Mandate Fraud Policy

Date adopted: 18th May 2017 Next review date: May 2018

Rev Level	Revision Date	Description of Changes
01 02	27/03/2012 18/05/2017	• Initial Release • No changes

Prepared:	Approved:	Released:
	David Sword 18th May 2017	David Sword
Signature	Signature	Signature
Electronic copies valid without signature		

Chair's signature: David Sword 18th May 2017

1 Introduction

Ormiston Academies Trust (OAT) processes a significant number of payments via internet Banking systems. The purpose of this document is to provide clear guidance to employees on the handling requests from the groups supplier base to change banking information for making such payments. In applying the policy, all individuals must have due regard to the best interests of the Organisation

2 Objectives

The objectives of the OAT Policy are:
To ensure all requests for change are valid
To ensure supplier banking details are validated and up to date

3 Scope

The Policies and Procedures apply to all employees of OAT.
Criminals are using increasingly sophisticated means of committing fraud so we all need to be aware and not take correspondence and telephone calls at face value unless you are satisfied that the source is genuine.

Telephone calls requesting information relating to payments due/remittances

If you receive a telephone call requesting details of payments to be made to a supplier or requesting details or copies of remittance advices you should ask them to provide the following details for security

1. Details of invoice numbers in query
2. The value of the invoices
3. The purchase orders that the invoices relate to
4. The date the last payment was made to them and its value.

You should then advise the caller that you will call them back, obtain a name and telephone number.

You should then telephone **the contact number held on our system** to respond to the enquiry. Do not respond directly to email requests without verifying that it is from a genuine contact.

Where you have a regular contact person at a supplier who you know is genuine you can respond without undergoing these checks.

If you receive any suspicious calls or correspondence do not respond immediately. Refer any such calls/correspondence to the Business Director to decide what action should be taken.

Telephone calls requesting information relating to payments due/remittances

When a request is received to amend Bank Account Details on our system it should be passed to the Business Director in the first instance.

The account should be changed immediately to payment by cheque until all security checks are completed.

A letter should be sent to the address held on our system notifying the supplier that a request had been made to change bank details, that if the request was not made by them to contact us immediately, that a face-to face meeting with a known contact will be required before bank details will be changed and that payments will be made by cheque until our security checks are complete (This letter may be supplemented by either an email/telephone call to a **known** contact if this is felt appropriate to maintain Supplier Relationships).

Security checks

1. Check the original request.

    a. If the request is made by telephone make a note of the telephone number, time and date shown on the telephone display. Ask the caller for the following information:
        i. Their name
        ii. Their Job Title
        iii. Company name
        iv. Telephone number
        v. Request written confirmation of details by email/letter or fax
        vi. Open the suppliers file on Open (Payables/Enquiries/Supplier Enquiry) Click on supplier account and then click on Notes icon and enter details of time and date of call and information provided by caller. At the end of the note put your name and date.
        vii. Go to Supplier Maintenance and amend payment type from BACS to Cheque.

    b. Written requests or confirmation in writing as per (1.a.v.) above
        i. Carefully check details on the document. Check that address, telephone number, email format (make sure that company name is spelled exactly the same as email on system) agrees to information already held on the system. Check that letterheads are exactly the same as copy invoices already scanned to system. Often suppliers show their bank details on invoices for BACS payments, this is also a useful double check if you are suspicious
        ii. Check details of person requesting the change. (This can be done by looking up the company website, checking with colleagues e.g. do they have correct job title, is signature the same as any previous correspondence, ring the company and ask receptionist to confirm if they have a person by that name working there and what their job title is etc.)
        iii. Contact the company by telephone and arrange a face to face meeting (this should preferably be with someone who is known to a staff member of the Association) to confirm the bank details.
        iv. Details of the meeting should be made in writing and any documentary evidence copied and signed by colleague.
        v. All documentary evidence should then be passed to either (nominated individual) to authorise changes to be made on the finance system.
        vi. Once approved Supplier Master Details should be amended. Details of changes printed off and signed by person making changes. The changes should be reviewed and countersigned by a Manager.

Exception reporting

Exception reports should be run periodically to identify all changes made to supplier details during the period by the Business Director. The report should be checked against the evidence file maintained in support of change requests, in order to confirm that appropriate documentation has been retained in each instance, and that the checks undertaken prior to the implementation of each change have been in line with procedures.