FRAUD POLICY

Policy Classification: Strategic

Status: Approved

Policy Lead:	Director of Finance & Corporate Services
Date Approved:	December 2019
Last Review Date:	New Policy
Review Due Date:	December 2024
Review Period:	5 years unless required earlier due to changes in the law, regulation, best practice or requirement of the Association

REFERENCE PAGE

Document Title:	Fraud Policy
Aim:	set out Eildon's responsibilities for fraud prevention
Objective:	1 The Eildon Group will ensure that the highest standards of governance and partnership working are adhered to, including compliance with our regulatory frameworks
Scope of Policy:	All stakeholders
Nominated Officer:	Director of Finance & Corporate Services
Approval Source:	Board
Legal and Regulatory References:	Computer Misuse Act 1990 SHR Notifiable Events Regulatory Guidance
Procedural References:	Eildon IT Security, Access and Protection of Information Policy Eildon Resolution of Difficulties Policy
Consultation Completed:	N/A
Risk Implications:	3- New policy
Equalities Assessment:	All Eildon policies and key documents are developed with the clear objective of ensuring that they do not discriminate against any person and have negative impacts for equality groups. We will always welcome comments on the impact of a policy on particular groups of people in respect of, but not limited to, age, disability, gender reassignment, race, religion, sex or sexual orientation, being pregnant or on maternity leave and children's rights and wellbeing.
Accessibility:	Accessible electronically/online and in print. All documents can be translated and made available in audio, braille and large print versions upon request.

INTRODUCTION

The purpose of this statement is to give the Association's policy on fraud and set out its responsibilities for its prevention. It also refers to the Procedure for the Management of Suspected Fraud, which outlines the action to be taken if you discover or suspect fraud.

The Association's aim is to have a culture of honesty and integrity, where there is zero tolerance of fraud and corruption (see the Association's Resolution of Difficulties Policy) and fraud and corruption is minimised. In this respect there is a requirement that all individuals and organisations, associated in whatever way with the Association, will act with honesty and integrity to safeguard the resources for which Eildon is responsible.

Fraud is an ever present threat to these resources and must be a concern to all employees and persons working for Eildon. Fraud can potentially be perpetrated by staff, Board members, consultants, suppliers, contractors or development partners, individually or in collusion with others.

The Resolution of Difficulties and its accompanying procedures (including the specialised Fraud Procedures) provides a checklist of actions and a guide to follow in the event that fraud is suspected. It covers:

- Notifying suspected fraud;
- The investigation process;
- Liaison with police and external audit;
- Initiation of recovery action;
- Reporting process;
- Care Inspectorate; and
- Scottish Social Services Council

Its purpose is to define authority, control, responsibility and reporting for the management of suspected fraud, theft or other financial irregularity.

Communication with the Scottish Housing Regulator (SHR) and with lenders is addressed by the SHR Notifiable Events Regulatory Guidance.

DEFINITION OF FRAUD

The term "fraud" is used to describe such acts as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion. For practical purposes fraud may be defined as the use of deception with the intention of obtaining an advantage, avoiding an obligation or causing loss to another party. The criminal act is the attempt to deceive and attempted fraud is therefore treated as seriously as accomplished fraud.

Computer fraud is where information technology equipment has been used to manipulate programs or data dishonestly (for example, by altering, substituting or destroying records, or creating spurious records), or where the use of an IT system was a material factor in the preparation of fraud. Theft or fraudulent use of computer time and resources, including unauthorised personal browsing on the internet, is included in this definition (see the Association's IT Security, Access and Protection of Information Policy).

THE ASSOCIATION'S ATTITUDE TO FRAUD

The Association takes the most serious view of any attempt to commit fraud by members of staff, contractors, their employees and agents on behalf of the Association and others. Staff involved in impropriety of any kind will be subject to disciplinary action, including prosecution, if appropriate. The Association treats attempted fraud as seriously as accomplished fraud.

The Association would urge prosecution of those committing an offence as documented within the Computer Misuse Act 1990. All Association staff must comply with the IT Security, Access and Protection of Information Policy and are required to read and sign the Network Access Request Form*.* Misuse of the Association's e-mail and Internet facilities may lead to disciplinary action that could include dismissal (see the Association's Resolution of Difficulties Policy and accompanying procedures (including the specialised Fraud Procedures)). The Association may also seek to claim damages through the Civil Courts.

RESPONSIBILITIES

The Association is responsible to the Board for:

- Developing and maintaining effective controls to help prevent or detect fraud;
- Carrying out vigorous and prompt investigations if fraud occurs;
- Taking appropriate disciplinary and/or legal action against perpetrators of fraud; and
- Taking disciplinary action against managers where their failures have contributed to the commission of fraud.

STAFF RESPONSIBILITIES

Line managers are responsible for the prevention and detection of fraud by ensuring that an adequate system of internal control exists within their areas of responsibility, and these controls operate effectively.

As a result, there is a need for all managers to:

- Identify and assess the risks involved in the operations for which they are responsible;
- Develop and maintain effective controls to prevent and detect fraud;
- Ensure compliance with controls; and
- Ensure agreed procedures are followed.

Every staff member has a duty to ensure that the Association's reputation and its assets are safeguarded. In the first instance, any suspicion of fraud, theft or other irregularity should be reported, as a matter of urgency by that member of staff to their line manager or by a Board member to the Chief Executive or Chair. If this would be inappropriate (where for example the line manager might be involved), then concerns should be reported upwards to the:

- The relevant Director or
- Director of Finance & Corporate Services or
- Chief Executive or, where absent, Chair of the Association; or
- Where it is the Chair of the Association that is being reported this should be reported to the Chair of the Audit & Risk Committee.

Additionally, all concerns must be reported to the Director of Finance & Corporate Services unless such action is thought to compromise the complaint. (The Director of Finance & Corporate Services' role is to be responsible for the oversight and control of fraud and appropriate reporting).

MANAGEMENT OF SUSPECTED FRAUD

The Association has a Procedure for the Management of Suspected Fraud which can act as a checklist of actions and a guide to follow in the event of fraud being suspected.

REVIEW

This policy should be reviewed within five years unless required earlier due to changes in the law, regulation, best practice or requirements of the Association.