Orbis Internal Audit- Schools Bulletin

Fraud & Financial Irregularity – Autumn 2019

Background

The issues highlighted in our bulletins have come from our interaction with schools, either through school audits or where we have been contacted to provide advice. They are produced jointly by the Orbis Internal Audit partnership incorporating Surrey County Council, East Sussex County Council and Brighton and Hove City Council.

If you missed any of the previous bulletins these can be found here.

Objective

The objective of these bulletins is designed to assist School Governors in meeting their core strategic functions as set out in the Governance Handbook published by the Department for Education.

- Ensuring clarity of vision, ethos and strategic direction;
- Holding executive leaders to account for the educational performance of the organisation and its pupils, and the performance management of staff; and
- Overseeing the financial performance of the organisation and making sure its money is well spent.

Whilst we will generally focus on the last of these strategic functions, advice and guidance will also cover the other two strategic functions. The Governance Handbook states that asking the right questions is equally important in relation to money as it is to educational performance.

Fraud

Schools are as vulnerable to fraud and financial irregularity as other public bodies. Examples of fraud or financial irregularity may include collusion with external contractors or agencies, misappropriation of funds or theft.

Fraud can be defined as 'a deliberate act which can involve deception and/or concealment and is intended to cause detriment to another or give an unfair or illegal advantage to the perpetrator or others'. Generally speaking, fraud can be broadly categorised into two forms, internal and external. Internal Fraud is committed by someone connected to the school. This may be an employee, but can be anyone who has access to the financial systems or assets. External fraud involves an outside party attempting to extract money from a school.

Where fraud is committed internally it can be particularly distressing. Fraudsters are often a valued trusted member of the school community. This is often why normal expected financial controls are overlooked or weakened. Any financial loss from fraud or financial irregularity is likely to have a direct impact on funds available to support pupil's education.

The Audit Commissions report 'Protecting the Public Purse' (2014) suggested that in the year

2013/14 there were 206 detected cases of fraud in LA maintained schools, worth £2.33 million, with an average value of £11,313. Over half of cases (54%) and almost 2/3 of the value (62%) involved fraud by staff. In 2017/18 it was estimated that the figure had risen to £2.8m for detected loss. As these were detected cases, the true value is likely to be much higher.

Schools may also be vulnerable to other members of their school community, such as pupils and volunteers (including governors), who are tempted to financially benefit from their relationship with the school. Financial loss from voluntary and community funds is fairly common in addition to the main school budget.

Governors have a duty to be aware of potential risks and how they can be minimised.

External Fraud

As well as ensuring there are robust controls in place internally to minimise the risk of fraud, Governors and all school staff should be aware of several types of external fraud that have been increasing in recent times.

Social Engineering:
Social engineering refers to psychological manipulation of people into performing actions or divulging confidential information. It is often one of many steps in a more complex fraud scheme. Social engineering is a booming crime category because cybercriminals understand that it's easier to deceive a person than a machine. Human beings are still the gatekeepers of valuable data. Bank accounts, file storage, credit card details; they are all protected by passwords and those passwords can be obtained with deception. Fraudsters may use information found on personal social media accounts to gain trust.

Phishing:
Phishing describes a type of social engineering attack where attackers influence users to do 'the wrong thing', such as disclosing information or clicking a bad link. Phishing can be conducted via a text message, social media, by phone or by email. Phishing is commonly used for theft of information and installation of malware (including ransomware). It could also be the first step in a targeted attack against the school, where the aim could be something much more specific, like the theft of sensitive data or an attempt to obtain money by deception.

Spear Phishing:
Phishing attempts directed at specific individuals or companies have been termed spear phishing. In contrast to bulk phishing, spear phishing attackers often gather and use personal information about their target to increase their probability of success. Scammers may impersonate one of your colleagues or managers and it is not always easy to spot these attempts. This may lead you to click on links, accept software updates or open attachments via email, social media messages or electronic popup messages. In doing so, you could unwittingly compromise sensitive information, provide access to organisational finances or facilitate technical attacks on our network.

A large number of local schools were recently subject to a targeted spear phishing attempt, which saw an attacker target multiple School Business Managers/Bursars by email asking for payment to be made against an overdue invoice. These emails appeared to come from the Headteacher of each school, as the names of officers are routinely published on school websites. In some cases financial loss was only just averted following lengthy email conversations with the attacker. If you

are not expecting the email, it's right to be suspicious!

We have also seen an increase in fraudulent emails, requesting a change to bank details. The latest example appeared to be sent by a member of staff to the Business Manager advising that they had changed their bank account for salary payments. It was subsequently identified that the e-mail address was bogus and had been "spoofed" so it looked like the employee's genuine address. In recent months these frauds have become more sophisticated and fraudsters often gain personal information from social media to make the e-mails seem more believable. It is strongly advised that when a supplier or member of staff advises of a change to their bank account that they are contacted by telephone using independent contact details to confirm the request. Further advice can be sought from Internal Audit or your finance contact.

The following link gives some general guidance of phishing and spear phishing: https://www.youtube.com/watch?v=ygON2B9-xTw

In summary:

- Are you expecting the email?
- Think before you click
- Verify the communication is genuine without replying
- Seek advice

Suspicion of Fraud or Financial Irregularity

If you suspect a fraud or a financial irregularity:

DON'T
• do anything which alerts the suspect(s).
• carry out any form of investigation.
• do anything which may prejudice a subsequent disciplinary hearing and/or police investigation.

DO
• contact Internal Audit.
• treat the matter as urgent.
• if it is safe to do so, secure all the relevant records and other evidence.
• make a written note of all the facts that you are aware of, together with dates and time where applicable.

Questions for Governors?

Governors have a duty to be aware of potential risks and how they can be minimised. Poor financial controls increase the risk of fraudulent activity and make it easier for fraudsters to operate. Early detection means that any financial loss can be minimised. Below are some questions for governors to consider and they may want to seek assurance from the Headteacher and School Business Manager that robust controls are in place.

Do governors and staff know what to do if they suspect a fraud or theft has been committed?

Do governors and staff know how to identify potentially fraudulent external communication and how to protect the school?

Has the whistleblowing policy been reviewed and are staff aware of it and able to easily access a

copy? This improves the likelihood of fraudulent or inappropriate activity being reported.

Are all declarations of interest up to date and complete? Where a conflict does exist how is this managed by the school? This helps identify potential conflicts, such as links to suppliers, other staff or governors, and ensures they are considered and appropriately managed before they influence decision making.

Is there a regular review of detailed budget monitoring reports and are significant variances queried?

Voluntary (school) funds are particularly vulnerable to theft or inappropriate use, how often do governors review these accounts? This Improves scrutiny and challenge over use of school funds and may identify issues and minimise loss. Voluntary funds are also required to be audited annually.

Are asset/equipment registers maintained and regularly reviewed? School equipment, particularly ICT, is vulnerable to theft.

Are there robust financial procedures in place for the receipt of income and processing of payments made by the school and are these followed? These would include the following:

- Bank reconciliations are completed monthly and any unexpected payments investigated.
- Purchase orders are raised and approved in advance of ordering goods, works and services. This helps staff to challenge demands for payment or bogus invoices.
- Segregation of duties exists in financial processes. It is harder to commit fraud or behave inappropriately if there is more than one person involved.
- At least two people are involved in the receipt, reconciliation and banking of cash.
- Use of purchasing cards is monitored and reviewed regularly. They are particularly vulnerable to fraud or theft and there are many examples where the card has been used by other staff, as the card was made available to others or details of the card have been shared.
- Individual pay claims are checked for accuracy before approval by a line manager. This includes reimbursement for staff expenses, claims for additional hours or other pay increases.
- Payroll is reconciled monthly, variances are investigated and it is signed off by the Headteacher.

Key Contacts and Further Advice

Georgia Steers, Senior Auditor, Orbis Internal Audit & Counter Fraud
☎ 01273 294578 ✉ Georgia.Steers@brighton-hove.gov.uk
Carolyn Sheehan, Principal Auditor, Orbis Internal Audit & Counter Fraud
☎ 01273 291319 ✉ Carolyn.Sheehan@brighton-hove.gov.uk

To Report Fraudulent Activity

Brighton & Hove City Council ☎ 01273 291700, ✉ anti-fraud@brighton-hove.gov.uk
East Sussex County Council ☎ 01273 481995, ✉ confidentialreporting@eastsussex.gov.uk
Surrey County Council ☎ 03456 009009, ✉ internal.audit@surreycc.gov.uk