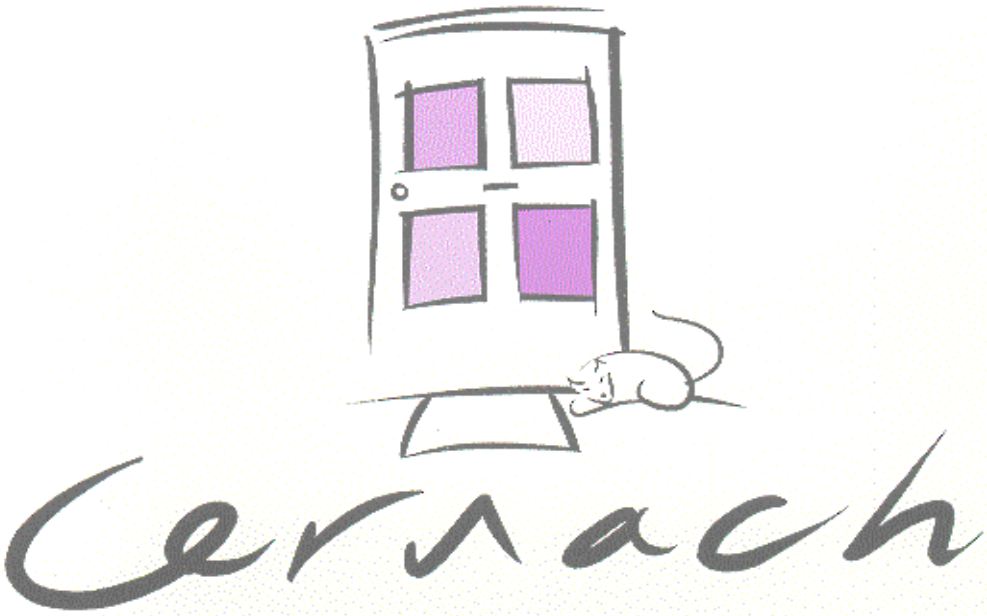

Policy on Dealing with Allegations of Fraud

Date Approved by Management Committee: 15 August 2024
Latest review date: August 2028

1. Introduction

1.1 Cernach Housing Association recognises the importance of protecting the organisation including its tenants, its operations, its employees, suppliers, and its assets against financial risks, operational breaches and unethical activities.

1.2 Losses due to fraud, theft or corrupt practices could have a direct effect on the level and quality of service provision. The Association plays an important role in the local area and any instances of fraud or corruption could be damaging for its reputation, as well as for the reputation of the registered social landlord sector in general.

1.3 It is wrong to assume therefore that actual financial losses are the only negative outcome of frauds. The full cost is usually much greater than the amount stolen, as the costs associated with correction may be material. Staff morale and the level of confidence of tenants, partners, suppliers, lenders and the Scottish Housing Regulator may decline as a result of fraud.

1.4 It is also important to recognise the potential for non-financial fraud, such as falsification of records, procurement fraud or try to obtain/give a benefit through fraudulent means.

1.5 Cernach Housing Association has a responsibility to its tenants, staff, partners, suppliers and other stakeholders in general to take all reasonable steps to prevent the occurrence of fraud. This policy sets out in more detail procedures for:

- fraud prevention and detection
- the investigating and reporting of fraud
- recording of fraud
- responsibilities

Information is also provided on risk management, internal controls, management checks, staff training and the Bribery Act 2010.

1.6 This policy applies to all employees and to temporary workers, consultants, contractors, agents and subsidiaries acting on Cernach's behalf. It also applies to Committee members. Breaches of this policy are likely to constitute a serious disciplinary, contractual and/or criminal action for the individual(s) concerned.

1.7 Please note that an equality impact assessment has been completed and this is attached at Appendix 1.

2. Fraud definition and examples

2.1 Fraud can be defined as any act (actual or alleged) or wilful dishonesty to gain an individual or collective advantage. It is taken to include theft, deception, bribery, forgery, extortion, corruption, conspiracy, embezzlement, misappropriation, concealment of material facts and collusion. For practical purposes, fraud may be defined as the use of deception with the intention of obtaining advantage, avoiding an obligation or causing loss to another party.

2.2 In addition to the more traditional, in-person, type frauds, the risk of cyber fraud has also become more prevalent in recent years as (i) we become more reliant on ICT and (ii) methods of fraud become more sophisticated.

2.3 Staff should be aware that gifts, including hospitality offered by contractors/ suppliers or service providers, may place an employee in a vulnerable position. Even when offered and accepted in innocence, such gifts may be misconstrued by others. The offer, acceptance or refusal of gifts and hospitality should be in line with the Association's entitlements, payments and benefits policy and associated guidance.

2.4 Some examples of fraud that could be perpetrated against the Association are:

- Theft of cash or other assets, including via cyber means – please see separate section on cyber fraud below (section 2.5)
- False accounting and/or making fraudulent statements with a view to personal gain or gain for another
- Bribery or corruption – offering, giving, soliciting or accepting an inducement or reward that may influence the actions taken by the Association's staff, for example in the procurement of goods or services
- Claims for payment of works of maintenance that have not been completed, do not exist, are exaggerated or are excessive
- Claims for payment of supplies that have not been provided
- Falsification of expenses and invoices
- Falsification of time clocking entries
- Falsification of entries in the Kelio time management system, including asking your line manager or other authorised person to approve false entries
- Falsification of annual leave, sick leave, medical appointment leave, special leave or any other permitted category of leave
- Knowingly providing false information on job applications and requests for funding
- Alteration or falsification of records (computerised or manual)

- Failure to account for monies collected
- Tenancy fraud – including false applications and illegal sub-letting
- Acceptance of bribes for access to housing
- Payroll fraud
- Housing benefit fraud
- Procurement fraud
- Bank mandate fraud
- Online fraud

Whilst the above list is comprehensive, is not exhaustive and the Association may define other actions not specified above as fraud.

2.5 **Cyber fraud**

2.5.1 Due to the reliance on digital methods of working, particularly banking, the Association expects there to be several ways in which external parties will seek to commit incidents of cyber fraud against the Association.

2.5.2 Generally, cyber fraud will be categorised as some level of malicious and unauthorised access to systems. The Association therefore deploys several methods to minimise the likelihood and impact of this situation occurring.

2.5.3 This list is non-exhaustive, and indeed will grow as systems become more sophisticated, but some methods the Association deploys are as follows: -

- Use of personal accounts and passwords for all members of staff on all systems, which should not be shared under any circumstances
- Multi-factor authentication on systems wherever possible, but currently set up for Office 365, banking system access, Committee paper access and payment system access.
- Endpoint device continuous monitoring protection on every Association device
- Security Operations Centre (SOC) system deployed across the Association's ICT infrastructure
- Access to the Association's Office 365 network geolocked to the UK.
- Warning messages from all email senders outside the Association's domain.
- Regular phishing training campaigns for all staff
- Cyber Essentials Plus accreditation

2.5.4 The Association has adopted the SFHA model cyber incident response plan which can be referred to in the event of a cyber fraud issue.

2.6 **Internal and external frauds**

2.6.1 For the purposes of this policy statement, frauds can be internal, external or a combination of both. The policy defines these in sections 2.6.2 and 2.6.3 below.

2.6.2 Internal frauds are those committed by a staff member, a Committee member or someone acting on the Association's behalf who has access to the Association's office and/or systems. Examples of internal fraud include a member of staff or Committee taking an inducement to award a contract to a specific company, a staff member embezzling Association funds, or manipulation of records to grant a tenancy to a person who would otherwise not receive the offer. The procedure for dealing with an internal fraud is noted at Appendix 1.

2.6.3 External frauds are those committed by someone not connected to the Association in the manner described in section 2.6.2. An example of an external fraud would be a mandate fraud, submitting a hoax invoice for payment of services that were not received and/or requested or providing information known to be false in order to increase the likelihood of receiving a job offer or offer of a tenancy.

2.7 **The Bribery Act 2010**

2.7.1 The Bribery Act 2010 codifies the law relating to bribery and corruption. Corruption is the misuse of office or power for private gain; bribery is a form of corruption and means that it falls within the scope of this policy. Under the Bribery Act 2010 it is illegal to:

- Offer, promise to give or to pay a bribe
- Request, agree to receive or accept a bribe
- Bribe a foreign public official
- Fail to have adequate procedures in place to prevent bribery

2.7.3 Staff and Committee should be aware that any breach of the Bribery Act is likely to be dealt with as a breach of criminal law.

3. Fraud prevention

3.1 Cernach Housing Association has established a system of internal controls, policies and procedures, in an effort to deter, prevent and detect fraud and corruption.

3.2 All new employees (including those on temporary contracts) are asked to provide details of any current unspent criminal offences in the Association's employment application form. The Association will verify details provided in the application form including references and educational checks and will obtain a Basic Disclosure under the PVG scheme in Scotland (unless the nature of the post requires an Enhanced Disclosure, in which case this will be obtained).

3.3 All suppliers and contractors must be in good standing and subject to any screening by the Association in line with the Association's procurement policy.

3.4 All contractual agreements with the Association will contain the provision prohibiting fraudulent or corruptive acts and will include information about reporting fraud and corruption.

3.5 All staff will receive fraud and corruption awareness training at appropriate intervals and an anti-fraud culture will be promoted throughout the organisation.

4. Fraud detection

4.1 The primary responsibility for detecting fraud lies with the Management Committee and, on an operational basis, senior staff. However, all staff have a responsibility to be aware of the potential for fraud and take the necessary steps to minimise the risk to the Association. Senior staff should ensure that staff in their areas of operation are familiar with the common types of fraud.

4.2 The Association is not advocating the creation of an overtly suspicious environment, but it expects staff to be alert to the potential for fraud in areas where they operate.

4.3 The Association's auditors, through their evaluation of the control framework (internal auditors) and during the annual audit (external auditors), also have a role to play in preventing and detecting fraud, however this is not the main remit of audit.

5. Investigation and reporting fraud

5.1 Staff will often be the first to notice the potential for fraud; this is also the case where an actual fraud, or attempted fraud, takes place. Staff suspicious of fraud should report their concerns to their line manager or the Director. This requirement to alert is not confined to suspicions about other members of staff, but includes any misgivings staff may have about contractors, consultants, agents, suppliers, etc.

5.2 Where it appears that the fraud may involve the Director, the most senior member of staff not implicated should notify the Association's Chairperson as soon as reasonably practical. The Chairperson will then notify the Scottish Housing Regulator and both the internal and external auditors who will guide them accordingly.

5.3 Staff should not be dissuaded from reporting actual or suspected fraud as all cases will be treated in the strictest confidence. The Association is fully committed to supporting and protecting staff that raise legitimate concerns where possible. However, the Association cannot guarantee anonymity and may have to provide, for example, witness statements to assist with any investigation.

5.4 Provided the allegations have been made lawfully, without malice and in the public interest, the employment position of the person will not be disadvantaged for reasons of making this allegation. The Association's whistleblowing policy contains further information on this.

5.5 Any action(s) aimed at preventing the reporting of fraud/attempted fraud, including any attempts at intimidation, will be treated seriously and the Association will take appropriate advice which could, in some circumstances, lead to reporting the action(s) to the police.

5.6 Fraudulent or corrupt activity by a staff member is regarded as a breach of contract and, where there are grounds for suspicion, suspension is likely pending the outcome of enquiries. Where there are grounds to suspect that criminal fraud has occurred the Association's policy in all such cases is to advise the police. The Association will co-operate fully with the police.

5.7 The Association may start its own investigation while any police investigation is ongoing; the Association will liaise with its solicitors in this regard to ensure that it is not acting in a manner that could compromise any criminal investigation. If necessary, the Association may have to delay invoking its own internal disciplinary procedures pending conclusion of any criminal proceedings.

5.8 Where dishonesty is detected, disciplinary procedures will be instigated and this may lead to dismissal of the individual concerned. If required, the Association's auditors or any other appointed independent investigator will be asked to carry out a fuller investigation and to provide independence in the investigation. In all cases the Association will co-operate fully with those carrying out the investigation.

6. Fraud register

6.1 The Director will be responsible for ensuring that all frauds, suspected or actual, are recorded in the fraud register. Entries in the register will be reported to the Committee as they arise and the register will be reviewed by the Committee and signed off by the Chairperson or Secretary and Director.

6.2 The register will contain the following information:

- Scope and circumstances arising; summary of what happened
- Action taken by the Association
- Outcome
- Any control action required as a result of the fraud
- Estimate of loss/potential loss
- Extent of/potential for recovery of loss
- Date reported to the Scottish Housing Regulator (all suspected or actual fraudulent activity is to be reported)

6.3 Should any loss through fraud be sustained by the Association, the Management Committee will take all reasonable steps to recoup the loss if the loss is of a material amount. The loss may be recouped from the perpetrator of the fraud or through an insurance fidelity guarantee claim.

6.4 The fraud register is a hard copy book and is kept in the Association's fireproof safe.

7. Responsibilities

7.1 <u>Management Committee</u>

7.1.1 The Committee has overall responsibility for establishing adequate systems of internal control and for ensuring that these are regularly reviewed for effectiveness and compliance.

7.1.2 It is acknowledged that there can never be any absolute guarantees that internal checks and systems and procedures established will always prevent fraud, corruption or malpractice occurring. However, a good system of evaluating and testing internal controls (via, for example, internal audit) helps identify any systemic weaknesses and reduce the risk of fraud occurring.

7.1.3 The Management Committee sets the annual programme of internal audit and receives reports on the outcome of all internal audits that are carried out. The Committee also approves action plans for implementing recommendations. The internal auditor attends the Management Committee at least once each

year (generally in November or December) in addition to attendance at quarterly Assurance sub-Committee meetings.

7.1.4 The Committee Code of Conduct notes that it is the responsibility of all members to report details of alleged, detected, suspected or attempted fraud, corruption and/or malpractice committed by any person should they become aware of this.

7.2 Assurance sub-Committee

7.2.1 The Assurance sub-Committee monitors progress in relation to agreed recommendations; the staff team is responsible for implementing the recommendations.

7.2.2 The external auditor's annual management letter will be considered by the Management Committee who will agree the response to the management letter and thereafter will the sub-Committee will monitor the implementation of any recommendations agreed.

7.3 Senior staff

7.3.1 Headed by the Director, the senior staff have a responsibility for preventing fraud. The senior staff team comprises the Director, Depute Director, Corporate Services & Assurance Manager, Senior Housing Officer, Senior Maintenance Officer and finance agent (services). Senior staff will ensure that all staff act in a manner that promotes the following:

- Identification of risks to which systems and procedures are exposed
- Developing and maintaining effective internal controls to prevent fraud
- Establishing an environment that promotes compliance with internal controls
- Promoting fraud awareness
- Fostering an anti-fraud culture
- Ensuring that if a fraud or attempted fraud occurs a vigorous and prompt investigation takes place without regard to position held or length of service
- Take appropriate disciplinary and legal action in all cases where justified
- Reviewing systems and procedures to prevent similar frauds arising

8. Risk management

8.1 While senior staff are responsible for assessing and controlling the level of risk within their areas of authority, it is the responsibility of all staff to be aware of fraud and take the necessary steps to minimise the risk to the Association.

8.2 Managing the risk of fraud is the same in principle as managing any other business risk. It is best approached systematically both at corporate and operational levels. Managers should identify risk areas, assess the scale of risk, allocate responsibility for managing specific risks and implement and test controls to minimise the risks.

8.3 Senior staff also have a responsibility to familiarise themselves with common fraud techniques in areas for which they have control. This should include being alert to signs which indicate that fraud is taking place.

9. Internal controls

9.1 Internal controls are the key element in preventing fraud. They should be documented, communicated to all staff and the importance of compliance regularly reminded to staff. It is the responsibility of each line manager to ensure that controls within their areas of responsibility have been documented and that they are communicated and operate effectively.

9.2 Managers should:

- Assess the types of risk involved in the operations for which they are responsible
- Review and test the control systems for which they are responsible regularly
- Ensure that there is effective compliance with controls
- Satisfy themselves that their systems continue to operate effectively

9.3 Senior staff should periodically monitor compliance with controls, for example by including them in the internal audit programme. It should be emphasised that the main remit of internal audit is to evaluate the effectiveness of the overall framework of internal control, with management being responsible for ensuring implementation and monitoring of the framework.

10. Corporate governance

10.1 The Scottish Housing Regulator monitors the Association's adherence to corporate governance requirements through their publication of the annual Engagement Plans and also through more in depth and focused on-site inspections and, more so, desktop reviews of various statutory returns.

10.2 Development of best practice and recommendations arising regulatory and advisory publications will continue to be important in the development of an

environment in which awareness of responsibility for fraud prevention and detection can flourish.

11. Staff training

11.1 The whole staff team combines to ensure that the business is operates in an effective and appropriate manner on a day-to-day basis and, as such, are likely to be best placed to detect fraud/attempted fraud. It is therefore crucial that the policy on fraud prevention and investigation is fully communicated to all staff **and** that this is supplemented by periodic training.

11.2 Best practice recruitment policies, such as detailed application forms that include a statement on relevant unspent convictions, written and verbal communication with referees and past employers and verification of criminal record checks, educational and professional qualifications will be strictly used to help ensure that the Association avoids employing individuals with an increased likelihood of committing fraud.

11.3 Staff awareness of relevant policies and procedures is fundamental to the effective operation of systems. Best practice includes:

- Instruction and discussion on control and probity issues as part of staff induction
- Staff training on operational procedures
- Desktop instructions for specific tasks
- Ensuring that staff are aware of changes to control systems, policies and procedures

12. Policy review

12.1 This policy will be reviewed every four years, or earlier in line with legal, regulatory or best practice requirements. The next review will take place in or before August 2028.

Appendix 1

Fraud response plan – internal fraud

1. Introduction

1.1 The purpose of this plan is to outline the steps to be followed in the event of a suspected fraud where it is thought that the perpetrator is internal – ie staff member, Committee member or someone acting on the Association's behalf such as a contractor or consultant. It provides a consistent framework for investigating and reporting fraud by defining authority levels, responsibilities for action and lines of reporting. This plan should be read in conjunction with Association's fraud policy (to which it is appended) and the whistleblowing policy.

2. Initiating action

2.1 Suspicion of fraud may be captured through a number of means. This includes internal audit work, external audit, whistleblowing, or any member of staff noticing or suspecting that something is "not quite right". In all cases the Director should be alerted to the matter without delay. In the Director's absence (or if the Director is the suspected perpetrator or is somehow implicated in the fraud/potential fraud), another member of the senior management team should be informed so that they can inform the Chairperson.

2.2 The Director (or in their absence or inability to participate, another member of senior staff) will as soon as possible and normally within 24 hours, convene a meeting with the Depute Director and/or Corporate Services & Assurance Manager and Chairperson to decide on initial action to be taken (this will be known as the Fraud Response Group). This action will normally involve:

- Identify someone to act as Investigating Officer (or Co-ordinating Officer if a separate police investigation is ongoing) – this should normally be a member of the senior management team or the internal auditor
- Informing external auditors of the matter and agreeing arrangements for keeping the external auditors informed about progress/outcome
- Considering how to secure records/assets and prevent further loss
- Seeking legal advice from the Association's solicitors, as required
- Confirming responsibilities and arrangements for submitting relevant regulatory notifications, for example raising a notifiable event
- Confirming requirements and arrangements for notifying funders
- Agreeing membership of the Fraud Response Group going forward

2.3 The Director should advise the Chairperson as soon as an investigation under this procedure has been initiated and/or a Fraud Response Group has been established if the Chairperson is not available to attend the initial meeting.

3. Preliminary investigations

3.1 The Investigating Officer must conduct an initial information gathering exercise to enable the circumstances to be investigated rigorously, confidentially and without undue delay. They should thereafter report their initial findings to the Fraud Response Group, any interim conclusions and provide an action plan to guide the full investigation if this is the recommended course of action.

3.2 The Fraud Response Group will consider the Investigating Officer's report, but the information will not be disclosed or discussed with anyone else who does not have a legitimate need to know. In cases where an individual is suspected of fraud, which a subsequent investigation does not substantiate, every effort must be made to minimise potential damage to the individual's reputation.

4. Involving the police

4.1 Where preliminary investigations establish that there are reasonable grounds to suspect that a financial fraud has taken place (or has been attempted), it is the Association's policy to pass details directly to the police, normally without undue delay and prior to any further internal investigation. The Director will notify the Chair of the Committee of this action.

4.2 The police will lead any further criminal investigations from this stage. All employees are required to co-operate fully with police enquiries in this regard. The Director will establish and maintain appropriate lines of communication with the police. The Director will also liaise with the Association's solicitor to gauge whether any internal investigation should be suspended pending the police enquiry or whether it can proceed.

5. Subsequent investigations

5.1 Where preliminary investigations provide reasonable grounds for suspecting a member or members of staff of fraud, the Fraud Response Group will decide whether there is a requirement to suspend the suspect(s). It will do so, with reference to the Association's disciplinary procedure.

5.2 In these circumstances, the person(s) concerned should be allowed to collect personal property, but should not be able to remove any property belonging to

the Association. Any keys to premises should be retained by the Association and placed in the safe; the alarm code should be changed.

5.3 The ICT support agent should be asked to withdraw, without delay, access permissions to the Association's computer systems and any social media/website passwords should be changed. The person(s) involved should be requested to hand over all ICT and communications equipment provided to them by the Association, including laptops, mobile telephones and other devices.

5.4 If no suspension takes place following preliminary investigations, the Fraud Response Group should review this at subsequent stages of the ensuing investigation.

5.5 The Investigating Officer will consider whether it is necessary to investigate systems other than that which has given rise to suspicion, through which the employee may have had opportunities to misappropriate Association assets, and report their opinion in this regard to the Fraud Response Group; the Group will then determine whether there is a need to collect additional information in order to provide an appropriate level of evidence.

5.6 Depending on the nature of the suspected fraud, the investigation may require technical expertise that the Investigating Officer does not possess. In these circumstances, the Fraud Response Group has responsibility for the appointment of external specialists to lead or contribute to the investigation.

5.7 Any requests for information from the press or other external agency concerning any fraud investigation must be referred to the Director; the Director may wish to engage the services of a public relations expert in order to decide the best way to respond to any press requests in order to avoid damage to the Association's reputation. Under no circumstances should the Investigating Officer or any other employee provide statements or information to the press or external agencies.

6. Recovery of losses

6.1 The Investigating Officer will ensure that the amount of any loss is quantified wherever possible. Repayment of losses will be sought in all cases. Where the loss is substantial, legal advice should be obtained without delay about the need to freeze the suspect's assets through the court, pending conclusion of the investigation. Legal advice should also be obtained about prospects for recovering losses through the civil court, where the perpetrator refuses repayment. The Association will normally expect to recover costs in addition to losses.

6.2 The Investigating Officer, in discussion with any other relevant parties, should also decide whether any of the losses warrant a claim under any current insurance policy.

7. Investigation report

7.1 On completion of a fraud investigation, the Investigating Officer will submit a written report to the Fraud Response Group. If a fraud has been established, the report will contain:

- A description of the incident, the people involved, and the means of perpetrating the fraud
- The measures taken to prevent a recurrence
- Quantification of losses
- Statement on any reputational or other non-financial damage
- Progress with recovery action (if appropriate)
- Progress with disciplinary action (if applicable)
- Progress with criminal action (if applicable)
- Actions taken to prevent and detect similar incidents.

7.2 The report will normally be submitted to the next Committee meeting. Where the fraud is significant, in terms of losses incurred, or particularly novel, unusual or complex, a special Committee meeting may be convened.

7.3 If no fraud/attempted fraud has been established, the report will include an opinion on whether the initial allegations were vexatious or malicious. If the Investigation Officer concludes that they may have been vexatious or malicious, the Fraud Response Group will consider the appropriate action to take against those responsible. This may involve invoking the Association's disciplinary procedures and could result in dismissal. Legal advice will be followed at all stages in such circumstances.

8. Review of the fraud response plan – internal fraud

8.1 This plan will be reviewed every four years in conjunction with the fraud policy. The review may be earlier to respond to legal, regulatory or best practice requirements. The next review will take place in August 2028 or earlier.