial Services matters.
- **Averse risk appetite** for not complying with law and regulations or deviation from business' conduct standards for financial crime to occur within any part of the organisation.
- **Averse risk appetite** in relation to unethical behaviour by our staff.

The Group acknowledges however, that in certain scenarios even after extensive controls have been implemented, a matter may still sit outside the agreed Risk Appetite. In this situation, a risk exception waiver will be required.

2.2. Policy Framework

Post Office has established a suite of financial crime policies and procedures, on a risk sensitive approach which are subject to an annual review and which are relevant to this Policy. The Policy suite is designed to combat money laundering, terrorist financing, bribery, corruption and fraud and ensure adherence to relevant sanctions regimes.

2.3 Who must comply?

Compliance with this Policy is mandatory for all Post Office employees.

Where non-compliance is identified, the matter must be referred to the General Counsel. Where it is identified that an instance of non-compliance is caused through wilful disregard or negligence, this will be treated as a disciplinary offence.

[3] The Risk appetite was agreed by the Group's Board January 2015

POL00447923

2.4 Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks, so they remain within the defined Risk Appetite statements. There must be mechanisms in place within each business unit to demonstrate compliance. The minimum control standards 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 minimum control standards in consideration of the stated risk appetite. The subsequent pages define the terms used in greater detail:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Making a Victim Crime Report	Post Office does not have appropriate oversight over any Victim Crime Report made by Post Office or its employee/s.	Preventative Control: Where Post Office suspects that it, its Employees, Operators or Customers may have been the victim of crime, Post Office Legal must assess whether a Victim Crime Report should be made. The General Counsel shall make the final decision on whether to make a Victim Crime Report. When Post Office makes a Victim Crime Report, it will be for third party Law Enforcement Agencies and Prosecution Teams to consider whether further action (e.g. a prosecution) should be taken.	General Counsel	
Conduct of Private Prosecutions	All duties as a private prosecutor are not discharged.	Directive Control: Post Office shall not conduct Private Prosecutions or Criminal Investigations with a view to bringing Private Prosecutions. Post Office must consult with its shareholder if any deviation from this is contemplated.	The Department for Business Energy & Industrial Strategy and the Post Office Board.	

POL00447923

Provision of information to Law Enforcement Agencies	The provision or withholding of information to Law Enforcement Agencies conflicts with other legal obligations or rights.	Preventative Control: Any material to be disclosed which is not Low Risk Data as classified by this Policy will be submitted for review by Post Office Legal (or by any Nominated Criminal Law Advisors acting on their behalf) prior to disclosure. Post Office Legal will make the final decision on what material shall be disclosed and on what basis. Nothing in this Policy shall permit the voluntary disclosure of information where that would result in non-compliance with other legal obligations (e.g. the Data Protection Act 2018 or General Data Protection Regulation). All policies and processes which support this Policy shall expressly state that nothing in the Policy or associated documents shall prevent Post Office or its employees from complying with legal obligations and/or the requirement to protect, to the fullest extent possible, the identity of whistle-blowers. Mandatory Orders must be sought if necessary to ensure the lawful provision of information, unless disclosure is otherwise approved by the General Counsel.	Recipient of request for disclosure & General Counsel	
Provision of information to Law Enforcement Agencies	If Post Office does not deal and continue to deal appropriately with any issues concerning the reliability of information it	Preventative Control: Where any Post Office employee receives a request to provide information to a Law Enforcement Agency, they must direct that	All Employees	

POL00447923

	has provided to Law Enforcement Agencies, this could result in improper reliance on that information and/or unsafe convictions.	request to Legal, Compliance or Security to manage. <u>Preventative Control</u>: Where such a request is received by or escalated to Legal, Compliance or Security and relates to the provision of information for intelligence purposes, Legal, Compliance or Security shall comply with the "Flowchart: Provision of Data to Law Enforcement for Intelligence Purposes" tool (Tool 1) in determining whether/how to respond. Tool 1 provides that additional controls must be complied with in respect of data listed in Appendix 2. <u>Directive Control</u>: Where Post Office or its employees are asked or compelled to provide witness statements relating to any information that is not Low Risk Data, the request must be escalated to Post Office Legal. <u>Preventative Control</u>: Post Office Legal (or any Nominated Criminal Law Advisors acting on their behalf) will assess the risks in providing that data and determine whether the evidence can be provided on a voluntary basis, whether a Mandatory Order or Board approval is required, whether any information so provided should be accompanied by an Advisory Notice, and/or whether any other risk mitigation action is appropriate. <u>Preventative Control</u>:	General Counsel/ Group Operations Director All Employees General Counsel All Employees	

POL00447923

		Post Office Employees must notify Post Office Legal if they become aware of any issues which may undermine the reliability of any information provided to Law Enforcement Agencies, and/or if any additional types of information not presently recorded in Appendix 3 are provided to Law Enforcement Agencies. Post Office Legal must review this Policy, its Appendices and any Advisory Notices and apply and/or revise them as appropriate if it becomes aware of any issues that may undermine the reliability or accuracy of any information provided to Law Enforcement Agencies.	All Employees and General Counsel	
Provision of information to Law Enforcement Agencies	Information provided to a Law Enforcement Agency is not retained such that Post Office cannot subsequently identify and/or verify the information provided.	<u>Preventative Control</u>: Centralised records shall be maintained for the longer of 6 years or until the end of any criminal proceedings: 1. of any Victim Crime Report made by Post Office to the police; 2. of any known ongoing Criminal Investigation or prosecution arising from a Victim Crime Report or where Post Office has been asked to provide assistance; 3. of any information, data, material or evidence (witness statements or exhibits) provided to Law Enforcement Agencies.	General Counsel/ Group Operations Director	
Provision of information to Law	If Post Office does not monitor ongoing investigations and	<u>Preventative Control</u>: Post Office shall maintain a list of known ongoing Criminal Investigations where Post	Group Operations Director	

POL00447923

Enforcement Agencies	prosecutions by Law Enforcement Agencies, Post Office may not be aware of issues arising in such cases and/or may fail to identify material in its possession which satisfies the Disclosure Test.	Office or its Employees or Operators are the victim and any Public Prosecutions of which it is aware, updated with developments and reported regularly to the General Counsel. <u>Preventative Control</u>: Post Office shall make regular contact with the Prosecution Team to request an update in relation to any developments in the case, so that Post Office can identify and if appropriate provide any further Disclosable Material in the case. <u>Preventative Control</u>: Any additional material to be disclosed will be submitted to Post Office Legal for review by them or Nominated Criminal Law Advisors prior to its disclosure.	Group Operations Director General Counsel/ Group Operations Director	
Training	Breaches of the Policy occur as a result of inadequate training	Preventative Control: Training shall be provided to ensure that those to whom the Policy applies understand their obligations and how to fulfil them.	General Counsel/ Compliance Director	

POL00447923

3. Tool & Definitions

3.1. Tool

1. Flowchart: Provision of Data to Law Enforcement for Intelligence Purposes

The Provision of Data to Law Enforcement for Intelligence Purposes flowchart has been designed to determine the level of risk exposure and escalation required when providing data to external Law Enforcement Agencies for intelligence purposes. It sets out the process which must be followed in all cases where Post Office employees or associates are asked or compelled to provide information to Law Enforcement Agencies. (see below).

3.2 Definitions

"**Advisory Notice**" – refers to the Notice which must be sent to any Law Enforcement Agency where required by Tool 1 or Appendix 2.

"**Criminal Investigation**" – refers to an investigation conducted to the criminal standard, for the primary purpose of ascertaining whether a person should be charged with a criminal offence.

"**Disclosable Material**" – refers to material which satisfies the Disclosure Test.

"**Disclosure Test**" – refers to the test set out in s.3 Criminal Procedure and Investigations Act 1996. Material is said to satisfy the disclosure test if it might reasonably be considered capable of undermining the case for the prosecution or of assisting the case for the accused.

"**Law Enforcement Agencies**" – refers to any agency which is responsible for law enforcement in the United Kingdom, including (but not limited to): police forces, the National Crime Agency, Her Majesty's Revenue and Customs, Immigration Enforcement and Border Force, the Financial Conduct Authority, the Information Commissioner's Office, the Prudential Regulation Authority, and the Office of Communications (commonly known as OfCom). Where a Law Enforcement Agency also conducts regulatory (or other functions), this Policy apples to circumstances in which the body is exercising criminal law or regulatory investigation or enforcement functions.

"Low Risk Data" – refers to the categories of data which have been identified in Appendix 1 as being "low-risk".

"**Mandatory Order**" – refers to an order or notice that Post Office is legally required to comply with (including, but not limited to: a witness summons or a production order).

"**Nominated Criminal Law Advisors**" – refers to external criminal legal advisors that may from time to time be appointed by Post Office Limited.

"**Operator**" – refers to Franchisees and Agents of Limited Companies who operate Post Office Limited Branches.

"**Private Prosecution**" – a prosecution brought by, or on behalf of, Post Office Limited, rather than by a Law Enforcement Agency or public prosecutor.

"**Prosecution Team**" – refers to the individuals who are responsible for the investigation and prosecution of a criminal case. This will most commonly be the police officer in charge of the investigation and the Crown Prosecution Service reviewing lawyer who has conduct of the case, but extends to any external law enforcement investigator and reviewing lawyer.

"**Public Prosecution**" – refers to a prosecution brought by a Law Enforcement Agency or public prosecutor (such as the Crown Prosecution Service).

"**Victim Crime Report**" – refers to a report made by Post Office to the police when Post Office suspects that it or its Operators or customers may have been the victim of criminal misconduct connected with the Post Office.

POL00447923

4. Where to go for help

4.1. Additional Policies

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

4.2. How to raise a concern

Any Post Office employee who suspects that there is a breach of this Policy should report this without any undue delay.

Whistleblowing can be reported via the following channels:

- Their line manager,
- A senior member of the HR Team, or
- If either or both are not available, staff can contact the Post Office's Whistleblowing Officer, who can be contacted by email at: whistleblowing GRO or by telephone on: GRO.
- The confidential Whistleblowing Speak Up service 'Ethicspoint' provided by Navex Global via telephone on GRO, or
- Via a secure on-line web portal: http://postoffice.ethicspoint.com/ In some instances it may be appropriate for the individual to report in the form of a complaint to Grapevine, the Customer Support Team or the Executive Correspondence Team.

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 Post Office Legal team.

POL00447923

5. Governance

5.1. Governance Responsibilities

The Policy sponsor, responsible for overseeing this Policy is the General Counsel of Post Office Limited.

The Policy owner is the General Counsel who is responsible for ensuring that the Compliance Director conducts an annual review of this Policy and tests compliance across the Post Office. Additionally, the General Counsel and the Compliance Director are responsible for providing appropriate and timely reporting to the Risk and Compliance Committee and the Audit and Risk Committee.

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

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

POL00447923

6. Control

Date	Version	Updated by	Change Details
25 July 2020	0.1		

6.1. Policy Approval

Committee	Date Approved
GE	12 August 2020
POL Board	22 September 2020

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

Policy Sponsor: Ben Foat

Policy Owner: Ben Foat

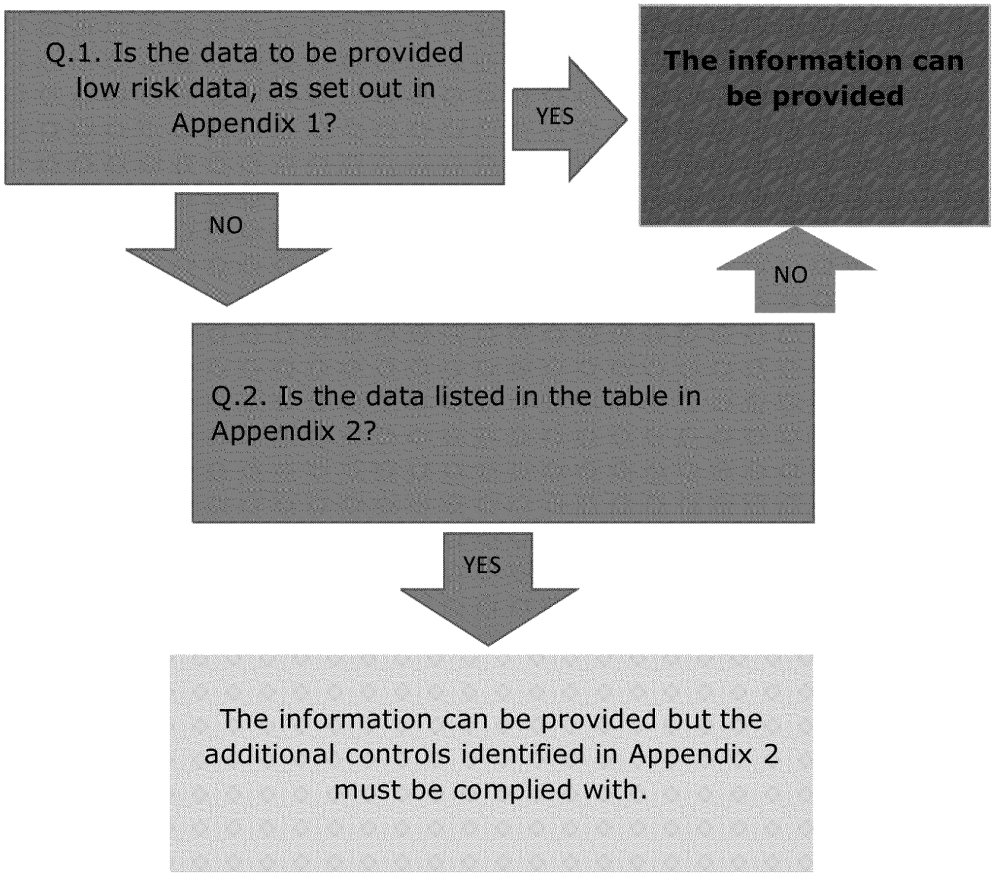
Policy Author: Rodric Williams

Next review: 24/07/2021

POL00447923

Tool 1: Flowchart: Provision of Information to Law Enforcement for Intelligence Purposes

1. This Tool is to be used when Post Office receives a request to provide data to law enforcement agencies for **intelligence** purposes only. If at any stage, a request is made for a witness statement, or for data to be exhibited for use in evidence, please seek advice from Post Office Legal, unless the data is 'low risk', as set out in Appendix 1.



2. Nothing in this Tool shall be interpreted as permitting the voluntary disclosure of data where such provision would result in non-compliance with other legal obligations (for example, but not limited to, the Data Protection Act 2018 or the General Data Protection Regulation). Mandatory Orders must be sought if necessary, to ensure the lawful provision of data.

POL00447923

Cooperation with Law Enforcement Agencies and Addressing Suspected Criminal Misconduct

Appendix 1

1. Although the following categories of data contain personal data (as defined by the Data Protection Act 2018), they have been classified by Legal and Compliance as 'low risk data' for the purpose of this policy. Such data can be supplied to Law Enforcement Agencies without referral to Post Office Legal:[4]

    i. CCTV;
    ii. Audio recordings;
    iii. Confirmation of a bank card number used in a particular transaction;
    iv. Details of a payment made using a particular bank card;
    v. HR records;
    vi. Data derived from the Brands Database;
    vii. The name / address / phone number / driving licence number / passport number provided by a customer during a transaction;
    viii. Safe opening and closing times.

2. The business can apply to Legal and Compliance to add/ remove items to/from this list. Such requests should be sent to Post Office Legal.

[4] In the event that the reader has doubt about whether data can be supplied to a Law Enforcement Agency, they should contact the Data Protection Team for clarification.

POL00447923

Cooperation with Law Enforcement Agencies and Addressing Suspected Criminal Misconduct

Appendix 2

1. The following categories of data have been identified as requiring additional controls before the data can be provided to a law enforcement agency:

Type of data	**Additional controls required when providing data for intelligence purposes**
Data deriving from Legacy Horizon or HNG-X	The following Advisory Notice must be provided: "Post Office Limited wishes to assist law enforcement agencies wherever possible. However, please note that the information provided derives in whole or in part from a historic version of the Horizon computer system used by Post Office. The accuracy and reliability of data deriving from this version of Horizon was the subject of the recent High Court case of *Bates & Ors v Post Office Ltd* (No 6: Horizon Issues) [2019] EWHC 3408. Furthermore, the CCRC has recently referred the convictions of 4 individuals whose cases featured evidence derived from the Legacy Horizon and HNG-X systems to the Court of Appeal."
[Add further data types as necessary]	*[Draft Advisory Notice as appropriate, drawing attention to any potential issue identified]*

POL00447923

Appendix 3

Categories of data which Post Office provides to Law Enforcement Agencies[5]

Type of request/provision of data	Law Enforcement Agencies making request	Responsibility for responding to request (Security, Compliance etc)	Type of data sought / provided	Underlying system	Is the data held by POL or a third party (e.g. Fujitsu)
Raising Suspicious Activity Reports ("SARs")	Reports to National Crime Agency("NCA") required under the Money Laundering Regulations	Compliance	1)Details of customers who travel branch to branch making Bureau de Change transactions / make large Foreign Exchange cash transactions; 2)Details of POL staff members who regularly split Bureau transactions so that they are under the ID threshold; 3)Names of branches processing unusually large amounts of cash; 4) the identity of a card used in a particular transaction and details of other branches in which that card was used, for example, details of banking deposits made through Link. 5) CCTV	1)Horizon and AML Credence 2)Horizon, Credence and AML Credence 3) Credence and Branch Finder 4) TESQA 5) CCTV system	1)Horizon data and Credence data is held by POL 2) Horizon data and Credence data is held by POL 3) Credence and Branch Finder data are held by POL 4)TESQA data is held by POL

[5]This table has been prepared using information provided by the business as of May 2020. It is possible therefore that this table is not a comprehensive list of all types of data which POL provides to Law Enforcement Agencies. It will be updated as the Policy Owner is made aware of additional types of data which POL provides to Law Enforcement Agencies not already captured within the table; or when new requests, for types of data not previously requested by Law Enforcement Agencies are made.

POL00447923

Type of request/provision of data	Law Enforcement Agencies making request	Responsibility for responding to request (Security, Compliance etc)	Type of data sought / provided	Underlying system	Is the data held by POL or a third party (e.g. Fujitsu)
					5) CCTV data is held by POL and agents
Responding to requests from the NCA / regulator etc for further details relating to SARs which have been raised by POL	NCA / regulator	Compliance	As above	As above	As above
SAR disclosures (when POL is asked to provide data in response to a SAR raised by another agency where the SAR names an individual linked to POL)	NCA	Compliance	1)Details relating to the subject of the SAR (e.g. confirmation that the individual works for POL and which branch they work in) 2)Details of Horizon User that processed transactions reported in the SAR Disclosure (e.g. confirmation the transactions were processed by the subject)	1)HR records 2)Credence	1)HR data is held by POL 2)Credence data is held by POL
Responding to JMLIT requests pursuant to s.7 Crime and Courts Act 2013 • Normal s.7 requests (6	HMRC / Financial Conduct Authority / NCA / Serious Fraud Office / Home Office / police / banks	Compliance	1) Subject information captured on Brands - Details relating to a particular subject's footprint (email address, phone number, address, dob, products and services used 2) Branch bureau de Change transaction and customer information 3) Reports received by Grapevine	1)Horizon / Brands database 2)AML Credence	1)Horizon data is held by POL Brands data is held by POL. 2)Credence data is held by POL

POL00447923

Type of request/provision of data	Law Enforcement Agencies making request	Responsibility for responding to request (Security, Compliance etc)	Type of data sought / provided	Underlying system	Is the data held by POL or a third party (e.g. Fujitsu)
week turnaround) • Expedited s.7 requests (response asap, but normal office times) • Terrorist Incident s.7 requests (24/7/365 response required immediately) • Threat to life incident s.7 request (24/7/365 response required immediately)			4) SAR database recording details of all SARs received and reported to the NCA	3) King's Security systems 4) Excel spreadsheet held in secure AML drive 5)TESQA – if full card numbers are listed	3)King's Security systems 4)Excel spreadsheet in held by POL 5)TESQA data is held by POL
Responding to requests from regulatory bodies	HMRC	Compliance	Transactional data for audit purposes	Horizon AML Credence	Horizon data and Credence data is held by POL
Sharing intelligence / data	Regulator (if regulatory		Difficult to quantify. Could be transactional information from Horizon		

POL00447923

Type of request/provision of data	Law Enforcement Agencies making request	Responsibility for responding to request (Security, Compliance etc)	Type of data sought / provided	Underlying system	Is the data held by POL or a third party (e.g. Fujitsu)
following a whistleblowing investigation / sharing intelligence with regulators in the event that a regulatory breach is identified	breach is identified)				
Providing assistance following terrorist incidents	Police	Security Team / Compliance (this would be via a s.7 request)	Details of transactions made using a particular bank card	Horizon	Horizon data is held by POL
Assisting missing persons enquiries	Police	Security Team	Confirmation of whether a bank card has been used / whether there has been other activity on the missing person's account(s)	Horizon	Horizon data is held by POL
Providing intelligence or evidence in relation to incidents which have occurred on the "public side of the counter" e.g. robbery in the branch	Police/ HMRC / NCA / Bank Fraud Department / SFO / Immigration	Security Team	1) CCTV; 2) confirmation of a bank card number used in a particular transaction; 3) details of a payment made or transaction undertaken using a particular bank card; 4) requests for information about whether an individual's bank card has been used in the PO network; 5) Branch alarm data; 6) Safe data (opening/closing times)	1) CCTV system 2) Horizon 3) Credence 4)HoRice 5)TEQSA 6)Grapevine	1) CCTV data is held by POL and agents 2) Horizon data is held by POL 3) Credence data is held by POL 4) HoRice data is held by POL

POL00447923

Type of request/provision of data	Law Enforcement Agencies making request	Responsibility for responding to request (Security, Compliance etc)	Type of data sought / provided	Underlying system	Is the data held by POL or a third party (e.g. Fujitsu)
					5) TESQA data is held by POL. 6) Grapevine and ARQ data is POL data but it is held externally. ARQ data is held by Fujitsu.
Providing intelligence or evidence in relation to incidents occurring on the "post office side of the counter" e.g. where a PO staff member is accused of theft from the branch.	Police / NCA / HMRC	Security Team	1) Branch trading statements 2) cash declarations 3) ARQ data 4) HR records 5) calls made to Post Office helplines (e.g. NBSC helpline)	1) Horizon 2) Horizon 3) Horizon 4) HR records 5) Puzzle Server	1-3) Horizon data is held by POL 4) HR records are held by POL. 5) Helpline recordings are held by POL on the puzzle server.
Information requested via a DPA request	HMRC / NCA / police / banks	Financial Crime Team / Security Team	1) Customer and transactional details 2) Names of branches processing unusually large amounts of cash;	1) Horizon and Credence	1)Horizon data&

POL00447923

Type of request/provision of data	Law Enforcement Agencies making request	Responsibility for responding to request (Security, Compliance etc)	Type of data sought / provided	Underlying system	Is the data held by POL or a third party (e.g. Fujitsu)
			3) the identity of a card used in a particular transaction and details of other branches in which that card was used; details of banking deposits made through Link; 4) CCTV	(including AML Credence) 2) Credence and Branch Finder 3) TESQA 4) CCTV system	Credence data is held by POL 2) Credence and Branch Finder data is held by POL 3)TESQA data is held by POL 4)CCTV data is held by POL and Agents
Ofcom information requests under S135, S136 or S137 of the Comms Act 2003.	Ofcom	Compliance	Various types 1)Revenues and volumes of traffic customer numbers traffic usage. 2)Documents and correspondence such as emails and letters with any party.	Various sources 1)Most volume and network data is provided by Fujitsu and is extracted on a bespoke basis by them. 2)Emails are held in the email system Mimecast. 3)Documents held on sharepoint and	Various holders 1)Fujitsu are external supplier and hold information on behalf of POL. 2)Mimecast is external 3)Sharepoint and Laptops are POL owned.

POL00447923

Type of request/provision of data	Law Enforcement Agencies making request	Responsibility for responding to request (Security, Compliance etc)	Type of data sought / provided	Underlying system	Is the data held by POL or a third party (e.g. Fujitsu)
				employee laptops.	