BAYSTON HILL
PARISH COUNCIL

Add-on Financial Policies and Procedures

Supplier Account Set Up and Change Procedures

Contents

1. Supplier Account Set Up

1.1 Supplier details

To open up a new supplier account the following information must be obtained –

Full trading name
Address, including postcode
Telephone number
E-mail address (for remittance advice notes to be sent to)

1.2 Supplier payment details

Ideally all supplier payments should be made by BACS rather than cheque.

Bank details required are -

Name of account
Bank address
Sort code
Account Number

All bank details must be received in writing by post on company headed paper signed by an appropriate person.

Once received, and before these details are used to make any payment, they must be verified by making a telephone call to the supplier. Do not use the telephone number sent with the bank details, if there is one, without checking it is genuine against an invoice, their website and/or the telephone directory. Always ask to check the details with the accounts department. They are to give you the details to verify to the letter. Never read back the details from the letter. Get the name of the person you speak to and record this information.

Further checks, such as personal ID, may be required depending on what is received.

If these verification checks cannot be made before payment is due then the supplier should be paid by cheque until verification is complete.

2. Changes to Supplier Details

2.1 Changes to supplier details

This procedure aims to minimise the potential for Mandate Fraud (see section 3).

If anyone contacts you by telephone, e-mail or letter to change any supplier details always telephone the accounts department back to confirm the change. Be wary if it is to change the telephone number and particularly cautious if it is to change bank details.

2.2 Changes to bank details

Follow the same procedures as in section 1.2 by only accepting changes in writing and then verifying the changes by telephoning the accounts department of the supplier. Do not make any changes or payments into this new bank account until full verification has been made and these have been signed off by the Finance Manager.

2.3 Keep notes

Make notes of all telephone conversations including names of who you have spoken to. Keep all of these notes together with the original letter/e-mail received giving details of the bank change for 7 years.

2.4 Supplier review

A periodic review of suppliers should be undertaken to identify and remove any old/dormant accounts from list of payees on Internet Banking. This reduces the likelihood of any old supplier information being used to secure fraudulent payments.

3. Mandate Fraud

3.1 Mandate Fraud

(from https://www.met.police.uk/advice/advice-and-information/fa/fraud/business-fraud/mandate-and-cheque-fraud/)

Mandate Fraud is also known as Creditor Fraud, Payment Diversion Fraud and Supplier Account Takeover Fraud.

Changing bank accounts is an unusual occurrence and therefore any request to update records should be treated with suspicion. Changes should be authorised at a senior level.

This fraud involves the changing of account details for supplier or customer accounts in order to gain control of an account and benefit from unauthorised payments. This could include changing of bank details in a direct debit, manipulation of credit card activity, or changing of an employee's bank account details for their salary, particularly when a bonus is due.

Fraudsters rely on the Payee (Company) name not being checked by the Banks. In most cases, only the Sort Code and Account Number are checked by the receiving bank.

Additionally, company details, including signatures on published accounts, are copied from the internet.

All companies and organisations are urged to ensure that they have robust authorisation and monitoring procedures in place for the creation and changing of bank details and monitoring of payments.

This also applies when providing account details on order to set up new payments or amend them.

Requests may be received by phone, letter or email to update account details. These requests must be monitored, checked and authorised before changes are made.

3.2 Details of suppliers are obtained from :

- Inside knowledge, including corrupt staff acting fraudulently.
- Publicly announced contracts.
- On-line transparency of contracts, particularly public sector contracts.
- Internet research about the targeted organisation, their activities and identifying key staff.
- Social Engineering to gain information from unsuspecting employees, this may include telephoning companies to gain information about their procedures.

3.3 The approach is made by :

- Telephone: there may be some urgency or reason to get changes made in a hurry: this is an indication of a potential fraud.
- A written request (letter or fax): this may be on ‘official’ looking letterhead quoting publicly available information such as company registration and director details.
- An email request: using information and logo’s that look legitimate and have a reply email address that is ‘spoofed’ to give the impression that it is legitimate.

3.4 In all cases

All the information presented may be correct, including directors, key contract staff, and signatories, having been collated and checked against different sources. They may be routed directly or in such a way that they appear to be from another part of the organisation, even if apparently authorised by a senior manager, the request should be thoroughly checked.

3.5 Recommendations

- All staff should be wary of providing sensitive company information, by phone or other means, especially contract and account information including references.
- Establish with suppliers, and internally, points of contact for handling and changing sensitive information that may benefit fraudsters.
- Call-back your supplier using records in your system (not on the letter) to check the veracity of the request.

- Get a confirmatory email from the expected corporate email address.
- Make a note of your enquiries; be willing to double check information.
- Other policies may need review – clear desk, information security, staff vetting, internal and external financial controls.
- Do not publish account details and signatories on yearly reports.

3.6 Further checks that may be considered

- Enquiries to verify the new payee account details. With most types of bank transfer, only the Sort Code and Account number are verified, not the account holder's name.
- When contacting companies, do not automatically use the information provided on suspicious letters, faxes and email. Check this against contract documentation, payment records and other information. Contact the accounts department direct and not the name on the letter.
- Internet checks may highlight discrepancies and previous attempts. However, fraudsters may create incorrect records on the web, including business directory entries and web sites, in order to mislead.
- Check the details on any request doe change – company numbers, VAT registration, contact details, web and email information.
- Companies House information should be treated with caution. It is only a register and there are significant problems with details being changed in order to divert goods and payments.
- If making contact by phone, do this via main switchboards. Telephone calls may be re-directed, email addresses and incoming phone numbers are easily changed to look like legitimate ones.