Anti-Fraud Policy

Sponsor:	Corporate Director, Business Services
Owner:	Director of Business Services Operations
Date Approved:	24th March 2022
Date for Review:	March 2025 – 3-year review cycle
Distribution:	Non-Confidential for Internal and External Use

Policy Statement	Barnardo's is committed to conducting its operations in accordance with the highest standards of integrity and ethics. The organisation expects all of its Trustees, employees, volunteers and partners to meet the same standards. As such, we are committed to ensuring that Barnardo's, its funds and assets are appropriately protected from misappropriation, misuse, theft, fraud or misrepresentation, to ensure that all our funds and assets are directed to the benefit of the children, young people and families we serve. The **Fraud Act 2006** reshaped previous legislation to tackle a wide range of fraudulent activity, creating a new general offence of fraud and setting out three ways by which it is committed: ▪ fraud by false representation. ▪ fraud by failing to disclose information; and ▪ fraud by abuse of position. It also created new offences: ▪ obtaining services dishonestly with intent to avoid payment. ▪ possessing, making and supplying articles for use in frauds; and ▪ participating in a fraudulent business carried on by a sole trader. The Theft Act 1968 covers the criminal definition of theft and associated offences such as false accounting. All definitions and abbreviations can be found below. This policy should be read in conjunction with the policies highlighted in the relevant sections.

Policy Objectives	The objectives of this policy are to:
	▪ Ensure that Barnardo's complies with relevant charity legislation.
	▪ Define what constitutes fraud.
	▪ Detail our expectations of Trustees, employees, volunteers, and partners in relation to:
	  ○ undertaking training in relation to prevention of fraud.
	  ○ following approved processes and procedures designed to mitigate the risk of fraud and associated criminal acts.
	  ○ escalating concerns promptly and appropriately; and

	○ our response and general action plan in the event that a fraud is suspected or detected to ensure that further funds are not taken or at risk, and to recover as much of the misappropriated funds as possible. This policy does not cover the approach to safeguarding information from internal and external parties (eg bank account and credit card details of donors) to prevent their misuse, whether electronically or otherwise. For further information on these aspects, readers should refer to the **Information Security Policy**, **IT Code of Conduct**, **Data Protection Policy,** and all associated processes.

Scope	This policy applies to all Trustees, employees (i.e. all staff, workers and contractors) and volunteers in Barnardo's.

Definitions and Key Concepts

The following details various terms and definitions used within this policy.

Term	Explanation
Associated Party or Partner	Any individual or corporate party which is associated with Barnardo's in terms of provision of services (either providing services to Barnardo's or receiving services from Barnardo's), other than Service Users.
CEO Impersonation Fraud	A specific type of Invoice Fraud (see below) where the Fraudster impersonates a senior member of staff in the Charity via email, requesting an urgent payment to be made to a supplier/subcontractor, complete with bank payment details.
Contractual Partner	Any individual or corporate body that Barnardo's contracts with to provide services to it, including where we operate as a sub-contractor of a broader contract.
Due Diligence	The process and steps that need to be taken by Trustees to be reasonably assured of the provenance of the funds given to the charity, confident that they know the people and organisations the charity works with and are able to identify and manage associated risks.
Employees	Includes all staff, workers and contractors.
Fraud (including Theft)	Encompasses any dishonest act to obtain a gain or cause a loss, including, but not limited to: ▪ making a false representation to obtain a gain or to cause a loss. ▪ failing to disclose information in order to obtain a gain or to cause a loss. ▪ abusing a position to obtain a gain or to cause a loss; or ▪ dishonestly taking property belonging to another person or organisation with the intention of permanently depriving that person or organisation of the property. Fraudulent conduct can take many forms. Appendix 1

	attached contains a list of fraudulent conduct to which Barnardo's may be exposed.
Functional Fixed Assets	For the purposes of this policy, functional fixed assets include land, buildings, vehicles, and equipment.
Gift Aid	A scheme that enables tax-effective giving by individuals to charities in the United Kingdom. Any cash donations that the taxpayer makes to a charity after making a declaration are treated as being made after deduction of income tax at the basic rate, and the charity can reclaim the income tax paid on the gift from HMRC.
Identity Theft	A form of fraud in which person/company A pretends to be person/company B by assuming person/company B's identity. Typically, this is done in order to access resources or obtain credit and other benefits in person/company B's name.
Invoice Fraud	A form of fraud where the fraudster sends an organisation an email or letter, or phones purporting to be from a legitimate supplier/subcontractor, advising of a change of bank details for payment which are actually an account controlled by the fraudster
Joiners, Movers, or Leavers Process (JML Process)	The process followed by Line Managers in relation to giving or removing relevant access rights to/from Barnardo's IT and other systems for employees or volunteers when they join Barnardo's, move between departments, or leave the charity.
Money Laundering	The process of turning the proceeds of crime into property or money that can be accessed legitimately without arousing suspicion. The term 'laundering' is used because criminals turn 'dirty' money into 'clean' funds which can then be integrated into the legitimate economy as though they have been acquired lawfully.
National Crime Agency (NCA)	A crime-fighting agency with national and international reach and the mandate and powers to work in partnership with other law enforcement organisations to bring the full weight of the law to bear in cutting serious and organised crime.
Phishing	The criminally fraudulent practice of attempting to acquire sensitive information (such as usernames, passwords, bank account details) by masquerading as a reputable organisation in electronic communication (i.e. emails).
Service Providers	Any individual or corporate body that is engaged by Barnardo's to perform services on its behalf, including all sub-contractors and agents of Barnardo's.
Serious Incident	An incident that has occurred in a charity is considered serious if it has resulted or could result in a significant loss of funds or a significant risk to the charity's property, activities, beneficiaries or reputation. If a charity has an annual income of more

		than £25,000 its Trustees must, as part of the annual return, sign a declaration that there have been no serious incidents which ought to have been reported to the Commission but were not. If the Trustees are unable to make this declaration the annual return will not be complete, and they will have defaulted on their legal requirements.
	Smishing	The criminally fraudulent practice of attempting to acquire sensitive information (such as usernames, passwords, bank account details) by masquerading as a reputable organisation in text communication.
	Suspicious Activity Report (SAR)	A disclosure to the National Crime Agency under either the Proceeds of Crime Act 2002 or the Terrorism Act 2000.
	Vishing	The criminally fraudulent practice of attempting to acquire sensitive information (such as usernames, passwords, bank account details) by masquerading as a reputable organisation in voice communication (i.e. phone calls or voice messages).

Roles and Responsibilities

The main roles and responsibilities in relation to this policy are as follows:

Role	Responsibility
Board of Trustees	To ensure that this policy is in place and is appropriately communicated and embedded in the organisation, clearly highlighting its importance.
Audit & Finance Committee	To review and approve the policy at relevant intervals; and oversee and monitor the adequacy and effectiveness of the policy and associated processes and procedures across Barnardo's.
CLT	To reinforce the importance of adherence to this policy and all associated processes and procedures on an ongoing basis.
Policy Sponsor	To ensure: the policy and associated processes and procedures are reviewed at regular intervals and remain appropriate in the light of emerging best practice; the policy is appropriately implemented and enforced; the Audit and Finance Committee receives relevant and timely information to assist in its oversight and monitoring of the policy; and that all Trustees, employees, and volunteers receive appropriate regular training/awareness messaging on the requirements within this policy.
Policy Owner	To maintain the policy and associated procedures; develop training/awareness notifications for all Trustees, employees, and volunteers; undertake periodic risk assessments of the fraud and associated risks facing the organisation; and ensure that management information demonstrating adherence to this policy is produced and provided to relevant

		parties.
	Line Managers	To ensure that all their employees (including volunteers) undertake the training/are made aware of the requirements of the policy as part of induction and at agreed frequencies thereafter; and follow the procedures outlined in this policy.
	All Trustees, employees & volunteers	To follow this policy and associated processes and procedures. This includes co-operating with any investigation as appropriate.
	Internal Audit	To independently review adherence to this policy and associated processes and procedures across the charity.

Policy

1. Overarching Principles:

It is essential that Barnardo's Trustees, employees, and volunteers act in the best interests of the charity at all times, and hence appropriately protect the funds and all assets of the charity, ensuring that they are not misappropriated, misused, misrepresented, stolen or subjected to fraud.

You **must:**

- act in the best interests of the charity at all times.
- ensure that all transactions are entered into and authorised appropriately/in line with policy (e.g., following Barnardo's procurement, tendering or other approved process), supported by appropriate written evidence, (e.g., approved contracts, purchase orders, original (VAT) receipts etc) and are promptly and accurately recorded in Barnardo's financial records.
- follow the required processes and procedures outlined in this Policy at all times, together with those outlined in any applicable Directorate or other local policy.
- ensure relevant documentation which supports financial items (income or expenditure) are retained in line with Barnardo's Document Retention Policy (unless specifically stated otherwise); and
- immediately report ***any*** attempted, suspected, or actual fraud identified, regardless of amount or method (including cyber related fraud), to the Corporate Director Business Services, the Director of Audit and Assurance, or the Company Secretary.

You **must not**:

- engage in unauthorised transactions involving Barnardo's funds or assets, including committing to any contract, payment, asset transfer or other obligation on behalf of Barnardo's, unless authorised to do so;
- take or use Barnardo's funds or other assets without appropriate authorisation.
- enter into unwritten agreements, side letters or off-the-books arrangements that do not meet Barnardo's contracting standards.

- approve any financial transactions that are outside appropriate policy or unsupported by appropriate written evidence, such as a contract, purchase order, invoice, or receipt.
- disguise the true nature of any contract, payment, asset transfer or other obligation — for instance, by improperly recording the counterparty, the value of the transaction, or the purpose of the transaction in Barnardo's financial records.
- disclose confidential information connected with Barnardo's to anyone regardless of the circumstances, unless appropriately authorised to do so, including never disclosing your passwords, any bank details, PINs etc.
- open suspect attachments on emails, instead report such incidents to the IS Service Desk.
- make a false representation on behalf of Barnardo's at any time.
- fail to disclose relevant information or deliberately or knowingly provide false or inaccurate information when requested by Barnardo's or Associated Party.
- account falsely in relation to any aspect of your dealings with Barnardo's, including claiming expenses outside policy guidelines or destroying, concealing, or altering any documentation relating to Barnardo's; or
- abuse a position of trust (or exploiting a conflict) to obtain an improper advantage for Barnardo's, yourself or any person associated with you, such as by rigging a procurement exercise to benefit family members or friends

2. Reporting and response

Barnardo's is committed to responding to any allegation of fraud in accordance with the Fraud Response Plan appended to this Anti-Fraud Policy.

All instances of attempted, suspected, or actual fraud identified, **regardless of amount or method**, must be immediately reported to the Corporate Director Business Services, the Director of Audit and Assurance, or the Company Secretary.

You may choose to remain anonymous when reporting a known or suspected issue and you will not be subject to reprisals for reporting information about potential problems in good faith.

If you feel someone in Barnardo's has experienced retaliation as a consequence of making a good faith report, please immediately contact the Director of People.

Any report of suspected, attempted, or actual fraud will be treated extremely seriously and investigated in full, using the procedures outlined in this policy. The Director of Audit and Assurance, with support from relevant areas, will be accountable for implementing the Fraud Response Plan, as detailed in Appendix 3. If the allegation of Fraud involves Audit and Assurance in any regard, the report must be promptly forwarded/made to the Chair of the Trustees.

If you are asked by Barnardo's to assist with an investigation, you should

always provide truthful and accurate information. Providing untrue or misleading statements, or encouraging others to do so, may result in disciplinary action.

If you are contacted by the police or any other investigatory agency concerning allegations of fraud, please immediately contact: the Corporate Director Business Services C or the Company Secretary.

If you are notified that documents in your possession are required for an investigation or legal matter, you should follow directions to preserve those documents. You must never destroy, conceal, or alter those documents in any way.

Failure to abide by any of the principles and procedures in this policy could result in disciplinary action, up to and including termination of employment. It may also involve notification to relevant law enforcement agencies for investigation and prosecution, or commencement of civil proceedings. In particular, Barnardo's has a **zero-tolerance** approach to fraud or theft and will diligently work with the relevant authorities to investigate suspected, attempted or actual fraud and theft and will support the prosecution of the perpetrators of such activity where appropriate.

3. Warning Signs of Fraudulent Conduct:

There are many signs of fraudulent conduct, including, but not limited to:

- discrepancies in accounting records.
- insufficient support for transactions (e.g., expenses claim's that are not supported by original receipts, or requests for payments to suppliers that are not supported by contracts or original invoices).
- missing financial records.
- duplicated payments or other transactions.
- significant unexplained variances between forecasted accounting figures and actual accounting figures.
- use of restricted funds for general purposes.
- discrepancies in asset registers.
- indications that income is being under-reported or expenditure over-reported.
- significant cash transactions that cannot be fully audited.
- reluctance on the part of individuals dealing with financial matters to accept assistance, have an over-protective behaviour towards their work, or never/rarely take holidays of more than a few days consecutively; and
- inconsistent, vague or implausible responses from individuals dealing with financial matters.

If you identify any of the above warning signs (or other related concerning matters), please immediately contact: Corporate Director Business Services, the Director of Audit and Assurance, or the Company Secretary. They can also provide further guidance on potential fraud warning signs (or provide resources to assist).

There are a range of minimum controls which need to be consistently and appropriately operated throughout Barnardo's to ensure that the charity is adequately protected against fraud. Further details on these are provided

	in the relevant sections below. **3. Record Keeping Requirements:** Barnardo's Trustees, employees, volunteers, and partners must take appropriate steps to ensure that: ▪ all transactions entered in to by Barnardo's: ○ are authorised appropriately/in line with policy (e.g., following Barnardo's procurement, tendering or other approved process); ○ are supported by appropriate written evidence, (e.g., approved contracts, purchase orders, original (VAT) receipts etc); and ○ are promptly and accurately recorded in Barnardo's financial records, with the relevant details appropriately recorded (such as the recipient, the value and the purpose of the transaction); and ▪ all information/documentation pertaining to the financial records of the charity must be retained securely in line with Barnardo's Document Retention Policy (unless stated otherwise). Detailed requirements are provided below where relevant. **4. Risk Assessment:** Fraudsters and criminals are continuously adapting their techniques and becoming increasingly sophisticated in their methods, adopting new technologies and targeting organisations' vulnerabilities. This is against the background of various responsibilities being placed on Barnardo's in Charity and other legislation around taking reasonable precautions to protect the financial and other assets of the Charity. Given this, the Policy Owner, with assistance from relevant individuals and information gleaned from internal fraud investigations and wider market intelligence on fraud trends, will undertake a detailed risk assessment of the fraud and theft risks facing Barnardo's at least every two years. This will then be used to inform required changes to this policy, any associated processes and procedures or training/awareness notifications as required. **5. Communication and Training Requirements:** To facilitate the appropriate understanding and embedding of this policy and its associated processes and controls: ▪ there must be periodic communication of the importance of appropriate adherence to this policy, including how to report any concerns. ▪ relevant personnel must be given training in relevant financial processes, procedures, and associated controls; and ▪ all Trustees, employees and volunteers must receive training/be made aware of the requirements of this policy as part of their induction process and at suitably regular intervals thereafter.

Mandatory Procedures	There are various mandatory procedures relating to this policy.

Associated Guidance and Other Documents of Note	As outlined above, the requirements in this policy should be considered alongside the requirements of the following policies: ▪ Gifts and Hospitality Policy ▪ Anti-Bribery and Corruption Policy ▪ Conflicts of Interest Policy ▪ Anti-Money Laundering Policy ▪ Due Diligence (Acceptance and Refusal of Donations and Working with Third Parties) Policy ▪ Sub-Contractor Due Diligence Process ▪ Procurement Policy ▪ Tendering Policy/High Value/Opportunity Process

References	▪ None

Compliance and Oversight	Compliance with this policy will be assured by: ▪ **The Policy Owner:** reviewing relevant training records; undertaking investigations into suspected or actual fraud to identify potential weaknesses in controls and hence actions required; and undertaking random reviews of fraud mitigation processes, and relevant records on a minimum annual basis to ensure it is appropriately embedded. ▪ **Internal Audit:** as part of any audit, Internal Audit will, where appropriate, consider and review relevant fraud controls highlighting any concerns together with relevant recommendations. Internal Audit may also lead the investigations into more material instances of fraud.

Review and Approval	This policy will be reviewed by the Policy Owner at least every three years following each Risk Assessment undertaken or earlier in the event of: identification of serious weaknesses in relevant processes and procedures following investigations into attempted, suspected or actual fraud; or market intelligence related to changes in the techniques and methods being used by fraudsters. The Policy will be subject to approval by the Audit and Finance Committee.

Appendix 1 – Potential Types of Fraudulent Conduct

There are many potential types of fraudulent conduct to which Barnardo's may be exposed, including, but not limited to:

- taking or misusing assets, including financial assets, without authorisation.
- false accounting.
- destroying, concealing, or altering documentary records.
- providing inaccurate information to obtain an improper advantage; or
- abusing a position of trust to obtain an improper advantage, such as by rigging a procurement exercise to benefit family members or friends.

Detailed examples:

- banking system theft and fraud, including misuse of the charity's bank account.
- fraudulent credit or debit card transactions or charges.
- intercepting postal donations and cheques.
- failing to pass on money from public charitable collections.
- stealing or 'skimming-off' money from cash collections.
- fake fundraising events and requests for donations (i.e., by parties fraudulently portraying themselves at Barnardo's).
- theft from charity shops and trading activities.
- using the charity's databases or inventories for personal profit or unauthorised private commercial use.
- fake grant applications.
- claiming inappropriate expenses.
- fraudulent Gift Aid claims.
- the creation of false invoices or purchase orders.
- the creation of false employees or inflated expenses, overtime, or other claims; or
- providing services to beneficiaries who do not exist, and other forms of identity fraud.

Appendix 2 – Advice Provided to Donors to Minimize Risk of Fraud or Theft

Information Provided to All Donors

To help protect all donors who donate directly to the charity (other than through external collection tins or fundraising events) from mass market fraud, we:

- always send them a thank you acknowledgement for the donation.
- if we need to change the details of the bank account to which the payment is made, we will contact them by letter and ask them to contact us using their regular contact approach
- we will never contact them to change information by text or email or ask for confidential bank account information, such as bank passwords etc; and
- .

Spoof Websites

We provide the following advice to donors or customers who are proposing to make donations through websites:

- always update your information online by using the process you have used before or open a new browser window and type in the website address of the legitimate organisation's account maintenance page.
- be wary of unfamiliar website addresses, as they may not be genuine. Only use the address that you have used before or start at your normal homepage. Avoid unfamiliar links or pop-up screens.
- always report fraudulent or suspicious emails to your Internet Service Provider (ISP). This will help to ensure that bogus websites are shut down before they can do further harm.
- take note of the header address on the website. Spoof sites are more likely to have an excessively long line of characters in the header, with the business name somewhere in the string. Many secure sites have padlock symbols and other secure technology to look out for; and
- if you have any doubts about an email or website, make a copy of its address and send it to the IS Service desk who will confirm that it is genuine.

Appendix 3 – Fraud Action/Response Plan

Initial Review

Upon receipt of a report regarding an actual or suspected fraud, the Director of Audit and Assurance, together with the Corporate Director Business Services and the Company Secretary, must review the report and determine an appropriate response.

If the report concerns an allegation of fraud involving any member of Audit and Assurance, the report must promptly be forwarded to the Chair of the Board of Trustees, who will be responsible for identifying an appropriate member of CLT to review the report and determine an appropriate response. (As such, references to the Director of Audit and Assurance should be interpreted as the CLT member designated by the Chair of the Board of Trustees if relevant).

Response

In most cases, the appropriate response will be to conduct an investigation to determine the credibility of the allegation, which will be led by the Director of Audit and Assurance, potentially assisted by a small team (the 'Investigation Team'). On consultation with relevant parties, including the CEO and, potentially, members of the Board of Trustees, it may be agreed that external advisors, such as lawyers or accountants, should be appointed to assist with the investigation.

On deciding the proposed response, the Director of Audit and Assurance must notify the Risk Committee, (or if the report potentially concerns a member of the Board of Trustees, the Chair of the Board of Trustees). (As such, references to the Risk Committee should be interpreted to mean the Chair of the Board of Trustees if relevant).

Confidentiality

All parties to the investigation (internal or external) must maintain strict confidentiality at all times, and, as such, should receive official documentation to confirm this as part of their appointment to the Investigation Team. A breach of confidentiality could undermine the integrity of the investigation, and, therefore, the subsequent actions which may be open to the charity depending on the outcome of the investigation.

This is particularly the case if a target of the investigation is given prior notice that would allow them time to destroy, conceal or alter documents or other evidence before it has been preserved and collated.

Investigation

The Director of Audit and Assurance must determine the following:

- objectives of the investigation
  These are likely to include the following (which is not necessarily exhaustive):
  - assessing the allegation to determine whether it is credible and supported by evidence.
  - identifying any Trustees, employees, volunteers, or external partners potentially involved in the allegations.
  - the nature and type of investigation which is required to obtain any further evidence required or to identify the degree of involvement of relevant parties. This may involve reviewing physical and electronic records, interviews, and other methods.
  - collating relevant evidence relating to the allegations and preserving all relevant documentation/information.

- preventing the fraud from being continued/preserving the charity's assets (*e.g.*, preventing further unauthorised asset disposals).
- determining whether external reporting is required to the police or other agencies, such as the Charity Commission.
- determining whether disciplinary measures are required; and
- determining whether remedial measures are required.

- whether (depending on the nature of the allegation and investigation) document retention procedures (including electronic destruction processes) should be temporarily suspended in relation to the area(s) involved.
- the investigation plan, including a timetable for completing the investigation within a reasonable period.
- the approach and parties to internal and external reporting

Having determined the above, it should be shared with relevant individuals for approval, especially in relation to the timescales involved and whether early notification is required to relevant external parties dependent on the nature of the allegation. This will minimally be a relevant CLT member (or if they are potentially implicated, then the CEO) and potentially the Risk Committee.

Evidence Preservation and Collection

The Investigation Team must take appropriate steps to collect and preserve evidence relating to the allegations. This will, as noted above, include considering whether standard document retention procedures should be temporarily suspended, including ensuring the preservation of any electronic records such as email archives.

Such information will be reviewed and collated for use as evidence, together with information obtained through the conducting of relevant interviews.

All evidence preservation and collection measures must be conducted in accordance with applicable laws and internal policies, such as HR procedures for formal or informal interviews. This may also include consultation with relevant external advisors, such as lawyers, accountants or forensic specialists, to advise on or assist with evidence preservation and collection.

Asset Protection

At the outset and throughout the course of the investigation, the Director of Audit and Assurance and the Investigation Team must actively consider (and appropriately document) whether there is a reasonable risk/grounds for suspecting that there is an active and continuing risk of fraud (*e.g.*, further unauthorised asset disposals). If there is, then the Director of Audit and Assurance must take appropriate measures to ensure that assets are protected.

Such an action may involve the following:

- the suspension or amendment of current processes and procedures (e.g., amending payment authorisers, the authorisation levels, increasing the number of authorisers required to approve certain types of activity and so on); and/or
- the temporary suspension of potentially involved parties (Trustees, employees, volunteers, or partners)

whilst the investigation is conducted.

If such action is deemed appropriate, and in particular if certain parties are to be temporarily suspended, then the Director of Audit and Assurance must, as appropriate:

- consult with the Risk Committee and the Director of People before any employee, volunteer or partner is temporarily suspended; or
- consult with the Chair of the Board of Trustees and the Director of People before any Trustee is temporarily suspended.

Reporting

It is essential that appropriate internal and, where deemed appropriate, external reporting is undertaken at appropriate intervals throughout and at the end of the investigation.

- ***Internal Reporting***
  At the conclusion of the investigation, the Director of Audit and Assurance must prepare a detailed report describing:
  - the investigation processes.
  - the outcome of the investigation, including the evidential basis for any factual findings; and
  - any recommendations arising from the investigation, including recommendations relating to required external reporting, disciplinary measures, or remedial measures.

  A copy of the report must be provided to, at least, the Chair of the Trustees and the Risk Committee, who will review, debate and confirm their acceptance of the conclusions and recommendations, or agree amends thereto, which the Director of Audit and Assurance will update to finalise.
- ***External Reporting***
  In some cases, due to the size and nature of the fraud, an allegation may need to be reported to the police or other agencies, such as the Charity Commission (in line with their Serious Incident Reporting Guidelines). It should be noted that the Charity Commission recommends all fraud should be reported to the police.

  The Chair of the Board of Trustees and/or the Risk Committee must be consulted prior to the allegation being reported to any external body.

  Clearly, if the allegation is very material, or evidence is obtained during the investigation which materially alters the scale and nature of the potential fraud, consideration should be given to notifying relevant external parties at that point (as opposed to waiting for the investigation to conclude) but must always be done with the knowledge of the Chair of the Board of Trustees and/or the Risk Committee.

  All relevant parties should co-operate with such external reporting and any subsequent investigation as appropriate.

Disciplinary Action

Where an investigation provides reasonable grounds for suspecting that a Trustee, employee, volunteer or partner may have engaged in fraudulent conduct, the Director of Audit and Assurance, in consultation with other relevant parties in line with internal policies, should make a recommendation as to whether disciplinary measures are merited. At a minimum, there should be consultation with the Risk Committee and the Director of People. External advice may be sought where termination or suspension of employment, or other significant disciplinary measures, are proposed.

Remedial Investigation

At the start, throughout and the conclusion of an investigation, the Director of Audit and Assurance, along with other relevant individuals (such as Policy Owners, the Risk Committee etc) must consider whether further remediation action is required, including,

but not limited to enhancements to existing policies, processes and procedures; training; and controls and the testing thereof.

The Director of Audit and Assurance must then:

- monitor the implementation of any such remedial measures.
- report on implementation progress to Risk Committee on an ongoing basis (as part of ongoing reporting); and
- test the effectiveness of implementation within an agreed period, reporting on the results to the Risk Committee in line with standard reporting.

Further, it should be considered whether Trustees, Senior Managers or other employees would benefit from understanding any 'lessons learned' from the investigation. In which case, relevant learning documentation including training should be considered for production by Audit and Assurance based on the allegation and investigation, suitably anonymised.

Appendix 4 – References to Particular Types of (Cyber Related) Fraud

As highlighted in the main policy, fraudsters and criminals are continuously adapting their techniques and becoming increasingly sophisticated in their methods, adopting new technologies and targeting organisations' vulnerabilities. This has led to an increasing incidence of Cyber Related Fraud in recent years. Some key examples are below:

Protection Against Invoice Fraud and CEO Impersonation Fraud

Invoice Fraud - A form of fraud where the fraudster sends an organisation an email or letter, or phones purporting to be from a legitimate supplier/subcontractor, advising of a change of bank details for payment which are actually an account controlled by the fraudster.

CEO Impersonation Fraud - A specific type of Invoice Fraud (see below) where the Fraudster impersonates a senior member of staff in the Charity via email, requesting an urgent payment to be made to a supplier/subcontractor, complete with bank payment details.

Key Controls:

- All relevant employees and volunteers in Income and Innovation, Children's Services and Finance to receive relevant training/awareness raising on these types of fraud.
- Any receipt of information purporting to be from a supplier/subcontractor etc. informing of a change in bank details for payments should be separately independently verified in full – ideally by contacting your preferred (single) point of contact in the partner organisation.
- Similarly, any email purporting to be from senior management requesting an urgent payment with bank details included should be independently verified.
- Ensure all relevant financial controls are in place (e.g., bank reconciliations, reviews of supplier information, monthly reviews of expenditure at a transaction level for each cost centre etc.); and
- ***All instances*** of such suspected, attempted or actual frauds should be immediately notified to the Corporate Director Business Service, the Director of Audit and Assurance or the Company Secretary.

Protection Against Phishing, Vishing and Smishing Scams

Phishing - The criminally fraudulent practice of attempting to acquire sensitive information (such as usernames, passwords, bank account details) by masquerading as a reputable organisation in electronic communication (i.e., emails).

Vishing - The criminally fraudulent practice of attempting to acquire sensitive information (such as usernames, passwords, bank account details) by masquerading as a reputable organisation in voice communication (i.e., phone calls or voice messages).

Smishing - The criminally fraudulent practice of attempting to acquire sensitive information (such as usernames, passwords, bank account details) by masquerading as a reputable organisation in text communication.

Key Controls:

- All relevant employees and volunteers to receive relevant training/awareness raising on these types of fraud.
- Never disclose personal or security information on a site accessed through a link in an email.
- Never click on links or open attachments from senders you are unsure of.
- If suspicious, terminate the call and call back using your usual contact number and aim to speak to your usual contact – not one provided by the caller.
- On sites requiring sensitive information to be input look for https in the website address – the 's' stands for 'secure'.
- ***All instances*** of such suspected, attempted, or actual frauds should be immediately notified to the Corporate Director Business Services, the Director of Audit and Assurance or the Company Secretary.

Remember – no bank will ever ask for your full password or PIN at any time or for any reason and they will never ask for permission to access your PC or systems.

These controls also help us to protect Barnardo's against Malware and Ransomware.

Document Control

Version History:

Version	Date	Author	Status	Comment
0.1	20/8/2017	Sheree Howard	Draft	Based on initial external legal draft, with substantial rework and numerous additions, including all controls
0.2	11/9/2017	Sheree Howard	Draft	Split policy and mandatory procedures plus some minor changes
1.0	22/01/2019	James Sherrett	Final	Minor amendments before finalisation and publication
2.0	27/10/2021	Matt McHugh	Final	Review of the policy in line with review schedule. Approved by Director of Business Services Operations (Policy Owner) in January 2022. Approved by Board of Trustees March 2022.