Prevention of Financial Crime Policy

Published April 2026
Review date February 2029

1. Aim and scope of policy

We are committed to preventing, detecting and guarding against the impacts of financial crime and to reporting concerns appropriately and responsibly. This policy outlines how we do this and applies to the whole VIVID group.

We have a zero-tolerance approach to all forms of financial crime, including fraud. This applies to staff, board members, formally involved customers, volunteers, contractors, suppliers and any other organisations or individuals we work with or who act on our behalf. All such parties are expected to understand and comply with this policy.

We aim to uphold legislation and regulation relating to financial crime, including:

- Bribery Act 2010;
- Computer Misuse Act 1990;
- Criminal Finances Act 2017;
- The Money Laundering, Terrorist Financing & Transfer of Funds (Information on the Payer) Regulations 2017 (MLR);
- Fraud Act 2006;
- Prevention of Social Housing Fraud Act 2013;
- Proceeds of Crime Act 2002 (PoCA);
- Serious Crime Act 2015;
- Terrorism Act 2000;
- Economic Crime and Corporate Transparency Act 2023 (ECCTA)

We comply with the requirements of the Economic Crime and Corporate Transparency Act 2023 (ECCTA), including the "Failure to Prevent Fraud" offence. We maintain reasonable and proportionate procedures to prevent fraud by employees, agents, contractors, subsidiaries and other associated persons, particularly where fraud is intended to benefit VIVID. Our approach is informed by government guidance and the following principles: proportionality, top level commitment, risk assessment, due diligence, communication and training, and ongoing monitoring and review.

2. Definitions

Financial crime covers a wide range of illegal activities that can harm our organisation, our customers and the wider community. For the purposes of this policy, the terms below set out the key types of financial crime we aim to prevent, detect, and respond to. These definitions ensure a shared understanding of the behaviours and activities that fall within scope.

Bribery is offering, giving, requesting or accepting money or anything of value to influence the actions or decisions of another person in breach of expectation of good faith, impartiality or trust

Corruption is dishonesty or fraudulent behaviour by people in positions of authority, typically involving bribery, abuse of power or misuse of entrusted resources

Financial cybercrime is criminal activity carried out using computers, digital systems or the internet. It includes unauthorised access, interference or misuse of computer systems with the intention of securing financial gain or causing financial loss

Fraud is wrongful or criminal deception intended to result in personal or financial gain, or to cause loss to another party. It can include the following offences:

- fraud by false representation
- false accounting
- fraud by abuse of position
- fraudulent trading
- cheating the public revenue
- false statements by company directors
- participation in fraudulent business

Money laundering is the process of concealing the criminal origin of money or assets by converting them into funds or assets that appear legitimate

Tax evasion is the illegal act of deliberately cheating the public revenue or fraudulently avoiding payment taxes owed to HMRC or other tax authorities (e.g. HM Revenue & Customs (HMRC) and other taxation authorities) or fraudulently evading tax

Tax evasion facilitation occurs when an individual or organisation deliberately and dishonestly helps, enables or assists another person to evade tax

Terrorist financing is the provision or collection of funds, assets or financial support with the intention that they be used to support terrorist acts or organisations. It is often linked to money laundering.

Theft is dishonestly taking property belonging to another person with the intention of permanently depriving them of it

3. Policy

Financial Crime

We prevent and mitigate **Financial Crime, including fraud** through the following governance, control and oversight measures:

Governance Framework

- Our Rules which provide our overarching governance framework, including how we make charitable donations in accordance with these Rules
- Standing orders, reviewed annually, which set out how our Board operates and the authority delegated to committees and the Executive Team
- Financial Regulations, including delegated authority limits, reviewed annually to ensure strong financial control
- Intra-group agreements, which set clear terms, roles and responsibilities between us and our subsidiaries
- Compliance with our Code of Governance, ensuring integrity, accountability and transparency in all activities

Companies House Filings

- Robust controls to ensure all information filed with Companies House is complete, accurate and submitted on time
- Maintain an appropriate registered office address and a registered email address capable of receiving official communications and ensure such communications are monitored and acted upon
- Cooperate with Companies House where queries are raised and will promptly correct any inaccuracies identified, using internal escalation to the CFO and Company Secretary where necessary

Internal Financial Controls and processes

- Robust internal financial processes and controls covering income, purchasing, payments, property, investments and financial monitoring – and reviewing compliance with these regularly
- Regular management account reviews, undertaken monthly by the Executive Team and at least six times a year by the Board, providing financial oversight and early identification of anomalies or irregularities

Supplier and Contractor Controls

- Procurement Procedures supported by an approved supplier list
- Due diligence checks on suppliers and contractors at tender stage and throughout the relationship
- Requirements for suppliers to have measures in place to prevent financial crime
- Clear contract terms that specify services, payments and include clauses allowing termination where financial crime is identified

Standards of Conduct

- Code of Conduct, Declarations of Interest process and Gifts and Hospitality procedure and register to ensure transparency and prevent conflicts of interest

Whistleblowing and reporting

- A Speak Up policy to enable safe reporting of concerns, including suspicions of financial crime, and to provide guidance on investigation and escalation

Risk Management and Assurance

- Strategic and Operational risk registers, with financial crime risks recorded, monitored and updated in line with our Risk Management Framework, which is annually reviewed by Audit and Risk Committee (ARC);
- Risk assessment embedded into new activity, considered for every new project, business activity, processes change or new technology through capital proposals to the Project Approvals Committee (PAC) and project level risk registers
- A robust Assurance plan, including:
  - Scheduled specialist deep-dive audits focused on high-risk or complex areas
  - Quarterly internal audits assessing the effectiveness of operational controls
  - Formal approval of the plan annually by the Audit and Risk Committee (ARC), with progress and findings reviewed at every ARC meeting

Internal Audit

- Our financial crime arrangements are subject to independent assurance via both external and internal audit
- External auditors are appointed annually by the Board
- Internal auditors are appointed or renewed annually by ARC, with a full re-tender undertaken at least every ten years

- ARC approves the annual assurance plan and reviews it at every meeting to ensure audit coverage reflects the current risk environment

Identity Verification (ECCTA)

- We comply with the identity verification requirements introduced by the Economic Crime and Corporate Transparency Act 2023. This includes ensuring identity verification is completed for:
    - Directors and any individuals appointed to the Board prior to, or immediately on, appointment;
    - Persons with Significant Control (PSCs); and
    - Individuals who file information on our behalf at Companies House (including any Authorised Corporate Service Providers we instruct)

Regulatory compliance and Horizon Scanning

- The Senior Leadership team and other key staff review six-monthly legal update reports to help identify any emerging threats of financial crime in the social housing sector and wider business environment

Fraud Controls and Reporting

- Maintain reasonable and proportionate procedures to prevent fraud being committed by employees, agents, contractors, subsidiaries and other associated persons for our benefit
- Undertaking an annual Fraud Risk Assessment that considers fraud committed for the organisation's benefit, fraud committed by associated persons, and emerging external fraud threats. The assessment informs the design of our controls and is updated whenever circumstances or risk exposures change
- A "Financial Crime and Fraud Response Plan" in place (Appendix A), setting out how suspicions of financial crime and fraud can be reported, assessed, investigated and escalated or reported appropriately
- Maintaining a fraud register which is a standing item at every ARC meeting, documenting all known or suspected cases
- Regulatory reporting, including submitting an annual fraud losses return to the Regulator via NROSH+ within 6 months of year and reporting any material fraud at the earliest opportunity in line with regulatory requirements

Third Party and Joint Venture Controls

- Ensuring that any Joint Ventures we enter are managed through written contracts that set out roles, responsibilities and expectations, including provisions that address financial crime risks

Monitoring and Review

- Regularly monitoring the effectiveness of our financial crime and fraud prevention procedures, including reviewing and updating controls, policies and risk assessments to ensure they remain proportionate to our risk exposure, legal obligations and organisational changes
- Providing oversight through quarterly internal audit reviews, specialist deep dive audits, annual Fraud Risk Assessment and quarterly fraud and whistleblowing reports to the Audit and Risk Committee
- Reviewing and updating fraud and financial crime controls when new risks emerge or when lessons are learned from incidents, near-misses, internal audit findings or regulatory changes, including developments under the Economic Crime and Corporate Transparency Act 2023

Prevention and mitigation against Bribery, corruption and theft

We specifically prevent and mitigate against **Bribery, Corruption and Theft** informed by principles of the Bribery Act 2010:

Proportionality
Our Prevention of Financial Crime policy addresses bribery risks in a way that are proportionate to our size and sector-specific exposure. Our policies are approved by the appropriate level of authority and frequency as specified by our policy framework.

Top level commitment
Our Board demonstrates a clear commitment to preventing bribery and corruption with our organisation. They promote a culture where bribery, corruption and theft are unacceptable. We publicise our approach to preventing financial crime on our intranet and website

Gifts and Hospitality Controls
We maintain a Gifts and Hospitality Register, supported by a procedure requiring staff to declare all invitation or offers of gifts and hospitality. The register is reviewed annually at our Remuneration Committee annually to ensure appropriate oversight and identify any patterns or risks

Due diligence
We undertake proportionate due diligence on all individuals and organisations who performing services on our behalf. This includes checks embedded within our procurement procedures to identify and mitigate risks or bribery, corruption or theft

Prevention and Mitigation of Money Laundering (including Terrorist Financing)

We prevent, detect and mitigate risks associated with money laundering and terrorist financing):

Registration and Regulatory Compliance
- Registration with HMRC for our estate agency work, as required under the Money Laundering Regulations 2017
- Registration with the Financial Conduct Authority (FCA) for our consumer credit activities

Money Laundering Reporting Officer (MLRO)
- Our Chief Financial Officer is appointed as our MLRO (deputised by the CEO). All suspicions or concerns related to money laundering must be reported to the MLRO

Training
- Training is available for staff whose roles are relevant to AML compliance or who may encounter money laundering risks (e.g. consumer credit, sales and lettings, rent collection)
- Enhanced AML training can be provided for those working in higher risk areas of the business, where appropriate

Due diligence
- We conduct due diligence on relevant transactions and counter parties
- Due diligence on associated persons considers the risk that a third party could commit fraud intending to benefit VIVID. This may include financial checks, reference checks, reviewing control environments, contract clauses, and enhanced monitoring for higher risk arrangements

Reporting of suspicious activity

- Where we know or suspect money laundering or terrorist financing, staff must report this to the MLRO as soon as possible
- Reports must be made confidentially and securely
- Staff must not "tip off" any individual involved in suspected activity, in line with legal obligations and potential criminal activities under POCA and MLRs

Information Sharing to prevent economic crime (ECCTA 2023)

- Where appropriate and lawful, we may share information with other AML-regulated firms and relevant authorities to prevent and detect economic crime, including money laundering, fraud and terrorist financing. We'll comply with ECCTA provisions and applicable data protection law when doing so

Prevention of facilitation of tax evasion

- We publish an annual statement of our position to prevent tax evasion and the measures we take

Tenancy Fraud

We recognise Tenancy fraud as a form of financial loss, however, operational management of tenancy fraud is covered in our Housing and Neighbourhood Management Policy

4. Responsibilities

To support our defence against financial crime and fraud the following roles have key responsibilities:

The Board and Executive Board

- champion a zero-tolerance approach to fraud and financial crime
- encourage a Speak up culture where reports are taking seriously and actioned appropriately
- appoint an MLRO who makes sure we work within money laundering law
- Ensure adequate resources and oversight are in place

The Audit and Risk Committee (ARC)

- review and approve this policy at least every 3 years
- review reports relating to financial crime including fraud and recommend or approve appropriate action
- provide oversight and seek assurance that adequate systems of internal control are in place to prevent, detect, manage and report financial crime, including fraud
- provide oversight and seek assurance that management responds appropriately to identified weaknesses, incidents or control failures

Chief Financial Officer (also Company Secretary and MLRO)

- owns this policy
- lead and coordinate investigations into suspected financial fraud or other suspicious activity, in accordance with the Financial Crime and Fraud Response Plan
- submit Suspicious Activity Reports to the National Crime Agency where required
- ensure financial controls are robust and regularly reviewed
- report material fraud incidents to the Board and regulators as required
- ensure staff, agents and consultants receive suitable training on money laundering obligations

Risk and Assurance Manager

- review and maintain this policy
- undertake the annual fraud risk assessment
- submit quarterly fraud and whistleblowing reports to the Audit and Risk Committee

- provide timely and accurate information to ARC, including reporting significant control weaknesses or incidents
- monitor the effectiveness of internal controls related to fraud and financial crime
- provide advice and guidance to teams on fraud prevention measures and emerging risks

Governance Manager
- maintain our fraud register, ensuring incidents and actions are accurately recorded
- coordinate and arrange anti-money laundering training for relevant staff
- support the MLRO and Risk & Assurance Manager with information gathering, reporting and compliance activities
- act as a central point of contact for queries relating to fraud, bribery, money laundering and other financial crime policies
- monitor regulatory submissions and external reporting requirements relating to financial crime and fraud
- oversees the identity verification processes and maintaining records of verification outcomes and supporting evidence

Managers
- implement this policy in their processes and procedures
- implement financial crime and fraud controls within their operational areas
- make sure staff know what's expected of them and are properly trained
- encourage a Speak up culture and escalate concerns

Internal Audit
- independently assess the effectiveness of fraud controls
- conduct periodic reviews of fraud risk management procedures
- report findings to the Audit and Risk Committee

People Team
- support workplace investigations and disciplinary action where financial crime related misconduct is suspected and/or confirmed
- maintain confidentiality and ensure appropriate protection for staff who raise concerns or whistleblow
- escalate any reports or concerns relating to financial crime or fraud to the Chief Financial Officer
- provide advice to managers on conduct, sanctions and employment related implications arising from fraud or financial crime investigations
- ensure recruitment and vetting processes (e.g., right to work, references, DBS where applicable)
- support the organisation's fraud prevention controls
- maintain secure HR records relating to investigations, outcomes and sanctions

Staff, board members, formally involved residents, volunteers, and others acting on our behalf
- read and comply with this policy and related documents
- undertake training as necessitated by role
- report any suspected incidents of financial crime directly via the approved channels

5. Related documents

This policy should be read in conjunction with:

- Code of Conduct
- Declarations of Interest Guidance
- Speak Up Policy

- Gifts and Hospitality Procedure
- Data Protection Policy
- People Policy
- Housing and Neighbourhood Management Policy
- Group Financial Regulations
- VIVID Procurement Regulations
- Safeguarding of Vulnerable Adults Policy

Co-Creation	N/A
Equality Impact Assessment	This policy underwent an Equality Impact Assessment 20 February 2026
Policy Author	Lauren Ricketts, Risk and Assurance Manager
Policy Owner	David Ball, Chief Financial Officer
Approved by	Audit and Risk Committee
Approved Date	April 2026
Review Date	February 2029

Appendix A
Financial Crime and Fraud Response Plan

Purpose
This plan sets out the steps we take when any concern, allegation or suspicion of financial crime or fraud is raised. It provides clear, step-by-step guidance so all reports are handled consistently, promptly and professionally.
It supports our legal and regulatory obligations, including the Economic Crime and Corporate Transparency Act 2023.

When to report a concern?
You must report a concern **as soon as possible**, and **no later than 24 hours** after becoming aware of it.
Report if you notice or suspect:

- fraud, bribery or corruption
- theft, misuse of assets or dishonesty
- money laundering or suspicious transactions
- irregularities in financial records or decision making
- unusual supplier, contractor or customer behaviour
- cyber related financial activity that seems suspicious
- anything that "*doesn't look right*"

You do not need proof. Suspicion is enough.
Do not investigate yourself – this can compromise evidence and may impact further investigations.
Staff are also encouraged to report concerns about suppliers, contractors or other third parties we work with.
For illustrative examples of common fraud risks, see **Appendix B - Common Examples of Fraud**.

Why reporting matters?
Fraud and financial crime have real consequences. Every pound lost is a pound that cannot be invested in our homes, communities or customer services. Speaking up helps protect our customers, our colleagues, our reputation and the trust placed in us as a social housing provider.

How to report a concern
You can report concerns through any of these routes:

David Ball, Chief Financial Officer (CFO)	Mobile: 07770 811658
(Primary point of contact)	
Any member of the Senior Management Team – they will escalate on your behalf	
Speak Up routes (including anonymous reports):	
Duncan Short, Group Resources Director	Mobile: 07753 449295
Caroline Stockmann, Independent Board Member	Mobile: 07826 543693
Neil Hewitson, KPMG Internal Auditor	Mobile: 07810 404843

Any concerns relating to tenancy fraud or customer-related fraud should be reported via our Safeguarding route on iPC or by speaking directly to the Tenancy Support Team. If you don't have access to FSM/iPC, concerns can still be raised via the safeguarding email at safeguardingnotifications@vividhomes.co.uk

All reports will be treated confidentially.
If someone is at immediate risk, or a serious crime is taking place, call **999** and notify the CFO afterwards.

What happens after you report?

All reports will be escalated to the CFO to initiate the response plan.
If the CFO is unavailable, another member of the Executive Team will act as Investigation Lead.
We will:

- treat your report seriously and confidentially (within the limits of a full investigation)
- store information securely and retain it in line with our data retention schedule
- protect anyone speaking up in good faith – retaliation will not be tolerated
- provide support to anyone making a disclosure
- normally share the outcome with you wherever possible

We may contact you for further information during the investigation.
Incidents will be reported to the Executive Team, ARC or Board as appropriate.

Evidence preservation

Do not delete emails, files or system logs, and do not move or alter anything that may be relevant.
The CFO / Investigation Lead will advise how evidence should be secured.

External reporting

Where required, we will fulfil any external reporting duties, which may include;

- law enforcement
- Action Fraud
- the National Crime Agency (NCA) regarding Suspicious Activity Reports
- our regulator
- insurers
- other relevant authorities

What happens next?

The following response steps will be taken:

1. Report received - concern is logged and acknowledged
2. Immediate containment actions - steps taken to prevent further loss or risk
3. Initial assessment - CFO reviews information and determines next steps
4. Investigation - formal fact-finding, evidence-gathering and analysis
5. Outcome and actions - decisions, remediation and disciplinary or legal steps
6. Reporting and lessons learned - findings shared with Exec/ARC/Board as appropriate, and improvements built into our controls and processes

Learning and improvement

After each case, we will review what happened and update our controls, processes and training (as required) to reduce the risk of similar incidents in the future.

Appendix B
Common Examples of Fraud

Fraud can be committed by people inside or outside the organisation - including staff, contractors, customers or members of the public. Fraudulent activity undermines trust, wastes resources and affects the services we provide.
These examples illustrate some of the most common types of fraud we may encounter. They are *not exhaustive* - if in doubt, **report it**.

Internal Fraud Risks

- Theft of cash, stock, materials, or other assets — including attempts to conceal or disguise the theft
- Over-claiming mileage, travel, or subsistence expenses
- Claiming overtime or hours not worked
- Misappropriation or unauthorised sale of waste, scrap, or surplus materials
- Creation of fictitious or "ghost" employees on the payroll
- Forging signatures or altering financial or tenancy-related documents
- Writing off recoverable debts (e.g. rent arrears) without proper authorisation
- Misuse of company credit cards or unauthorised purchases
- Personal use of organisational assets (vehicles, tools, IT equipment etc)
- Manipulating housing allocation systems for personal or third-party benefit

External Fraud Risks

- Invoices for goods/services not delivered, inflated pricing or duplicate invoicing
- Expense claims not incurred or submitted multiple times
- Fraudulent changes to supplier bank details (mandate fraud)
- Collusive bidding or price-fixing in procurement
- False or exaggerated compensation, insurance or disrepair claims
- Bribes, gifts or incentives offered to staff or board members
- Forged documents or false identity used in tenancy applications
- Misuse of grant funding or fraudulent grant applications
- False housing benefit or Universal Credit claims
- Illegal subletting (tenancy fraud)
- Non-occupation or misrepresentation of household composition

Reporting concerns

For how to report a concern, please refer to **Appendix A – Fraud Response Plan**.

Suspicion is enough — you do not need proof.

All reports are treated confidentially. If someone is at immediate risk or a serious crime is taking place, call **999**.

Fraud Red Flags

Below is a list of common warning signs that something may not be right. If you spot any of these indicators, report it.

Behavioural Red Flags

These often signal personal risk factors, pressure or concealment:

- Sudden change in lifestyle or spending patterns
- Reluctance to take holidays or allow others to review their work
- Overly defensive when questioned about processes
- Unusual secrecy about records or systems
- Employees who insist on bypassing normal controls
- Close, unexplained relationships with contractors, suppliers, or customers
- A “can only be done by me” attitude

Financial / Transaction Red Flags

Signs that financial processes might have been manipulated:

- Transactions that don't match supporting documents
- Missing invoices, receipts or authorisation forms
- Duplicate payments or multiple invoices from the same supplier
- Invoices with vague descriptions or unusual urgency
- Payments made just below approval thresholds
- Unexplained write-offs of arrears or debts
- Inconsistencies between systems and manual records

Supplier / Contractor Red Flags

Particularly relevant in property services, development and procurement:

- Suppliers paid for goods or services not delivered
- Same supplier repeatedly used without competition
- Quotes that seem unusually high or unusually low
- Changes to supplier bank details without verification
- Contractors unwilling to provide documentation or proof of work
- Staff involved in awarding contracts showing unusual interest or influence

Customer / Tenancy Red Flags

Specific to social housing operations:

- Tenants refusing access for inspections or verification
- Signs of subletting (multiple people, different occupants, changed locks)
- Suspicious or inconsistent identity documents
- False household composition (undeclared occupants)
- Repeated disrepair claims with no evidence
- Overcrowding claims that don’t match occupancy
- Claims for compensation that seem exaggerated or patterned

Payroll / Staff Fraud Red Flags

Internal risks affecting wages, expenses and allowances:

- “Ghost” employees on payroll
- Overtime consistently claimed by a small number of individuals
- Mileage claims that do not match routes or dates

- Claims submitted late or repeatedly changed
- Unusual adjustments to payroll records

IT / Cyber Fraud Red Flags:
Increasingly common across housing providers:

- Unexpected requests to change bank details
- Emails asking for urgent payments or secrecy
- Login attempts outside usual hours
- Unauthorised system access or changed permissions
- Files or emails disappearing
- Staff reporting being locked out of systems