Happiness Outdoors Project

Financial Control Policy

Separation of Duties

No one person may both authorise and make 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 without authorisation from a Director.
- 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 Directors will scrutinise and approve an annual budget. The budget should include prudent income forecasts that the Directors have confidence that there is a reasonable expectation of securing the funding planned for.

Financial Reporting

Up-to-date financial reports should be discussed by the Directors regularly. Directors should discuss:

- 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

Cash

- Cash is kept 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

The account is to be reconciled at least monthly.

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 Directors. The list of people with access and their access levels are to be reviewed annually, as part of the audit preparation process.

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.

Unrestricted funds - are to be recorded separately to ensure these are accounted for.

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.

Expenditure

Delegation of Authority

Each budget line should have a specific nominated Director who has the authority to approve expenditure against that budget. Expenditure may not be authorised beyond the limit of the delegated budget without appropriate approval by another Director.

This may be sub delegated, subject to appropriate approval by line management. However, responsibility for all expenditure remains with the budget holder and, before delegating authority, he or she is to ensure that the individual to whom a delegation is made is issued with any necessary instructions and is competent.

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 verbally agreed by another Director and clearly specify budget lines and limits.

The authorising Director 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 (e.g. VAT) excluded if appropriate, before authorising payment.

Each invoice to be checked by two Directors 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 company 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.
- 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.

Pay and Remuneration

Pay is the single biggest cost and, therefore, particular safeguards need to be put in place.

- Any proposals to increase staffing are to be submitted to the Directors
- The payroll schedule should be checked and signed each month by the responsible Director. For example, to check any changes have been authorised, the rates used are correct, and issues such as staff being paid twice or for amounts or items that would not be expected.

Ensure that:

- A leave record system is in place and is properly up-to-date and maintained.
- A monitoring system for sick leave is in place and any excessive absences managed accordingly.
- Pay and personnel records are kept separate.

Payment Procedures

Payments systems, such as, debit cards and on-line systems and passwords should be adequately safeguarded. Passwords should not be written down (unless electronically and password-protected) 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.

Novel and Contentious Expenditure

This is defined as follows:

- **Novel** - does not meet the letter of 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 another Director.

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.

In general, the minimum value for an item to be treated as a capital asset is £100

- 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 or bribery is suspected, it is to be brought to the attention of a Director.

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 a Director.

Records

- Records are to be retained safely and securely. Records are retained for 7 years.
- 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

- 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.

Approval and Review

This policy will be reviewed by the Directors annually, as part of the financial planning cycle.

Version No	Approved By	Approval Date	Main Changes	Review Period
1.0	Directors	July 2024	Initial draft approved	Annually
2.0	Directors	September 2025	Updated in line with best practise	Annually