Anti Fraud Policy and Fraud Response Plan

Status of document: Approved			
Version: 1			
Date of approval: 3 February 2026			
Effective from: 3 February 2026			
Owner: Audit, Finance and Risk Committee			
Author: Director of Corporate Services and Chief of Staff			
Planned next review date: January 2031			
Version	Author	Date	Changes
1	DoCS; CoS	January 2026	Policy created – supersedes anti-financial crime policy.
1.1	CoS	February 2026	Minor addition to complete 1.3 of Fraud Response Plan.

1. Policy statement

1.1 The GOC has a zero-tolerance policy in relation to fraud and is committed to preventing, detecting and eliminating fraud. We will assess any suspected or reported cases promptly and, where necessary, investigate.

2. Purpose

2.1 This fraud policy and response plan sets out how the General Optical Council (GOC) will prevent, identify, investigate and respond to actual or suspected fraud, theft and irregularities.

2.2 The policy sets out the key terms relating to fraud, the roles and responsibilities of those working on the GOC's behalf, and what we have put in place to prevent and reduce the risk of fraud.

2.3 The plan gives a framework to follow in responding to allegations of fraud, bribery or corruption. It allows evidence to be gathered and collated in a way which informs decisions, while ensuring that evidence gathered will be admissible in any future criminal or civil action.

2.4 The GOC ensures that fraud prevention procedures are proportionate to the risks identified through formal assessments. For example:

- High-risk areas such as financial transactions and procurement are subject to enhanced controls;
- lower risk areas may be managed through periodic spot checks and awareness training; and
- procedures are reviewed regularly, to ensure they remain appropriate and effective.

3. Scope

3.1 This policy applies to anyone undertaking work on the GOC's behalf (the workforce). This includes all employees, agency staff, consultants, Council members, committee members, workers and contractors.

3.2 Everyone undertaking work on the GOC's behalf is expected to be familiar with their responsibilities under this policy.

4. Definitions

4.1 Please note that where we refer to 'fraud' throughout the policy, it could mean any of the following activities:

Abuse of position

4.2 Exploiting a position of trust within the GOC for financial, material or another inappropriate and/ or unauthorised benefit

Bribery

4.3 Bribery is illegal, and an offence under the Bribery Act 2010. The 4 key offences established by the Bribery Act 2010:

- offering, promising, or giving of a bribe to another person (section 1)
- requesting, agreeing to receive, or accepting a bribe (section 2)
- bribery of a foreign (non-UK) public official (section 6) and
- failure by commercial organisations to prevent bribery committed by their associated persons to obtain or retain business, or an advantage in the conduct of business (Section 7).

4.4 In this context, we take commercial organisations to include those organisations who tender to deliver services on behalf of the GOC. A key internal control for preventing bribery is the GOC gifts and hospitality policy.

Fraud

4.5 The Fraud Act 2006 defines fraud as one of the following:

- fraud by false representation (Section 2 of the Act);
- fraud by failure to disclose information when there is a legal duty to do so (Section 3 of the Act); and
- fraud by abuse of position (Section 4 of the Act).

4.6 In order for the activity to qualify, the following must apply:

- the conduct must be dishonest;
- the intention must be to make a gain; or cause a loss or the risk of a loss to another; and
- no gain or loss needs to have been made.

4.7 At the GOC, we make a distinction between ‘internal’ and ‘external’ fraud, though the two can be related to one another.

4.8 Internal fraud is fraud where an individual engaged by the GOC (either as a member, employee, contractor or worker) acts in a way that is fraudulent or intends to be fraudulent. This could be intending to make a gain or cause a loss or risk of loss against the GOC. It could also be using their relationship with the

GOC to intend to make a gain or cause a loss or risk of loss against another person or organisation. Internal fraud is likely to be a serious issue and could constitute a disciplinary matter, for example, for gross misconduct.

4.9 External fraud is fraud perpetrated by third parties against GOC (e.g. contract fraud or fraudulent invoices). In the case of contractor or suppliers, a finding of fraud will normally lead to termination of their contract. If there is any suspicion of collusion on the part of employees in an external fraud, the procedures relating to internal fraud will be adapted to apply as appropriate.

Misuse of equipment

4.10 Deliberately misusing materials or equipment belonging to the GOC for financial, material or other inappropriate benefit.

Theft

4.11 Dishonestly acquiring, using or disposing of physical or intellectual property belonging to GOC or to individuals working on behalf of the organisation.

5. Responsibilities

Council

5.1 As trustees of the GOC, Council has a duty to manage the charity's resources responsibly. This includes ensuring there are policies and procedures in place to:

- identify the risks of fraud at the GOC
- take actions to protect the GOC
- check that those actions are working.

5.2 The fraud policy and response plan and other related policies are a critical component of ensuring the appropriate internal controls are in place for preventing, detecting and eliminating fraud. Council has a collective responsibility to ensure that these policies and internal controls are in place and achieving their stated objectives. Council is also responsible for setting the corporate culture in respect to fraud and exhibiting the necessary leadership behaviours to ensure their leadership is visible to others.

5.3 Council members are encouraged and expected to raise any concerns. They should normally report any concerns to the Chair of Council, Senior Council Member, Chief Executive and Registrar or Chief of Staff.

5.4 If the issue concerns the Chief Executive the concern should be raised with the Chair of Council, or with the Senior Council Member it concerns the Chair of Council.

Audit, Finance and Risk Committee (ARC)

5.5 ARC has several delegated responsibilities from Council in relation to fraud prevention, monitoring the internal control environment and risk management. ARC will be responsible for supporting the executive with providing assurance to Council that these are working effectively and minimising risk and impact in relation to fraud.

5.6 ARC will be responsible for monitoring fraud and counter-fraud activities. This includes fraudulent activity reported via its regular exceptions report and periodic reviews of the internal control environment in respect to fraud.

SMT

5.7 SMT has a collective responsibility for reducing the risk of fraud and ensuring that the controls in place to prevent and investigate fraud. This includes creating an organisational culture that is effective in identifying, preventing and investigating fraud. Individual members of SMT are responsible for ensuring this culture is reflected in the work of their directorates, and in the leadership behaviours they exhibit and expect of their teams.

5.8 Individual members of SMT will also be responsible for ensuring that the departments responsible for identifying, preventing and investigating fraud are free to work without undue restriction and with the appropriate resources. These are likely to include (though not limited to):

- Finance
- Governance
- Internal and external audit
- IT
- Legal
- People and Culture

Leadership team

5.9 Leadership team is expected to appropriately assess and identify the risk of fraud in respect to their individual departments and put the appropriate controls in place to minimise this. Leadership Team members must ensure that advice is sought on how to minimise the risk of fraud from the appropriate departments, including:

- Finance
- Governance
- Internal and external audit
- IT
- Legal
- People and Culture

5.10 Leadership Team will be collectively responsible for regularly reviewing the internal control environment relating to the identification, prevention and

investigation of fraud. It will provide advice and assurance to SMT and where necessary escalate issues.

People managers

5.11 People managers have a responsibility to reduce fraud through the monitoring and oversight of the workforce, ensuring their own behaviour is consistent with GOC values and in contributing to a workplace culture that prioritises fraud prevention. All people managers should comply with their obligations in GOC policies designed to identify and prevent fraud. It is critical that all people managers are familiar with their responsibilities under the Fraud Response Plan. This will significantly reduce the risk that they will negatively impact the organisation's response to alleged fraud, either deliberately or by mistake. Failure to follow the requirements of the Fraud Response Plan is likely to be considered a serious matter and could lead to disciplinary action.

Employees, agency staff, consultants and contractors

5.12 Employees are encouraged and, indeed, expected to raise any concern that they may have, without fear of recrimination. To facilitate this, the GOC has a Freedom to Speak up Policy for employees, members and workers. Any concerns raised will be properly assessed and, where necessary, investigated. It is not always possible to protect the identity of the person raising concerns, especially is criminal behaviour is alleged, though the GOC will take steps to protect the individual from being treated unfairly because of the disclosure.

5.13 Employees are often the first to spot possible cases of fraud or corruption at an early stage. Employees should not try to carry out an investigation themselves. This may damage any subsequent enquiry.

5.14 In the first instance, staff should normally raise the concern with their line manager. Where staff have a difficulty in approaching their own manager, because there is a concern that either management are involved or may not take the matter seriously, they can contact any of the alternative people listed in the Freedom to Speak Up policy for employees, members and workers.

5.15 If the concern relates to a line manager, then employees should raise it with a director, and if it relates to a director, the concern should be raised with the Chief Executive and Registrar.

5.16 If the issue concerns the Chief Executive and Registrar the concern should be raised with the Chief of Staff and Head of People and Culture. If it relates to the Chair of Council, the concern should be raised with the Chief of Staff. Where concerns are raised regarding the Chief Executive and Registrar or members are raised, the Chief of Staff will do an initial assessment and then refer the matter to the most appropriate authority. This could include the Chair of Council (if the complaint is about the Chief Executive and Registrar), the Senior Council Member (if the complaint is about the Chair of Council) or others as suitable.

5.17 Regardless of seniority, discouraging or interfering with the reporting of fraud, or intimidating others so they are prevented from reporting fraud, is likely to

constitute gross misconduct and will be treated as a disciplinary matter. The freedom to speak up policy for employees, members and workers sets out a where people can access independent advice when whistleblowing.

6. Identifying, preventing and investigating fraud: the internal control environment

The internal control environment

6.1 The GOC operates an extensive internal control environment to identify, prevent and investigate fraud. This environment is also intended to minimise impact should a loss-event or instance of fraud occur. These internal controls fall into four categories:

- **Preventative:** Examples include staff induction, key financial control procedures (Segregation, Physical, Authorization, Management, Supervision, Organisation, Arithmetic, Personnel (SPAMSOAP)), regular cyber-security and fraud-awareness training, promoting a robust freedom to speak up culture, due diligence and pre-employment checks
- **Corrective:** Examples include management responses to internal audit recommendations, a formal investigation, lessons learned reviews, insurance policies, escalation to the Police and other authorities.
- **Directive:** Examples include employee role descriptions, code of conduct, GOC policies and standard operating procedures
- **Detective:** Examples include phishing exercises, exceptions reporting, regular reconciliation of financial transactions and internal audits.

6.2 It is essential all these systems work together in a coordinated way to prevent, identify and properly investigate fraud across the GOC.

6.3 The Director of Corporate Services will convene a quarterly review of the effectiveness of the internal control environment with the following key risk-owners and managers in the business:

- Chief Financial Officer (anti-financial crime and money laundering)
- Chief of Staff (ethics, probity, governance and compliance)
- Facilities manager (on-site security)
- Head of IT (cyber-security)
- Head of People and Culture (people and culture)

6.4 The sections below set out some of the specific areas the workforce should be aware of in respect to the internal control environment.

Communication

6.5 Everyone working on behalf of the GOC must understand and comply with their responsibilities under this policy. To support this, the GOC publishes this policy on its website and ensures it is accessible to the workforce. The policy will be provided to all new starters. Training and induction requirements will be determined as described in the section on training below.

Governance framework

6.6 The GOC operates within a governance framework of legislation, policies and procedures. A number of these have a critical role in the identification, prevention and investigation of fraud. These include, but are not limited to:

- Anti-fraud policy and response plan
- Contracts and procurement policy
- Council Scheme of Delegation
- Council Standing Orders
- Credit card policy
- Disciplinary Policy
- Expense Policy
- Financial Regulations
- Freedom to Speak Up Policy for Members, Workers and Employees
- Gifts and Hospitality policy
- Information Governance framework
- Investigations policy
- IT policy
- Management of Interests policy
- Member Code of Conduct Council
- Reward and Recognition Delegated Decision Making Framework
- Risk appetite
- Risk management policy
- Safeguarding policy
- Scheme of delegation for financial management
- Serious and significant incident policy

6.7 Everyone working on behalf of the GOC is expected to be familiar with their responsibilities as described in the framework.

Organisation-wide systems and processes

6.8 In addition to the governance framework, there are several financial, IT and people related systems and processes in place to prevent fraud and corruption, and to minimise loss where these do occur. We require everyone working on behalf of the GOC to act in accordance with their responsibilities as set out in the framework, and to comply with all reasonable instructions regarding the systems and processes relevant for their roles and responsibilities.

Procurement

6.9 The GOC requires all individuals engaging suppliers of services on behalf of the GOC to ensure that service suppliers are selected through a transparent and competitive selection process and due diligence is carried out on partners and suppliers before entering into contracts. Further information is set out in the GOC's contracts and procurement policy.

7. Identifying, preventing and investigating fraud: workforce

Culture and ethical environment

7.1 It is critical that the conduct of the workforce does not undermine public confidence in the regulation of registrants, or the GOC's ability to fulfil its statutory duties. A strong ethical culture is fundamental to preventing fraud and corruption. The GOC is committed to fostering an environment where integrity, transparency, and accountability are embedded in everyday practice. This means:

- **Tone from the Top:** Leaders must model ethical behaviour and demonstrate zero tolerance for fraud and corruption.
- **Open Communication:** The workforce should feel safe to raise concerns without fear of retaliation, supported by clear speaking up and reporting mechanisms.
- **Shared Responsibility:** Fraud prevention is not just a compliance function; it is a collective responsibility across the entire workforce.
- **Continuous Awareness:** Regular training and communication reinforce expectations around ethical conduct, fraud risks, and reporting obligations.
- **Values in Action:** Our organisational values guide decision-making and behaviour, ensuring that actions align with public trust and our statutory responsibilities.

7.2 A positive culture reduces opportunities for fraud and strengthens confidence in the GOC's ability to regulate effectively.

7.3 The workforce, including Leadership team, SMT, Council and committee members, are expected to adhere to the Nolan Principles of public life:

- **Selflessness:** Holders of public office should act solely in terms of the public interest.
- **Integrity:** Holders of public office must avoid placing themselves under any obligation to people or organisations that might try inappropriately to influence them in their work. They should not act or take decisions in order to gain financial or other material benefits for themselves, their family, or their friends. They must declare and resolve any interests and relationships.
- **Objectivity:** Holders of public office must act and take decisions impartially, fairly and on merit, using the best evidence and without discrimination or bias.
- **Accountability:** Holders of public office are accountable to the public for their decisions and actions and must submit themselves to the scrutiny necessary to ensure this.
- **Openness:** Holders of public office should act and take decisions in an open and transparent manner. Information should not be withheld from the public unless there are clear and lawful reasons for so doing.
- **Honesty:** Holders of public office should be truthful.

- **Leadership:** Holders of public office should exhibit these principles in their own behaviour and treat others with respect. They should actively promote and robustly support the principles and challenge poor behaviour wherever it occurs.

7.4 Members must comply with the Code of Conduct for Members and all relevant legislation, Charity Commission guidance and other applicable standards.

7.5 All individuals within the workforce must uphold GOC values and comply with the following requirements:

- **Declaration of Interests:** As set out in the *Management of Interests Policy*, all relevant interests must be declared.
- **Gifts and Hospitality:** Any offers of gifts or hospitality—whether accepted or declined—must be declared in accordance with the *Gifts and Hospitality Policy*. Failure to disclose such offers, whether intentional or inadvertent, is a serious matter and must be reported to the Chief of Staff.

7.6 Declarations of interests, gifts and hospitality may be subject to random or targeted verification checks, including comparison against procurement, contract and supplier records or publicly available data where appropriate.

Workforce recruitment

7.7 To minimise fraud risk, robust checks must be carried out during recruitment to verify, as far as possible, the integrity of potential workforce. Recruitment processes must comply with the relevant policies and written references must be obtained before formal engagement terms are offered. In exceptional circumstances, the GOC may permit people to begin without references with the agreement of the Head of People and Culture.

7.8 For temporary workforce roles, appropriate checks will be undertaken by the relevant contractor, agency, or workforce provider. The People Manager and Head of People and Culture are responsible for ensuring that systems for these checks are in place for all individuals working on behalf of the GOC.

Workforce contracts and related employment policies

7.9 Employment contracts, worker and consultancy agreements and any related people policies will include provisions designed to mitigate fraud and corruption risks. These will be reviewed regularly by the Head of People and Culture, with support from the Chief Legal Officer as appropriate, to ensure they remain current and reflect emerging responsibilities or risks related to fraud prevention, detection, and investigation.

Training

7.10 The Chief of Staff, Head of People and Culture and Director of Corporate Services will regularly review training requirements for those working on behalf of the GOC in relation to this policy and their roles and responsibilities. The training requirements will be documented in a compliance training plan.

7.11 The workforce will receive induction training on the Fraud Policy and the Freedom to Speak Up Policy. Mandatory fraud awareness and detection training will be provided periodically to all staff, with enhanced training for those engaged in finance, procurement, regulation, investigations, IT security or senior leadership roles.

Behavioural risk indicators

7.12 Concerns relating to conduct, behaviours, boundary issues, undeclared conflicts of interest, inappropriate relationships with suppliers or partners, or repeat low-level control breaches may collectively indicate increased fraud risk.

7.13 Where repeated conduct concerns arise, they may be reviewed collectively alongside fraud intelligence to assess whether escalation under the Fraud Response Plan is appropriate, even where individual incidents would not normally warrant full investigation.

Disciplinary measures as a preventative control

7.14 GOC disciplinary policies act as a preventative measure by ensuring that employees understand the consequences of engaging in fraudulent activity:

- **policy enforcement:** Breaches of this policy, including failure to declare interests, gifts, or hospitality, or any involvement in fraudulent activity, will be treated as serious misconduct.
- **consequences:** Disciplinary action may include formal warnings, suspension, or termination of engagement, in accordance with the relevant People policies and contractual/engagement terms.
- **referral to authorities:** Where appropriate, cases may be referred to law enforcement or regulatory bodies.
- **recording and reporting:** Outcomes of disciplinary processes will be documented and, where necessary, reported to relevant oversight bodies to maintain public confidence.

7.15 These measures are designed to reinforce ethical standards and deter fraudulent behaviour by making clear that misconduct will result in significant consequences.

7.16 Members are subject to a member code of conduct, and the code will reflect the specific responsibilities and preventative controls in place for members. The code will impose parallel standards and expectations to the rest of the workforce where it is appropriate to do so.

Annex 1: Fraud Response Plan

1. Relevant policies

1.1 The Chief of Staff will be responsible for ensuring that all matters of fraud utilise any relevant and related GOC policies and procedures, and that the relevant operational risk owner is engaged as appropriate in the process. For example, this may include using the investigation and disciplinary policies in the case of allegations of fraud related to employees.

1.2 The Chief of Staff and Head of People and Culture will be responsible for advising on compliance with the policies and procedures that are relevant to the issue, unless there is a conflict of interest. In such circumstances, expertise may be provided from elsewhere if the fraud response lead determines it necessary.

1.3 Where policies have not expressly covered a scenario, the fraud response lead will be responsible for determining the most appropriate course of action based on the GOC's statutory powers and duties.

2. Reporting fraud or corruption: what to do if you have concerns

2.1 We welcome speaking up and we will listen when someone does. By speaking up at work you will play a vital role in helping us improve the working environment for our employees, members, contractors and workers, and the services we provide for the public and our registrants.

2.2 Speaking up against acts of fraud is not easy. Before you do so, you should read the freedom to speak up for employees, members and workers, as this will help you understand your responsibilities and how the organisation will support you in speaking up or whistleblowing.

2.3 In any situation where you are concerned about fraud or corruption, you should contact Andy Mackay-Sim, the Chief of Staff, at whistle-blowing@optical.org

2.4 The freedom to speak up policy provides further details of alternative routes you can use to report fraud or corruption, if your concerns relate to the Chief of Staff.

2.5 It is not always possible to protect confidentiality, particularly when a crime is alleged to be committed or has been committed. However, the GOC is committed to protecting everyone who works on its behalf from unfair treatment as result of speaking up.

2.6 If an allegation is made in good faith, but it is not confirmed by the investigation, no action will be taken against the person raising the concern. Action will only be taken where there is clear evidence of deliberate bad faith intended to mislead or undermine others.

2.7 During an investigation, those working on behalf of the GOC should be careful about not breaching confidentiality and not voicing their concerns to others without good reason. To do so could jeopardise the investigation process. To support individuals who are involved in an issue, the relevant senior person (whether this is the strategic lead for speaking up or another relevant person) will identify someone that the individual can speak to if they need further support.

2.8 Where appropriate the GOC will ensure that the person raising the concern is kept informed of the investigation and its outcome, as set out in the GOC's investigation policy.

3. Fraud response plan

Initial assessment

3.1 Once information is received about a suspected fraud or a suspicion of corruption, it must be reported immediately to the Chief of Staff as strategic lead for speaking up. All allegations of fraud or corruption will be treated as a whistleblowing concern and will be considered under the relevant policies. The Chief of Staff will be responsible for signposting the relevant policy or policies, and any listed sources of external advice and support to the individual as a priority.

3.2 The Chief of Staff will make a provisional assessment based on risk and impact. This will consider the risks and impact including (but not limited to) financial loss, legal risk. reputational risk and public protection. The risk management policy and significant incident policy will be used in making such an assessment.

3.3 Where necessary, the Chief of Staff may consult with the relevant operational risk owners, such as the Head of People and Culture (for employee relations matters) or Chief Financial Officer (for fraud related to contract payments). The Chief of Staff will be responsible for logging all such assessments and providing a rationale for any action taken or not taken.

3.4 Nothing within this policy will prevent allegations which do not meet the criteria for fraud and corruption or do not engage the fraud response plan from being considered via other relevant policies if it is determined necessary for further action by the relevant operational risk owner or the Chief of Staff. It is important that the relevant risk owners coordinate with the Chief of Staff to ensure that an individual or individuals do not experience unfair treatment because of raising allegations in good faith.

Issues requiring a fraud response

3.5 The Chief of Staff will escalate any substantive allegations to the next stage of the process. This will require the engagement of the fraud response plan.

3.6 Where appropriate, the Chief of Staff will ensure that the Director of Corporate Services and/or Chief Executive and Registrar are informed.

3.7 The Chief of Staff will be responsible for assessing likely conflicts of interest and nominating a fraud response lead for each occasion that the fraud response plan is engaged, with the following conditions:

- Except in cases where there is an unmanageable conflict of interests, the Director of Corporate Services will act as the fraud response lead for employees up to and including Leadership Team. If the matter concerns the Chief of Staff, it will automatically be assigned to the Director of Corporate Services, unless that creates an unmanageable conflict.

- If the matter concerns SMT, or the Director of Corporate Services has an unmanageable conflict of interests, then the Chief Executive and Registrar will either act as fraud response lead or nominate a suitable alternative.

- If the matter concerns a member, the Chief of Staff will use the relevant policies related to member conduct to determine who is the appropriate fraud response lead.

3.8 If the matter concerns someone working on behalf of the GOC who is neither an employee nor member, then the Chief of Staff will consult with the relevant department head to identify a relevant fraud response lead.

3.9 The fraud response lead is expected to seek advice and expertise for the relevant operational risk owners where appropriate.

The fraud response-lead

3.10 The fraud response-lead should satisfy themselves that there are reasonable grounds for the suspicion and engage the relevant GOC policies.

3.11 The lead decision-maker will consider whether to:

- take steps to prevent a loss or minimise a loss;
- decide the level at which other members of the workforce should be involved and bring the allegations to their notice if appropriate, including any proposed next steps (such as engaging the disciplinary policy or investigation policy);
- take whatever action is needed to secure records and assets, including restrictions on access to office, laptops and data which can include monitoring of individual's laptops and also requesting back-up of data from an employee's laptop;
- decide whether to seek legal advice;
- decide whether the Police should be informed;
- review suspension of employees who are the subject of allegations with the relevant decision-manager; and/or
- agree a timetable for completion of the agreed action.

3.12 In reviewing options, the fraud response lead should seek advice from the Head of People and Culture (for all employees) and the Chief of Staff (for members) before making such a decision.

3.13 The Chief of Staff will log reports of suspected or actual frauds in a central Fraud Register. The Fraud Register will be reviewed periodically to identify emerging risks, recurring patterns or systemic weaknesses and inform preventative actions, policy updates and training priorities.

4. Investigation – Scope

4.1 Investigations will be undertaken in accordance with the GOC's investigations policy.

4.2 It is important to consider carefully the terms of reference for any investigative work necessary to establish the facts. Investigations should not be restricted solely to allegations against an individual that may lead to a charge of gross misconduct.

4.3 If there is a possibility that instances of serious misconduct (e.g. misconduct other than fraud) may also have occurred, these should be investigated at the same time as the fraud allegations.

Investigation manager – maintaining the integrity of an investigation where fraud or another crime is alleged

4.4 It is particularly critical in cases of alleged fraud that the investigation manager should retain securely any relevant documentation, in its original format and it should not be written on or altered in any way. Other items or equipment relevant to the investigation must be safeguarded without any alteration to their original condition, for example, laptops and any records thereon. It is expected that the workforce will comply with all reasonable requests for disclosure where personal devices have been used, particularly in cases where this has resulted in non-compliance with the GOC IT policy.

4.5 A detailed record of the investigation should be maintained. This should include a chronological file recording details of telephone conversations, discussions, meetings and interviews, details of documents reviewed, and details of any tests and analyses undertaken.

4.6 All interviews should be conducted in a fair and proper manner. Where there is the possibility of criminal prosecution, advice should be sought from the police to ensure that our proceedings do not prejudice the criminal investigation.

4.7 The fraud response lead and investigation administrator will ensure there is an appropriate legal, employment and financial expertise available to the investigation manager to provide advice and guidance as necessary.

5. Report and findings

5.1 As soon as any investigations and other related processes (such as disciplinary hearings) has been completed, reports and any other relevant documentation (subject to any confidentiality requirements) should be passed to the fraud response lead and Chief of Staff. The Chief of Staff is responsible for storing all information relating to alleged fraud securely and capturing any outcomes for the Fraud Register.

5.2 The fraud response lead and Chief of Staff will determine what information is shared with relevant regulators and other statutory authorities.

6. Referral to authorities

6.1 Any information shared externally will be co-ordinated by the Chief of Staff. This could include reporting to the police, Charity Commission, Professional Standards Authority (PSA), Privy Council and other statutory agencies and regulatory authorities.

7. Communications strategy

7.1 Any communications, internal or external will be managed by the GOC's Communications team.

8. Recovery and redress

8.1 The GOC's statutory role as a regulator and charity will be the first order of priority, followed closely by the recovery of GOC's assets. Where necessary, this will be through civil and criminal proceedings. The Director of Corporate Services will be responsible for making any decisions regarding the recovery of assets, with reference to relevant legal advice.

9. Post incident review

9.1 Where evidence of fraud or serious misconduct has been identified, the GOC will consider whether any action needs to be taken to prevent a recurrence. In such cases, a lessons learned exercise should be undertaken. The fraud response lead will be responsible for ensuring that the agreed recommendations are implemented.

9.2 A summary of the action plan will be shared with Audit, Finance and Risk Committee.

10. GDPR

10.1 All personal data obtained or processed during investigations will be handled in accordance with the UK GDPR and Data Protection Act 2018, ensuring proportionality, necessity, secure handling and timely deletion where no longer

required. This will be done in accordance with the GOC information governance policies and the relevant retention schedules for each relevant department.