Financial Controls policy

Charity No 1183575

Separation of Duties
No one person may both authorise and pay any payment or transfer. For example, an on-line banking payment or credit card transaction.

Conflict of Interest
No individual may:

- Authorise or make changes to his or her own pay or personnel entitlements or records, or.
- Make payments or enter into contracts with family members or organisations in which they have an interest, either directly or through a close family member.

Budgeting
The Board is to scrutinise and approve an annual budget. The budget should include prudent income forecasts that have been tested to confirm that there is a reasonable expectation of securing the funding planned for.

Financial Reporting
Up to date financial reports should be submitted to the Board regularly. Reports should use simple clear English that all board members will be able to understand and.

- Explain the charity's current and likely future financial position.
- Focus on the key issues and risks, the action being taken to address these and the expected outcome.
- Highlight any significant deviations from budget or funding shortfalls.

Financial Management
Trustees are to review financial reports, investigate any variances to budget/forecast and unusual or unexpected transactions that cannot be adequately explained and take appropriate action. Any significant issues should be reflected in reports to the Board.

Cash
- Cash and cheques are banked regularly, particularly if significant sums of cash are received.
- Cash is kept separate from personal money and is never used for personal expenditure.
- Where significant sums are to be banked, two individuals escort the money and it is transported by car, not on foot. In the event of a robbery, the money is to be handed over without resistance.
- Cash payments are avoided wherever possible.

Bank Accounts.
Bank, savings and any other form of investment are only to be opened with the written approval of the Trustees.

- The account is to be reconciled at least monthly.
- The bank reconciliation, statement, cashbook, chequebook and any other supporting documentation are cross checked.

Bank mandates, account signatories and e-banking access are to be kept up-to-date and individuals may only be added with the written approval of the trustees. The list of people with access and their access levels are to be reviewed annually, as part of the audit preparation process.

Cheques.
All cheque stubs should be completed fully. Cheque books are to be secured under lock and key, must be used in sequence and only one cheque book is to be held at any time.

Non-Standard Payment Requests.
To safeguard against AI deep fakes, any non-standard requests for payment, such as phone or video calls, must involve codewords or confirmations through a different channel.

Income
Regular checks are to be carried out to ensure that records are being accurately maintained and that there are no discrepancies in the accounting records. Specifically, that:

- Records of cash and cheques received agree with bank paying-in slips.
- The paying-in slips equate with the bank statements, both in terms of amount banked and date of credit; and
- All transfers or other direct payments into the bank can be identified and verified against paperwork.

Restricted funds - are to be accounted for separately to ensure these are only used in accordance with donors' restrictions.

Multi-year funding - is to be accounted for in a way that ensures future year funding is not inadvertently spent in the current accounting year.

Anonymous or suspicious donations - are to be subject to appropriate due diligence to minimize the risk of fraud.

Approval and Payment.
The prior approval of trustees is required for any projects or proposals in excess of £500 that are not included in the business plan and funded in the budget and for any that will result in a budget being overspent. All expenditure must be properly authorised, represent good value for money and be on appropriate items or services. Delegations and any subsequent changes are to be issued in writing and clearly specify budget lines and limits.

The treasurer is to check invoices received against orders and confirm that the goods or services have been received, are correctly priced, with any discounts or credit notes taken into account and sales tax (eg VAT) excluded if appropriate, before authorising payment.

The treasurer is to check each invoice before payment.

Electronic Payments. Anyone able to make payments is to be made aware of basic cyber security steps, including the risk of online scams, including AI voice scams. These can very convincingly imitate a member of your charity but using text and video. The following may indicate that a call is scam:

- Voice message scam calls are not live so you might notice that they use generic language.
- Where the call is live, you may be able to spot a slight delay in response as the fraudster types their reply into the software and you may even hear the tap of the keyboard).
- Be suspicious of any call or voice message out of the blue, particularly if it is from an unknown number.

Payment Procedures.

Payments systems, such as cheque books, credit cards and on-line systems and passwords should be adequately safeguarded. Physical items, such as e banking encryption devices and cheque books should be kept under lock and key when not in use. Passwords should not be written down or shared and should be changed regularly and if compromised. Accounting IT systems should be routinely backed up and back-ups stored off site in case of fire.

Cheques should always be crossed, blank cheques never signed, and mandates restricted to only those who need to sign cheques. Credit card limits should be kept as low as possible.

Travel Expenses.

Claims should be countersigned by the line manager to confirm that the journey was valid, undertaken and the amounts claimed were reasonable in the circumstances. Expenses claims are to be checked by Finance to ensure that the expenses policy has been complied with.

Other Issues

Fraud/Bribery.

If fraud is suspected, it is to be brought to the attention of the trustees.

Losses.

Any losses are to be investigated. The amount and circumstances of the loss are to be determined and, in particular, whether the loss arose from weaknesses in procedures and/or a failure to apply procedures correctly. Appropriate action is to be taken to ensure no further losses occur, arising from similar circumstances. The value of any item is to be at realisable value. Any loss must be approved for write off in line with the delegations from the Trustees. The loss is to be written off on the accounting system and the record of investigation and approval for write-off filed for audit purposes.

Records.

- Records are to be retained in accordance with the documents policy. In particular, cashbooks and other prime books of account are retained for 7 years and supporting vouchers for 18 months.
- A secure archive is identified, and records kept under lock and key.
- The archive is organised to enable records to be easily identified and retrieved.

Experience and Training.

- On appointment, appropriate work references are taken up and qualification certificates checked.
- Staff are competent and properly trained to carry out their duties in relation to finance.
- Staff are made aware of relevant financial policies on appointment and those with financial responsibilities are briefed by the finance team as part of their induction process.
- Relevant financial policy requirements are included in the Staff Handbook and job descriptions.
- That this and other guidance is readily available to staff and brought to their attention.

IT and Online Security

- Security software, such as anti-virus and firewalls, are to be kept up-to-date, preferably by automatic renewal.
- There are effective controls for authorising and managing access.
- Software updates are installed promptly.
- Passwords are strong, not shared and changed regularly.
- Data is remotely backed-up on a regular basis.

- There are disaster recovery procedures that would restore data quickly and fully enough; these have been tested.
- No sensitive financial information is to be entered into Large Language Model AI systems, such as ChatGPT or Gemini.
- Financial information, including back-ups, stored on shared drives is accessible only to those who need to have access to it.
- Adequate security procedures are in place for online purchasing.
- Staff and volunteers are aware of what they need to do (and not do) to maintain online security.