COUNTER FRAUD, BRIBERY AND CORRUPTION POLICY AND STRATEGY

2024 – 2028

Contents

COUNTER FRAUD, BRIBERY AND CORRUPTION POLICY AND STRATEGY

Introduction

1. The Museum is a world-class visitor attraction and leading science research centre. We use our unique collections and unrivalled expertise to tackle the biggest challenges facing the world today with a duty to care for the collections, and for stewardship of public resources more carefully.

2. The Museum is committed to the highest standards of ethical conduct in our activities. Ethics are an essential part of decision-making and of ensuring proper and transparent administration of the Museum, with all employees expected to follow the Code of Ethics.

3. This policy is designed to comply with the requirements of the Public Sector Fraud Authority's Continuous Improvement Framework, whilst helping staff understand the broad nature of fraud, their responsibilities and what to do if any member of staff suspects or discovers fraud is happening, either by another employee or a third party.

4. Fraud will be addressed through a multifaceted, risk-based approach which includes fraud prevention via appropriate training, awareness and controls, deterrence, detection, measurement, investigations, and sanctions.

5. The strategy is aligned with the Museum's Fraud Risk Assessment, which is maintained by Risk & Assurance and updated yearly.

6. Within the timeframe of this report, we will aim to move to a state where less fraud & error happen, despite increasing sophisticated technology and will use technology to help us achieve this. The key areas of focus to get to this state correspond to the risk & challenges set out below.

7. The response plan at Appendix 1, further clarifies reporting (including options for whistleblowing) and how any reports will be dealt with and investigated.

Key Risks and Challenges

- The sustained reduction in real terms in the Museum's government grant puts pressure on the Museum to maintain / introduce new robust infrastructure (such as cyber security or physical security of the Estate).
- Increased reliance on self-generated income could lead to Museum exploring wider sources of income and having greater exposure to funds linked to fraudulent activity. This could apply to any self-generated income including retail, catering, on site donations, temporary exhibitions, merchandising, corporate event hire, etc
- New areas of activity for the Museum are inherently risky and increase exposure to other types of fraud, such as intellectual property fraud.
- Cyber security and variants of phishing attacks remain popular and are becoming increasingly sophisticated, making it harder to decipher a genuine email from a phishing attack. The use of technology to automate the creation of highly convincing fake emails, personalised to the recipient, increases the chances of success for the attack.
- The Museum is entering a period of major capital investment, contracts, and purchases, which create significant risks in both the procurement and construction phases.
- New technologies pose both opportunities and threats for the Museum. For example, Artificial Intelligence is becoming increasing common place and is now actively used by researchers.

However, generative AI in particular, is leading to increasing genuine looking documents and images ('deepfakes').

- This could facilitate theft, direct or indirect manipulation e.g., faking photographs for Wildlife Photographer of the Year, which is much easier to do using AI.

Scope

8. This strategy applies to any Natural History Museum site, its Trading Company, and all staff, volunteers, contractors, their employees or agents, and others acting on behalf of the Museum. Staff includes permanent, fixed term contract, temporary and seconded staff, externally funded and Trustees.

9. The Fraud, Bribery and Corruption Response Plan **(Appendix 1)** sets out how to report suspicions and how investigations will be conducted and concluded

Fraud

10. The Fraud Act 2006 outlines three methods for fraud:

- False representation (a representation that is misleading or untrue and the person making it is aware of this).
- Failing to disclose information when there is a legal duty to do so; and
- Abuse of position (where a person occupies a position where they are expected to safeguard the financial interests of another person).

11. Put simply, fraud is an act of deception intended for personal gain or to cause a loss to another party. There does not need to be a direct financial gain / loss. The term also includes the use of IT equipment to manipulate or access programmes or data dishonestly, and is governed by the Computer Misuse Act 1990. The Office for National Statistics estimates that for the year ending March 2022, the latest data available, 61% of reported fraud was cyber related.

12. As fraud can be any form of deception to gain advantage, a broad range of activities constitute fraud, including (from most to least obvious):

- Travel & Subsistence overclaims
- Change to bank details / bogus boss e-mails
- Spurious invoicing
- Lower quality substitute products
- Flexi-working abuse
- Intellectual property misuse / theft
- Manipulation of KPIs

Bribery

13. The Bribery Act 2010 outlines four key offences:

- Offering or paying a bribe to another person
- Requesting or receiving a bribe
- Bribing a foreign public official to perform routine functions they are otherwise obligated to perform e.g., granting licences or permits
- Failure of commercial organisations to prevent active bribery being undertaken on their behalf.

14. Bribery can take many forms, including cash / payments gifts, lavish business entertainment or tickets to an event.

15. Under the Act the Museum may be liable for bribery committed for its benefit by staff or others acting on its behalf. To mount a successful defence against such a charge the Act requires the Museum to have in place adequate procedures designed to prevent bribery.

Corruption

16. Corruption is often most simply defined as “the abuse of entrusted power for private gain”. In a Museum context, this may mean any activity undertaken where an individual would personally benefit from the Museum’s brand/ activity. This could include misuse of the Museum’s logo to promote a private service. The same definition would apply to a similar abuse by an organisation without defined mechanisms by which to operate on the museum’s behalf.

Money Laundering

17. Money Laundering (ML) is a closely related crime to fraud, which involves integrating money from crime into legitimate use. Due diligence procedures are designed to adequately ensure that any donations have come from legitimate sources. This also applies to collections acquisitions, to ensure that additions to the collections were obtained legally.

18. Please refer to the Gift & Sponsorship Acceptance Policy and the Due Diligence Process for more guidance / information on due diligence within the Museum. Further information on due diligence with respect to collections acquisitions can be found in the Collections Development Policy.

Other Offences

21. Other offences include the misuse of IT equipment as set out in the Computer Misuse Act 1990. Additionally, the Data Protection Act 2018 requires the Museum to safeguard personal data of living persons. The Museum could be held responsible for personal data exposure if personal data is released through a cyber-attack, which may then lead to fines / additional reputational damage if the Museum is deemed liable (e.g. through not having sufficient controls to stop an attack).

Gifts and Hospitality

22. The **Gifts and Hospitality Policy, Procedure and Guidelines** sets out the Museum’s approach to staff receiving gifts and hospitality (G&H). The Museum can provide bona fide hospitality without breaching the Bribery Act 2010 provided it is proportionate and reasonable.

23. Given the potential for certain Museum staff to receive many offers of G&H, it is critical we adhere to policy and recording procedures. In either the giving or receiving of gifts or hospitality, there must be no explicit or implicit attempt to influence third parties or be influenced by third parties in relations with the Museum.

Facilitation payments

24. Staff and others acting on the Museum's behalf must not make payments to anyone to facilitate or expedite decisions or actions no matter how small the payment.

25. All Staff travelling abroad should undertake risk assessments and receive appropriate training, with travel to high-risk destinations not allowed. However, if an employee finds themselves in an exceptional situation where they need to make a payment to maintain their safety or extract themselves from a sudden and unexpected dangerous situation, (such as at a road check point, usually in politically volatile countries), payment should be made with a receipt requested and all details noted as soon as possible and reported to the Chief Operating Officer. Once back at the Museum, the situation will be reviewed to understand if it was avoidable. Please refer to the Travel Risk Management Policy for more information.

Anti-Fraud Statement

26. Suspected acts of fraud, bribery, or corruption by staff are viewed very seriously by the Museum and if confirmed following an investigation, will be subject to disciplinary action, irrespective of whether the activity was successful (discovered afterwards) or when it was taking place. In response to allegations, we will:

- investigate individual cases of suspicion thoroughly, dealing with them appropriately, promptly, and efficiently.
- refer individual cases to the relevant statutory authority to investigate when there are reasonable grounds to suspect criminal offences may have been committed. Investigations of staff misconduct may run concurrently with criminal investigations.
- refer all cases where investigation establishes that staff misconduct has occurred for consideration of disciplinary action.

27. As a non-departmental public body, we are also required to report all incidents of fraud or error on a quarterly basis to the Department for Culture, Media, and Sport. The returns are managed by Finance, who track both actual and prevented fraud.

28. Investigations will be undertaken by a counter fraud specialist in central government. Please see the Response Plan in Appendix 1 for more information.

Responsibilities

Museum Director

29. The Museum Director in his role as Accounting Officer has overall responsibility for ensuring the Museum has robust measures in place to counter fraud, theft, and bribery and corruption activity.

30. Day to day responsibility is delegated to the Chief Operating Officer, who is the Accountable Individual at board level responsible for such matters and the Museum's counter fraud champion.

31. The Museum is responsible to the Trustees (primarily through the Audit and Risk Committee) for:

- developing and maintaining effective controls to prevent and detect fraud, theft, bribery or corruption

- undertaking prompt investigations of fraud, theft, bribery, or corruption occur
- taking appropriate disciplinary and/or legal action against those who commit acts of fraud, theft, bribery or corruption
- taking disciplinary action against managers where their failures have contributed to the commission of acts of fraud, theft, bribery or corruption.

32. The Museum will also undertake all mandatory counter fraud processes, including:

- Use of Initial Fraud Impact Assessments
- Submission of quarterly performance data (managed by Finance)
- Compliance with the Counter Fraud Functional Standard
- Agreement of annual action plans and metrics

Staff Responsibilities

33. All staff have a duty to act honestly and with integrity, and ensure public funds are safeguarded in whatever area of the Museum you work. Additionally, all staff:

- must adhere to the controls designed to prevent and detect fraud, theft, bribery, or other forms of dishonesty.
- must alert their line manager immediately they notice an opportunity for fraud, theft bribery or any form of dishonesty, for example poor procedures or lack of effective supervision.
- should be alert to unusual behaviours, events or incidents that could be indicators of fraud (see the training for further information).
- must report immediately any suspected fraud, theft, bribery or any suspicious acts using the processes outlined in the **Whistleblowing Policy**.
- must assist in any investigations by making available all relevant information you have and by co-operating in interviews.

Contract Manager Responsibilities

34. In additional to general staff responsibilities listed in para (32), contract managers (for major, ongoing contracts) have some additional specific responsibilities, in both the procurement and contract management phases, including:

- Ensuring they have undertaken the level of contract management training commensurate with the risk and value of the contract(s) they manage.
    - This is currently undertaken via the Crown Commercial Service online training, which has three levels – foundation, intermediate and advanced, with each level building on the previous one. The foundation level will be adequate for most contract managers, but those with particularly high value contracts may need to undertake the intermediate and advanced training.
- Discussing anti-corruption commitments and controls with the preferred supplier – this may include adding a contract clause that the NHM can terminate the contract and take damages if such controls are breached.
- Ensuring there is an effective and safe reporting mechanism for breaches of procedures whether financial, health and safety related or other. This includes ensuring anyone working under the contract is aware of the procedure.
- Monitoring and auditing of work – ensuring that the work undertaken is of the right quality and quantity (this could apply to both major construction contracts and ongoing service / maintenance contracts as examples).

- More generally, contract managers are expected to have undertaken suitable training - to at least foundation level and proportionate to the risks of the contact(s) they manage - to ensure the best value for money from the contract can be achieved.

Heads of Department (HoDs)

35. HoDs are responsible for the prevention and detection of acts of fraud, theft, bribery, and corruption by ensuring an adequate system of internal control exists within their areas and that controls operate effectively, though regular reviews and testing.

36. All HoDs should assess fraud risks in the areas they are responsible for and are encouraged to log these in a risk register. Further information on this is available in the Risk Management Policy.

37. HoDs should also ensure that staff have undertaken appropriate contract management training and build this into their objectives where they do not currently hold it. The training is described above in paragraph 34. Further advice can be sought from either the Risk and Assurance Manager or the Procurement team.

Risk and Assurance Manager

36. The Risk and Assurance Manager is responsible for:

- Delivering an opinion to the Museum Director (Accounting Officer) on the adequacy of the arrangements for managing the risk of fraud, theft, bribery, and corruption and ensuring that the Museum promotes an anti-fraud, theft, bribery, and corruption culture.
- Completing reviews of control systems to support the detection and prevention of fraud, theft, bribery, and corruption.
- Maintaining a fraud, bribery, and corruption risk assessment/risk profile.
- Keeping up to date with the fraud ‘landscape’ and latest trends (such as the impact of emerging technology on fraud)
- Keeping the fraud training up to date, ensuring it as accurate and relevant
- offering advice and assistance on risk and control issues.
- Working with Finance to develop suitable counter-fraud metrics, to help assess the effectiveness of current counter-fraud processes.

Risk Assessment

37. It is important for the Museum to understand the risks it faces including fraud, bribery and corruption.

38. The Trustees and Museum Director take the view that risk management should be a part of our culture and integrated into our philosophy, practices, decision-making and planning processes. The Museum believes that risk management is everyone’s business.

39. The Museum maintains a centrally controlled high level and detailed fraud, bribery, and corruption risk profile. These are living documents and are updated on an on-going basis as new risks are highlighted. This helps to ensure lessons are learnt, risks are monitored and managed effectively.

Lessons Learned / Post Incident Evaluation

40. In the commission of fraud, theft, bribery, or other acts of corruption it is likely that weaknesses in existing control mechanisms and procedures will have been exploited or exposed. To prevent recurrence, it is essential that these weaknesses are identified and addressed.

41. Except in cases where a fraud is trivial, once any immediate investigation has taken place, a lessons learned review shall also be carried out. This should be done regardless of whether there was direct financial loss or possible indirect losses.

42. The senior manager of the area impacted is responsible for undertaking the review, which should be done within a month of the incident. Risk & Assurance can help and advise on any post incident reviews.

43. The methods used in the crime will have been established during the investigation. It will be necessary to:

- isolate the underlying control weaknesses. Each weakness should be quantified in terms of its contribution to the acts of fraud, theft, bribery or corruption and the risk of recurrence if it is not addressed.
- agree effective solutions.
- document the above and draw up an associated action plan.

44. As well as pursuing action to address control weaknesses in the area affected by the fraud, theft, bribery, or other irregularity, it is important that steps are taken to minimise similar risk throughout the Museum. Subject to secrecy considerations, a brief synopsis of significant irregularities should be prepared by the Risk and Assurance Manager setting out the key lessons learnt by the business. This report should be distributed to the Chief Operating Officer as a minimum as well as the Museum's Audit and Risk Committee and Museum Director if large or significant enough.

45. Once remedial procedures and controls have been developed and implemented it will be necessary to carry out new risk assessments.

Appendix 1 – Counter Fraud, Bribery & Corruption Response Plan

1. This Counter Fraud, Bribery and Corruption Response Plan sets out our policies and procedures for ensuring that all allegations of fraud, theft, bribery, or other acts of corrupt behaviour are promptly and effectively followed up and considered in a consistent and fair manner. The definition of fraud, bribery and corruption, the Museum's attitude to them and the roles and responsibilities of the various groups of staff involved in the prevention and detection of fraud, bribery and corruption are given in the Museum's Counter Fraud, Bribery and Corruption Strategy in the first part of the document.

2. This plan provides guidance to ensure that actions are taken to:

- minimise the risk of any subsequent losses.
- reduce any adverse operational and reputational effects.
- improve the likelihood and scale of recovery of assets.
- reduce the chance of a similar event recurring.

3. The plan includes guidance and information for staff on issues such as:

- to whom fraud, theft, bribery or corruption or the suspicion of these acts should be reported.
- the treatment of suspect employees, including supervision of their removal from the premises, the prompt recovery of Museum property, suspension and when appropriate termination.
- who within, or outside of, the Museum will investigate fraud, theft, bribery, or corruption.
- the securing and preserving of evidence, including documents and computer held evidence.
- the recovery of assets.
- the involvement of the Police, including issues to be considered in deciding whether to prosecute individuals concerned.
- the reporting of progress of the investigation to senior management
- the need to complete a post investigation review to highlight things done well and lessons learnt.
- the need for effective communication.

Notification of fraud, theft, or bribery

4. If you suspect a colleague, contractor or member of the public may be involved in fraud, theft, or corrupt activities then you are expected to report such suspicions to your line manager as soon as possible. This may be verbally at first, but you should record your concerns in writing afterwards. See the Whistleblowing section (#12 - # 14) below for more guidance.

5. In this context your "Line Manager" is the person in charge of the team in which you work, regardless of grade. If this person is not available, you should contact the next higher person, (i.e., the line manager's boss) instead.

6. If you feel your line manager may be involved, you should report your suspicions to their manager or directly to your HR Business Partner, the Internal Audit Manager, or the Union. See the 'Whistleblowing' section below for more information.

7. Where losses of IT equipment or mobile phones are discovered, these should be reported via the Technology Solutions Service Desk.

8. Any line manager who receives a fraud report from their staff or member of the public must report the incident immediately to their director, or the Chief Operating Officer.

9. The line manager should make discreet initial enquiries to ascertain the facts and confirm or refute the allegations as far as possible. It is important they do not take any action which may forewarn the alleged perpetrator, who may tamper or destroy evidence. They should seek to ensure that any readily available documentary evidence is secured for the investigation process. Discussing such suspicions more widely than necessary may also harm innocent colleagues. More guidance is given in the 'response' section below.

10. The line manager should never attempt to investigate the suspected fraud or corruption personally beyond these initial enquiries. If the suspected fraud or inappropriate behaviour has been undertaken using IT assets or mobile phones, under no circumstances should the ICT asset be accessed, as IT forensic specialists may need to be brought in. See the appendix 'The principles of computer-based evidence' for further information.

11. Any allegations shared, regardless of whether they involve a Museum employee, will only be shared with those who need to know. Most allegations escalated will need to include Finance, HR, Internal Audit and / or external investigators. Additionally, fraud or attempted fraud which involves the use of computers or networks should be reported to the Information Security Manager (Technology Solutions) and if a data breach is suspected, this also needs to be reported to the Data Protection Officer.

Whistleblowing

12. The Museum is committed to creating a culture that encourages staff and others to identify fraud, bribery and corruption risks and raise concerns.

13. The Whistleblowing Policy explains what to if you have a reasonable belief there has been serious wrongdoing in the Museum, the policy will enable you to raise your concerns without fear of reprisal. If there are any sensitive matters, or if you fear reprisal, you can raise the matter with HR, the Internal Audit Manager, or the Union. Please refer to the Policy for full details.

14. Our response will be determined by consideration of:

- the actual or potential financial loss
- the apparent extent of staff or management involvement
- likely media interest
- concerns regarding the potential impact on the Museum's reputation.

Response

15. If a suspected or actual fraud, theft, bribery, or irregularity is reported to you:

- make a written record of the key pieces of information received.
- preserve any evidence you have acquired or been given.
- evaluate the information given. As far as possible without raising any suspicion, you should check what you have been told. Is the allegation possible? Is the source reliable? Consider discussing this with your line manager or Head of Department, who will keep it in confidence.
- Anything that warrants further investigation should be notified to the Internal Audit Manager
- If an investigation is necessary, this will be undertaken by counter fraud specialists within government and will not be undertaken internally.

16. Additionally, the Museum will seek advice from the Public Sector Fraud Authority when dealing with highly complex, novel, and sensitive fraud cases, or cases that carry a high potential for reputational damage to the government.

17. It is then important to ensure that the individual(s) suspected is denied the opportunity to commit further acts of fraud, theft, bribery, or corruption. In the case of suspect clients, suppliers and other third parties, staff also having contact with them should be alerted to the problem and asked to cease normal dealings pending the conclusion of investigations.

18. In circumstances where staff involvement is suspected, beyond any initial fact finding, a hearing by HR may be undertaken and consideration will be given to:

- suspending the individual, pending conclusion of full investigations.
- securing the individual's desk, contents, and office, with the option for this to be supervised by either their manager or a union representative.
- revoking access to and disabling all the individual's digital accounts
- recovering the individual's Museum pass, keys, and Museum laptop & mobile phone
- ensuring that the individual leaves the premises immediately and does not have the opportunity to access, alter, remove, or destroy potential evidence, including data held on, or accessible through, a computer.
- If an employee is not physically present in the Museum at the time, disabling the TS accounts will prevent unauthorised access to Museum systems laptop and depending on the outcome of any investigation, the employee will be asked to come in to hand these over.
- securing accounting and other records, and where appropriate, suspending any authorisation levels.
- ensuring that no-one takes action which may change data held on a computer or other media which may subsequently be relied on in court, please see the Appendix.

19. These risk reduction procedures may be suspended temporarily to carry out evidence gathering procedures prior to revealing the existence of an allegation to the suspect. Also see paragraphs 26-31.

Fraud, theft, and bribery investigation

20. To help ensure the achievement of the investigation objectives, the investigation of suspected or actual acts of fraud, theft, bribery, or corruption needs to be carried out by people with the necessary specialist skills and training.

21. Any report requiring more than a standard internal investigation will be undertaken by a specialist counter fraud and investigation team who are members of the Government Counter Fraud Profession or other external specialists depending on the nature of the fraud.

22. An internal investigation may be something such as the misuse of a Government Procurement Card, where there is an obvious pattern of personal spending. If all or part of any loss can be recovered from a Museum insurance policy, then notification of the suspected fraud or theft should be made by registered letter to the insurer.

23. Data from any investigation will be held for six years, following the end of the investigation. Data is stored securely on the Museum's SharePoint site and the time information is in line with the Information Asset Register. Additionally, any personal data stored is kept in line with GDPR requirements.

Planning an investigation

24. To maximise the effectiveness of the investigation, clear objectives should be set at the earliest possible opportunity.

25. The principal objectives will be to:

- establish the facts, e.g., the scale of the fraud, theft, or bribery, how it was perpetrated and by whom, the loss or potential loss, to the Museum.
- minimise adverse publicity.
- minimise the adverse impacts on the Museum's business.
- recover funds or other assets.
- prevent the repetition and deter others.

Dealing with employee(s) under suspicion

26. It is important to ensure that any employee(s) who are under suspicion of committing fraud or corruption are treated fairly. Any action taken to suspend or dismiss an employee must only be taken in conjunction with the Director of HR or Head of HR.

27. Where the allegations are serious and there is a potential risk of evidence being tampered with or undue influence on the investigation then the employee should be given a leave of absence or suspended to allow the investigation to continue unhindered. Suspension is a neutral act to enable a full and fair investigation and should not be regarded as an indication of guilt.

28. If employee(s) are suspended, careful consideration will be given as to who should be informed and how the absence should be communicated to other employees or contacts. This will depend on the circumstances and will take account of the need to protect evidence and the organisation, as well as the suspended employee(s). Advice should be sought from HR, who will seek further legal advice if necessary.

29. Where an employee is to be informed of suspension(s), the following must be made clear:

- That there will be a fair and thorough investigation into any claim made.
- That the employee has been suspended to facilitate the investigation.
- That no assumption that the employee has been involved in any wrong-doing has been or should be made.
- That the matter is confidential and so the employee must not discuss this with anyone else not involved in the investigation

30. If the decision is made to allow the employee(s) under suspicion to remain in the workplace, additional pre-authorised surveillance may be necessary, including, for example, a search of the work area, filing cabinets and computer files.

31. Where material assets have clearly been stolen, the line manager in conjunction with security, should contact the police as soon as possible to log the thefts and record the crime reference number.

Recovery of Loss/Assets

32. NHM will seek to recover all assets lost or misappropriated as a result of fraud, theft, or corruption. The process of recovery will depend upon the nature and circumstances surrounding the loss, and whether the fraud results in criminal charges being laid.

33. Once the size and extent of the loss has been confirmed, action will be taken to trace and freeze the lost assets, where possible, so that the recovery process can be commenced.

34. Civil action will be considered on a case-by-case basis if criminal proceedings are not underway (where a confiscation order might be applied).

35. All losses, even if recovery has been made, must be reported to Finance so that the amount can be recorded and written off where appropriate as well as to avoid a reoccurrence in the future.

36. For cases which do not involve police involvement, consideration will be given as to how best to recover assets lost or misappropriated, which might include repayments by agreed arrangement, possibly through payroll deductions where fraud has been committed by employees.

Media management

37. If a significant fraud is suspected or proven, this may result in press enquiries, which will be handled by the Head of Media and PR.

38. To ensure uniformity one person only should deal with media enquiries. All relevant staff, senior managers, and the telephone operators should be made aware that all calls should be directed to the spokesperson who should be fully briefed on the agreed response and kept informed of developments.

Department for Digital, Culture, Media and Sport (DCMS)

39. The Museum is required to submit a quarterly fraud and error return (including nil returns) to DCMS. This exercise is required by the Cabinet Office who has the lead in supporting Government by taking initiatives to fight fraud against the public sector. In addition, the requirement to report fraud including: (a) loss due to proven and suspected fraud; (b) or prevented fraud is included in the Management Agreement with DCMS. Returns are completed by the Finance Team who should be notified of actual and attempted frauds.

Appendix to Response Plan

The principles of computer-based evidence

Computer-based evidence is the term used to describe information that may be presented in a Court of Law which originates from data stored on either a computer or computer media. There are five guiding principles:

- No action taken should change data held on a computer or other media which may subsequently be relied upon in Court.
- In exceptional circumstances where a person finds it necessary to access original data held on a target computer that person must be competent to do so and to give evidence explaining the relevance and the implications of their actions
- An audit trail or other record of all processes applied to computer-based evidence should be created and preserved. An independent third party should be able to repeat those processes and achieve the same result.
- The onus rests with the head of the investigation team to ensure compliance with any law pertaining to the possession of, or access to, information contained on a computer. He or she must be satisfied that the use of any copying device or actions of any person having access to the computer complies with these laws.
- The onus of ensuring that these principles are adhered to and that the evidence is admissible rests with the head of the investigation. He or she must be satisfied that the use of any copying device or actions of any person having access to the computer complies with these principles.

The onus is on the prosecution to show to the Court that the evidence produced is no more and no less now than when it was first taken into the possession of the investigating team.

Appendix 2 - Examples of Fraud

External Party Fraud

Examples include:

- procurement fraud e.g., invoicing twice for goods and services, colluding with staff or other suppliers in the tender process to win a contract unfairly, requesting payment for goods and services which have not been delivered.
- mandate fraud, an unauthorised request is made to change the details of a bank transfer mandate, to divert payments to a fraudsters' account.
- selling fake specimens to the Museum.
- using trickery to win a Museum competition.
- some deliberate intellectual property infringements may be a criminal offence – copyright, misuse of the Museum's logo, unauthorised use of patented products, processes, etc.
- e-crimes by people using computers and technology to commit fraud e.g., phishing, hacking, or social engineering frauds.

Insider Fraud

Inside fraudsters can hold any post at any level from the most senior manager to a junior member of staff.

Examples of fraud committed by insiders include:

- the theft of physical assets, including cash.
- false claims for travel and expenses, such as overstating mileage and claiming for journeys that were not made.
- misuse or unauthorised use of Government Procurement Cards.
- working elsewhere while on sick leave and faking being sick.
- payroll fraud e.g., claiming for overtime that was not worked or unauthorised hours.
- unauthorised use of Museum assets or intellectual property.
- a member of staff processing unauthorised payments to themselves.
- false references or false qualifications used to secure employment.
- staff colluding with criminals to defraud the Museum.
- fabrication and misrepresentation of science research data.

Appendix 3 – Related Policies and Procedures

The Museum has a framework of policies and procedures to support the application of this strategy. This strategy should be read in conjunction with the related policies and procedures.

Other related references

- Whistleblowing Policy
- Gifts and Hospitality Policy
- Procurement Matters 2 - Conflicts of Interest, Gifts, Hospitality, and Inducements
- Financial Regulations
- Business Expenses Guidelines
- Code of Conduct
- Disciplinary Policy
- Risk Management Policy / Guide to Effective Risk Management
- IT Security Policy
- IT Conditions of Use
- Good Research Practice

POLICY SIGN-OFF AND OWNERSHIP DETAILS		
Document name:	Counter Fraud, Bribery and Corruption Policy and Strategy	
Version number:	V1.0	
Document type:	☒ Policy ☒ Procedure ☐ Guidance	
For use by:	☒ All NHM staff (Museum-wide policy) ☐ External parties	
Approval level required:	Audit and Risk Committee	
Approved by:	**Name**	Audit and Risk Committee
	Date	November 2023
Review schedule	5 years maximum, or sooner if / when there are significant changes to the risk landscape, government counter fraud requirements or legislation.	
Effective from:	January 2024	
Date of next review:	December 2028	
Stakeholders consulted during draft or review process:	**Name**	**Title**
	Helen Whitehouse	Chief Operating Officer
	William Parsloe	Head of Legal
	Lewis Kershaw	Financial Accounting Manager
	Chris Sleep	Information Security Manager
	James Downs	Head of Security
Author: [Name, Title]	Kevin Coughlan, Risk & Assurance Manager	

REVISION HISTORY			
Version	**Date**	**Revision description/Summary of changes**	**Author** (Name, Title)
V1.0	Jan 2024	Major redraft – old policy not clear on version information so reset	Kevin Coughlan, Risk and Assurance Manager