

1.0 Policy Statement

Saffron and its wholly owned subsidiaries are committed to the prevention, detection and reporting of money laundering. This policy sets out the general approach it will adopt in furtherance of this.

Saffron recognises that money laundering risks are closely related to risks of other financial crime, including fraud and bribery. It operates a separate policy that deals with these discrete issues.

2.0 Policy Scope & Objectives

2.1 This policy applies to all employees, board and committee members. Failure by an employee or board or committee member to comply with this policy and procedure may lead to disciplinary action. It also applies to contractors, consultants and agents acting on behalf of Saffron where they are involved in relevant financial transactions or property dealings.

2.2 This policy and procedure is intended to comply with these regulations:

- Anti-Terrorism, Crime and Security Act 2001.
- Proceeds of Crime Act 2002 (POCA) (as amended by the Serious Organised Crime and Police Act 2005).
- Criminal Finances Act 2017.
- Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.
- Terrorism Act 2000 (as amended).
- The Money Laundering and Terrorist Financing (Amendment) Regulations 2019.
- The Money Laundering and Terrorist Financing (Amendment) (EU Exit) Regulations 2020.

2.3 The Proceeds of Crime Act 2002 (POCA) identifies money laundering offences as:

- Concealing, disguising, converting, transferring or removing criminal property from the UK.
- Entering into or becoming involved in an arrangement which facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person.
- Acquiring, using and or possessing criminal property.
- Failure to disclose knowledge or suspicion of money laundering.
- 'Tipping off' any person that such a disclosure has been made.
- Prejudicing an investigation – where a person knows or suspects that a money laundering investigation is being, or is about to be, conducted and takes action likely to prejudice that investigation (POCA 2002, s.342).

- 2.4 Not all of the Association's business is "relevant" for the purposes of the legislation. It is mainly accountancy, and property transactions undertaken by Legal Services, it is important that all employees are familiar with their legal responsibilities.
- 2.5 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017) requires 'relevant businesses' to put anti-money laundering systems in place for the purpose of identifying and preventing money laundering and reporting any suspicious activity.
- 2.6 'Relevant businesses' are obliged to register with a designated supervisory authority, such as the Financial Conduct Authority or His Majesty's Revenue and Customs (HMRC), as determined by the nature of their activities.

3.0 Definition of Money Laundering

- 3.1 Money laundering is defined as the process by which criminally obtained money or assets are exchanged for 'clean' money or assets with no obvious link to their criminal origins. Such criminal property can typically be derived from drugs trafficking, corruption, tax evasion, or theft. It also covers money, however come by, which is used to fund terrorism.

- 3.2 Money laundering can take several forms:

- Handling the proceeds of crime.
- Being directly involved with criminal or terrorist property.
- Entering into arrangements to facilitate the laundering of criminal or terrorist property.
- Investing the proceeds of crime into financial products, property purchase or other assets (such as Shared Ownership, Right to Buy or Right to Acquire sales).
- Using rental income derived from criminal activity to service or obscure illegitimate funds.
- Paying inflated prices for services or assets with no legitimate commercial justification.

- 3.3 Any employee could potentially be liable under money laundering laws if they suspect money laundering, become involved, and fail to act. While the risk to Saffron itself of violating these laws is low, it's crucial for all employees to understand their legal responsibilities, as serious criminal penalties may apply for regulatory breaches.

- 3.4 The key requirement is to promptly report any suspicious transaction or activity to the **Chief Commercial Officer**, who is the nominated Money Laundering Reporting Officer (MLRO). The MLRO's responsibility is to decide whether to send a report or 'disclosure' about the incident to the NCA. The report is called a 'Suspicious Activity Report'. (see section 3.5 below).

3.5 Money Laundering Reporting Officer (MLRO) and Deputy MLRO

- 3.5.1 Saffron shall at all times maintain a nominated Money Laundering Reporting Officer (MLRO). The MLRO holds statutory responsibilities under the Proceeds of Crime Act 2002 and the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, and must be a sufficiently senior member of staff with the authority, resources and access to information necessary to fulfil the role effectively.
- 3.5.2 Saffron shall also designate a Deputy MLRO, who shall act in the capacity of MLRO where the MLRO is absent (including annual leave, sickness or other planned or unplanned absence), has or may have a conflict of interest in relation to a specific report or matter, or where the MLRO post is temporarily vacant.
- 3.5.3 The Deputy MLRO shall have the same authority and access as the MLRO when acting in that capacity.
- 3.5.4 The current MLRO and Deputy MLRO post-holders are recorded in Appendix B to this policy, maintained by the Company Secretary and updated upon any change in post-holder.
- 3.5.5 Neither the MLRO nor the Deputy MLRO should be the same individual who originally submitted a Suspicious Activity Report internally – they must be able to take an independent view of the matter reported.
- 3.5.6 The appointment of the MLRO and Deputy MLRO shall be reported to the Audit and Risk Committee on an annual basis, or immediately upon any change.

4.0 Anticipating and preventing Money Laundering

- 4.1 Many criminals use property purchase as a means of laundering the proceeds of crime. Criminals will also use properties for illegal activities, such as drug dealing, prostitution and cannabis cultivation. By definition, money laundering involves the proceeds of crime. If we allow criminals to launder their money, we are allowing them to profit from their crimes – this could lead to serious reputational damage.
- 4.2 Saffron could suffer in a number of ways from the activities of money launderers who misuse properties, often causing serious damage and illegally sub-letting or occupying properties, and thereby reducing available housing stock.
- 4.3 Saffron could take on a new supplier whose company has been set up to launder the proceeds of crime or sell a home to someone who is laundering money. If financial transactions which Saffron has entered into are later proven to be related to criminal activities, we could be exposed to financial loss.

- 4.4 It is not possible to give a definitive list of ways to identify potential money laundering or guidance on how to decide whether to report suspicious activities. Risk factors that, either alone or collectively, might suggest the possibility of money laundering activity could include:
- A new customer seeking to procure assets or services from the Group.
 - A secretive person or business that, for example, refuses to provide requested information without a reasonable explanation.
 - Payment of any substantial sum in cash.
 - Concerns about the honesty, integrity, identity or location of the people involved.
 - Involvement of an unconnected third party without a logical reason or explanation.
 - Overpayments for no apparent reason.
 - Absence of any legitimate source for the funds received.
 - Significant changes in the size, nature, frequency of transactions with a customer that is without reasonable explanation.
 - Cancellation, reversal or requests for refunds of earlier transactions.
 - Requests for account details outside the normal course of business.
 - A history of poor business records, controls or inconsistent dealing.
 - A customer or supplier who is identified as, or connected to, a Politically Exposed Person (PEP), or a close family member or known close associate of a PEP (see section 8A).
 - Use of complex or unusual legal arrangements or ownership structures without apparent commercial purpose.
 - A transaction involving a jurisdiction with a high risk of money laundering or terrorist financing, as identified by the Financial Action Task Force (FATF).
- 4.5 Staff will be advised on checks and control measures relevant to their own areas of work, and how these should be implemented.

5.0 Obligations

- 5.1 Organisations falling under the money laundering regulations must:
- Appoint a MLRO and a Deputy MLRO to receive disclosures from employees of money laundering activity.
 - Implement a procedure for employees to report any suspicious activity.
 - Maintain client identification procedures (customer due diligence) in certain circumstances.
 - Maintain good record keeping.
 - Appoint a Deputy MLRO to cover the MLRO's absence or where a conflict of interest arises.
 - Apply enhanced due diligence (EDD) in higher-risk situations, including those involving PEPs and their family members or close associates.

- Provide appropriate training to all relevant staff, the MLRO and the Deputy MLRO.
- Conduct and document a written risk assessment proportionate to the size and nature of Saffron's activities.

6.0 Disclosing Suspicious Activity

- 6.1 Exceptionally large cash payments are deemed to be suspicious. No payment will be accepted in cash if it exceeds £5,000, other than in exceptional circumstances and with the authority of the relevant Director and the MLRO. Any such transactions will be reported immediately to the MLRO.
- 6.2 A supplier or customer may make an unusual request that doesn't seem to make sense or seek to engineer a transaction that doesn't add up commercially. Where there is suspicious activity or a suspicious transaction, or an employee becomes concerned that their involvement in a matter may amount to a prohibited act under the legislation, this must be immediately reported in confidence to the MLRO, or, if the MLRO is unavailable or has a conflict of interest, to the Deputy MLRO. Any delay may render the employee liable to prosecution.
- 6.3 The MLRO will ask for as much detail and documentation as possible. For example:
- Details of the people involved (name, address, company names, directorships, phone numbers).
 - Details of the nature of involvement.
 - Types and dates of money laundering activity involved.
 - Whether the transactions have happened, are ongoing or imminent.
 - Where they took place and how they were undertaken.
 - The (likely) amount of money or assets involved.
 - The reason to be suspicious.
 - Any other information to enable a sound judgment to be made on whether there are reasonable grounds for suspicion.
 - Whether the person involved is, or is connected to, a Politically Exposed Person (PEP), or a family member or known close associate of a PEP.
 - Any known beneficial ownership information in relation to corporate or business parties involved.
- 6.4 The MLRO will take over the enquiry and the employee must follow their directions and on no account make any further enquiries. All employees will be required to co-operate with the MLRO, the Deputy MLRO and the authorities in any subsequent investigation.
- 6.5 At no time should the employee voice any suspicions to the person(s) suspected of money laundering, even if consent is given by the MLRO to the transaction proceeding. Otherwise, a criminal offence of "tipping off" will be committed.

- 6.6 Where a suspicious activity report concerns the MLRO themselves, the report must be made directly to the Deputy MLRO. Where both the MLRO and the Deputy MLRO are themselves the subject of the report, or where both are otherwise implicated, the report must be made directly to the Board Chair or, where that is not practicable, to the relevant external authority (including the NCA). In such circumstances, the employee making the report should seek appropriate legal advice as necessary.

7.0 Consideration by the MLRO

- 7.1 The MLRO (or the Deputy MLRO acting in that capacity) will acknowledge the employee's report and respond within 5 working days of receipt of the report.
- 7.2 The MLRO will normally suspend the transaction if they suspect money laundering or terrorist financing. They will consider the report and make other confidential enquiries including:
- Reviewing other transaction patterns and volumes.
 - The length of any business relationship involved.
 - The number of any one-off transactions and linked one-off transactions.
 - Any identification evidence held.
 - Whether enhanced due diligence has been applied and what it revealed.
 - Whether any PEP, family member or close associate connection has been identified.
 - Whether source of funds or source of wealth information has been obtained and verified.
- 7.3 The MLRO will report the matter to the NCA if there is clear evidence of money laundering, or if there are reasonable grounds to suspect that it is taking place.
- 7.4 Where it is decided that consent is required from the NCA for a transaction to proceed, the transaction must not be undertaken until the NCA has specifically given consent. The NCA will respond with a decision within 7 working days. Otherwise, there is deemed consent that there is no objection from the NCA. Where the NCA issues a moratorium period (currently up to 31 calendar days following the initial 7 working day period), no transaction to which the SAR relates shall proceed during that moratorium.
- 7.5 Where the MLRO concludes that there are no reasonable grounds to suspect money laundering, consent will be given for the transaction(s) to proceed.
- 7.6 The NCA analyses Suspicious Activity Reports (SAR) and uses them to identify the proceeds of crime. The NCA counters money laundering and terrorism by passing on important information to law enforcement information agencies so that they can act. The MLRO will commit a criminal offence if they do not make a disclosure as soon as practicable to the NCA when they know or suspect that a person is engaged in money laundering, following a report made by an employee.

8.0 Customer Due Diligence

8.1 Extra care should be always taken to check the identity of customers and clients. In undertaking due diligence and identity checks, due regard will be given to data protection principles.

8.2 **Private individuals** should be asked to provide evidence of their full name, residential address and date of birth. Verification must be based on reliable independent sources, through government-issued documents provided by the customer, or information obtained electronically, or both, such as a valid passport or national identity card, photo card driving licence, national identity card, work permit issued by the Home Office.

Alternatively, a government-issued document without a photo should be produced, containing their full name and supported by evidence of their address such as recent evidence of entitlement to benefits plus a utility bill, bank, building society or credit union statement, or a most recent mortgage statement from a recognised lender.

8.3 The evidence should be checked, to include spelling of names, validity, photo likeness, whether addresses match etc. If an employee visits a customer at his or her home address, a record of this visit can constitute a check on their address (as a second document).

8.4 **Corporate customers, partnerships and private companies** must provide information such as their company registration number, registered address, VAT registration and evidence that individuals have the authority to act for that entity. It may be necessary to establish the beneficial owners of such entities.

Verification of identification must be from reliable independent sources, such as a search of a relevant company registry, or confirmation of the company's listing on a regulated market. If there is a beneficial owner, Saffron will decide on a risk-sensitive basis how it verifies their identity. This may include requiring the customer to provide information directly or making use of publicly available documents.

8A. Politically Exposed Persons (PEPs), Family Members and Close Associates

8A.1 A Politically Exposed Person (PEP) is an individual who is, or has been, entrusted with a prominent public function, such as MP's and government ministers. Local councillors and other middle-ranking or more junior officials are not PEPs by virtue of that role alone.

8A.2 Under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, enhanced due diligence (EDD) must be applied to PEPs themselves, to family members of PEPs (including spouses or civil partners, children and their spouses or partners, and parents), and to known close associates of PEPs, including individuals known to have

joint beneficial ownership of legal entities or arrangements with a PEP, or who are otherwise closely connected to a PEP.

- 8A.3 Where a customer, applicant or counterparty is identified as a PEP, or a family member or close associate of a PEP, the following enhanced measures must be applied: approval from the MLRO (or Deputy MLRO) must be obtained before establishing or continuing a business relationship; reasonable measures must be taken to establish the source of wealth and source of funds involved in the transaction or business relationship; and enhanced and ongoing monitoring of the relationship must be conducted.
- 8A.4 The fact that a person is or was a PEP, or is a family member or close associate of a PEP, does not automatically mean that they are involved in money laundering. However, the elevated risk profile means that additional scrutiny is required.
- 8A.5 PEP status should be considered to persist for at least 12 months after the individual leaves the prominent public function. After that period, the MLRO should assess whether the risk level has reduced sufficiently to apply standard customer due diligence.
- 8A.6 Staff should use commercially available screening tools or publicly available information to identify PEP status. Any screening undertaken must be documented and retained in accordance with section 10.0 of this policy.

9.0 Sales, Disposals and Connected Individuals

- 9.1 This section applies in addition to the general requirements of this policy where Saffron is selling or disposing of a home, including Shared Ownership, Shared Equity, Right to Buy and Right to Acquire sales, and works alongside Saffron's other relevant policies and procedures governing property sales and connected individuals.
- 9.2 Before a sale proceeds, a Homeownership Officer must complete the identity, address and source of funds checks set out in section 8 (and, where applicable, section 8A) above and section 9.3 below, obtaining original documents from the purchaser and retaining copies in line with section 10 (Record Keeping).
- 9.3 Purchasers must provide documentary evidence of the source of funds being used towards a purchase. This may include, but is not limited to: savings, release of a pension, sale of shares, sale of another property, inheritance, dividends from a UK company, gambling winnings, and compensation awards. In each case, evidence must link the funds to a legitimate source before the sale can proceed.

9.4 Gifted deposits, loans and beneficial interests

- 9.4.1 Where a purchaser is receiving money from a third party towards a purchase, Saffron must establish whether this is a gift, a loan, or gives rise to a

beneficial interest in the property, and obtain evidence of the relationship between the purchaser and the person providing the funds.

- 9.4.2 Gifted deposits will only be accepted from a purchaser's immediate family (spouse or civil partner, parent, sibling or child). Gifts from any other source, including extended family, friends or unconnected third parties, will not be accepted.
- 9.4.3 Where a gift is accepted, Saffron will require confirmation of the relationship between the purchaser and the donor, proof of the donor's identity and source of funds, and written confirmation that the sum is a gift with no rights retained over the property.

9.5 Connected individuals

- 9.5.1 A purchaser may be considered a connected individual where they are an employee of Saffron, a close relative of an employee, a Saffron Board member or close relative of a Board member, anyone involved in a Saffron procurement process, a supplier, contractor or agent connected with Saffron, or otherwise has a connection that could give them influence over a Saffron employee or access to commercially sensitive sales information.
- 9.5.2 All purchasers must be asked whether they have a connection to Saffron. Where a connection is declared, the Homeownership Officer must complete a Connected Individual Form recording the details of the connection and the transaction, and confirming that no preferential treatment has been given and that the standard eligibility, financial assessment and valuation processes have been followed.
- 9.5.3 The completed form must be signed by the Homeownership Officer and submitted to the Governance Team for review and sign-off by the delegated authoriser before the sale can proceed.

9.6 Mortgage finance

- 9.6.1 Where a purchase is funded in whole or in part by a mortgage, the purchaser must obtain mortgage finance from a lender approved by Saffron. As a minimum, the lender must be authorised to conduct mortgage lending in the United Kingdom and be a member of UK Finance (or any successor body).
- 9.6.2 Saffron reserves the right to decline a proposed lender where it considers this necessary to protect its security, assets or operational interests.

10.0 Record Keeping

- 10.1 Saffron will maintain records for at least five years of client identification evidence and details of all relevant business transactions carried out for clients. This is so that they may be used as evidence in any subsequent investigation by the authorities. The five-year retention period runs from the date on which the business relationship ends, or, in the case of a one-off transaction, from the date the transaction is completed.

- 10.2 The precise nature of the records is not prescribed by law, but they must be capable of providing an audit trail during any subsequent investigation, for example, distinguishing the client and the relevant transaction and recording in what form any funds were received.
- 10.3 All disclosure reports will be retained by the MLRO in a confidential file, for five years. Where a SAR has been submitted to the NCA, a copy of that report shall also be retained in the MLRO's confidential file for five years from the date of submission.
- 10.4 Records held under this policy are processed in accordance with Saffron's Data Protection Policy. The lawful basis for processing personal data in connection with AML obligations is legal obligation under Article 6(1)(c) of the UK GDPR. Retention of these records beyond the minimum five-year period is not permitted without separate justification under data protection law.

11.0 Monitoring and Reporting

- 11.1 The MLRO will advise the Executive Team and the Audit and Risk Committee at their next meeting of any report received. In order to maintain confidentiality and security, this will be limited to the fact that an incident has been reported and no details of the content of the report will be given.
- 11.2 The MLRO shall prepare quarterly AML Reports to the Audit and Risk Committee, covering: the number of internal suspicious activity reports received during the quarter; the number of SARs submitted to the NCA; any material changes to Saffron's AML risk profile.

12.0 Training

- 12.1 Employees will be trained at induction, and refresher training will be given at regular intervals to make sure that employees are aware of this policy.
- 12.2 The MLRO and Deputy MLRO shall receive role-specific training appropriate to their responsibilities, including on SAR submission procedures, enhanced due diligence obligations, PEP/family member considerations, and NCA consent procedures.
- 12.3 Training completion shall be recorded. Where an employee fails to complete required training, this should be escalated to their line manager.
- 12.4 Training materials shall be reviewed and updated at least every 36 months, or sooner where there are material changes to legislation, regulation or Saffron's risk profile.

13.0 Regulatory, Legal and Standards Considerations

- Anti-Terrorism, Crime and Security Act 2001
- Proceeds of Crime Act 2002 (POCA) (as amended by the Serious Organised Crime and Police Act 2005).

- Criminal Finances Act 2017
- Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
- Terrorism Act 2000 (as amended)
- The Money Laundering and Terrorist Financing (Amendment) Regulations 2019
- The Money Laundering and Terrorist Financing (Amendment) (EU Exit) Regulations 2020
- Economic Crime and Corporate Transparency Act 2023. This Act introduced the failure-to-prevent fraud offence (applicable to large organisations), reforms to Companies House transparency and beneficial ownership, and crypto-asset seizure powers. These provisions are relevant to Saffron's broader financial crime framework, including its AML obligations.

Regulatory standards: Saffron is a registered provider of social housing regulated by the Regulator of Social Housing (RSH). The RSH Governance and Financial Viability Standard requires registered providers to protect social housing assets and to safeguard the interests of taxpayers. Separately, guarding against the misuse of public funds is a fundamental statutory objective of the RSH under the Housing and Regeneration Act 2008. This policy supports Saffron's compliance with that Standard and contributes to its regulatory self-assessment under the RSH's co-regulatory framework.

AML Risk Assessment: In accordance with section 5.0 of this policy and MLR 2017 Regulation 18, Saffron maintains a written AML risk assessment proportionate to the size and nature of its activities. The current risk assessment is held by the Company Secretary.

14.0 Related Policies and Standards

- Speaking up (Whistle Blowing) Policy
- Probity Policy
- Gifts and Hospitality Policy
- Anti-Fraud, Bribery and Corruption Policy
- Code of Conduct
- Disciplinary Policy
- Data Protection Policy

Policy Title/Reference	Anti-Money Laundering Policy
Author/Owner	Head of Governance
Version Number	3.0
Approval Date	July 2026
Review Date	July 2028
Approval Authority	Audit and Risk Committee
Consulted with Tenant Group	Not applicable.

Appendix B – MLRO and Deputy MLRO Register

This register is maintained by the Company Secretary and updated upon any change in post-holder.

Role	Current Post-Holder	Date Appointed	Contact
Money Laundering Reporting Officer (MLRO)	Iain Innes	July 2020	01508 532053
Deputy MLRO	Tom Riches	July 2026	01508 532006