

# **Widcombe Community Hall CIO**

## **Financial Controls Policy**

### **Applicability**

This policy applies to all trustees, other volunteers, employees, contractors, and third-party representatives of our charity. Its requirements should be reflected in other policies and procedures, agreements and contracts, as necessary.

### **Separation of Duties**

Trustees have agreed to authorise three signatories on the bank account, any one of which may authorise payments.

### **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.

### **Contracting**

A robust contracting process is to be implemented with major contracts openly tendered, subject to board scrutiny and approval. Contracts and other agreements should be recorded in a simple contracts register and each reviewed annually to ensure these continue to meet the charity's needs and offer good value for money.

### **Budgeting – to be added when hall is in operation**

#### **Cash**

- Cash is secured under lock and key.
- Access is restricted to those who need access.
- A cash limit is set that is within the insurance limit.
- Cash is not sent through the post.
- Cash and cheques are banked regularly, particularly if significant sums of cash are received.
- Cash is banked 'gross' – that is income is not netted off against other expenditure. All transactions must be recorded.
- 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.

#### **Banking**

#### **Bank Accounts**

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

- The account is to be reconciled at least monthly. Signature of approval required by 2 trustees.
- The bank reconciliation, statement, cashbook, chequebook and any other supporting documentation are cross checked.

These checks are to be made by someone other than the person concerned with the original recording of the transactions.

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 Board

### **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.

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

### **Expenditure**

#### **Approval and Payment**

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.

Authorising officers are 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 Finance staff are to check each invoice before payment. Any that have not been appropriately authorised should be rejected and remain the personal responsibility of the individual who incurred the expenditure.

### **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.

Use the following to verify any caller where you are being asked to divulge sensitive information of make a funding transfer. Follow the cyber security methods outlined above, plus these may be helpful:

- Verify who the caller is by asking a question that only the real person would know the answer to.
  - For example, something discussed at a recent team meeting.
- If you are not sure, hang up and call the person back on the number you have stored for them.
- Consider creating a code word for you team that you can use to verify a caller.

### **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.

**Novel and Contentious Expenditure.** This is defined as follows:

- **Novel** - does not meet the letter of our regulations. That is, using a budget for a purpose for which it was not intended. For example, payment of a bonus to an individual, when there is no such provision in the pay policy. Or exceeding permissible limits. For example, payment of subsistence rates or class of hotel accommodation that exceed the limits in the expenses policy.

- **Contentious** - meets the letter of the relevant policy, but where the need for it or the cost involved may be questioned. For example, where subsistence has been approved within agreed limits, but alcohol or other inappropriate expenditure is claimed for.

Payment of any expenditure which may be novel or contentious requires the prior approval of the Board.

## **Assets**

### **Fixed Assets and Equipment**

Purchases of assets that have a life expectancy of, and will provide benefit for, more than one financial year may be treated as capital items and their value written down over the lifetime of the asset.

- A fixed asset register is maintained and reviewed annually.
- Items are allocated inventory codes and marked accordingly.
- Subsequent to the annual review, insurance cover is reviewed to prevent being under or over insured.
- Staff do not remove assets or items of equipment without prior approval.

## **Other Issues**

### **Fraud/Bribery**

If fraud is suspected, it is to be brought to the attention of the Chair or any other Trustee if the allegation involves the Chair.

### **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 Board. 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.

### **IT and Online Security – applies to equipment and systems owned by or used on behalf of the charity**

- 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.

On leaving the organisation, an individual's accounts are to be disabled.

### Version Control - Approval and Review

Version No	Approved By	Approval Date	Main Changes	Review Period
1.0	Trustees	1 <sup>st</sup> June 2026	First issue	Annually

### Regulatory Guidance

Charity Commission E&W

[Charities, fraud and financial crime](#)

[CC: 8 - Internal Financial Controls](#)

[Financial Controls Checklist](#)

[Compliance toolkit](#)

### Useful Links:

[Charity Governance Code: 4 Decisions, Risk, Control](#)

[CFDG: Banking for charities](#)

[BZ: Retention of accounting and other records](#)

[Charity Digital: Free anti-fraud resources for your charity \(Jan 24\)](#)

[NCSC: Password Guidance](#)

[Password strength checker](#)