South Gloucestershire Council 05 July 2019

Schools Counter Fraud and Data Protection Bulletin

Issue No. 46

Introduction

Preventing fraud is everybody's business. If you suspect fraud please contact your Head Teacher/ Manager without delay and notify internal audit for more advice. The Council has a dedicated email address for reporting suspected fraud: AuditFraud@southglos.gov.uk

The Council's fraud response plan advises you to contact internal audit who will advise and may undertake an investigation (if necessary). Your contacts in Internal Audit are:

Justine.Poulton@southglos.gov.uk – Audit Manager – 01454 865443

Justine.Lawson@southglos.gov.uk – Group Auditor 01454 865439

This bulletin provides you with information on the latest examples of fraud and some ideas of how to prevent you and your organisation from being the next victim. For the purposes of this bulletin, fraud is considered to cover a number of terms: including (but not limited to) bribery, corruption, mandate fraud, phishing, vishing and ransomware, see the glossary at the end of this document for more information.

In this issue

Changes to the Schools Financial Value Standard for 2019/20

Internal audit services are responsible for collecting all Schools Financial Value Standard documents by 31st March each year. The format of the form has significantly changed for 2019/20 and more information is required than previously. In particular, a number of the questions have changed and data is now requested as part of the return.

Do ensure that your School takes a look at the return in plenty of time before next year's deadline. The form may take a little longer to complete than previously. The Schools Financial Value Standard is a national requirement and all queries should be directed to the contact details contained on the .gov.uk website.

The required documents are located on the .gov.uk website, internal audit do not hold templates. This is to ensure that schools always use the most current version available.

New Financial Regulations for Schools

Thank you to all schools who have provided comments and feedback on the consultation for the refreshed financial regulations for schools. The Financial Regulations for Schools were approved by Schools Forum and should now be used by all Local Authority Maintained Schools. Copies of the financial regulations have been circulated to all schools by the Children, Adults and Health Department and awareness raising events were organised and well attended for June 2019.

Police Scotland warn of rise in teens targeted as money mules

Police Scotland has written to secondary schools across the country warning parents and teachers that criminal gangs are targeting teenagers to act as "money mules", as a senior officer warned youngsters are increasingly recruited online to move the proceeds of fraud through their own bank accounts. Children are being targeted online but also vulnerable to approaches at youth clubs, sports centres and outside schools. Adverts on Facebook and other social networking sites, as well as group invitations on Whatsapp, promised "easy money" and "investment opportunities", tricking young people into believing they are becoming involved in a legitimate financial occupation.

How to protect young people from this practice

Mules will often be asked to buy watches, computers, telephones, ipads, anything that can be sold on for a specific value. As well as alerting parents to keep a lookout for young people making unusually large transactions, the Police also warned parents to be alert to changes in purchasing behaviour. Young people should be suspicious of activities that appear too good to be true.

Purchase Card Fraud

A recent audit of purchase cards identified a new scam for would-be fraudsters. There are many ways a fraudster can obtain your purchase card details. This could be by a scammer emailing speculatively to warn you of a fraud on your account or they pose as your card issuer and ask for personal information. Once the link is pressed and information provided, the card details are extracted and used. Commonly, recent purchase have been online subscriptions such as Spotify, Now TV and Amazon Prime Membership. As the monthly amounts are relatively small they are not necessarily spotted straight away.

How to protect yourself and your organisation

To prevent the risk of this type of fraud, ensure:

- You independently check that your card issuer has contacted you, use a trusted contact to confirm request for information
- Purchase card statements are regularly and promptly checked to ensure all purchases are recognised and legitimate
- Pay special attention to regular subscriptions, make sure you know what Amazon purchases relate to, keep more detailed information for companies that are regularly used.

Almost two thirds of data breaches are a direct result of human error

A recent study has found that 89 percent of surveyed UK organisations have experienced a data breach, and human error is still the prevailing cause. A lack of security for remote/mobile working is also a main cause.

How to protect yourself and your organisation

Organisations will never completely eliminate human error associated with data breach risks. Risks can be reduced through ensuring there are sound checking and oversight processes. Here are some common measures which might help reduce the risk of human error:

-Take care with email address and written correspondence to ensure the ultimate recipient is correct.

-Remind staff to take care with papers that contain sensitive data, avoid taking them off the premises and do not transport with laptops which might be attractive to thieves.

-Think before you print, do you need a printed copy? Are you located near to the printer and able to collect your materials promptly? Who else has access to the printer?

-If necessary redact information to avoid sharing too much data.

World Pay Scam Risk

World Pay merchant services lets you take card payments securely on line, over the phone or using card machines. Where payments are accepted electronically, a charge will be levied by the provider. These charges need to be monitored as does the transactions on the bank account.

A case was identified, where numerous transactions for small amounts were made (less than £2) , followed by a large transaction for £3,800, which resulted in the bank account becoming overdrawn. Fraudsters will follow this pattern for a small number of test transactions followed by a major purchase when ‘scamming a card’.

It was only when the account became overdrawn and the bank requested that funds be transferred into the bank account to bring it back into credit that it was realised that the bank account in question had been subject to fraudulent activity.

How to protect yourself and your organisation

All bank accounts should to be reconciled to bank statements in a timely manner to ensure that no fraudulent transactions appear on the account. If any are identified, then you should contact your bank immediately and notify Internal Audit so that we may inform other Schools.

Glossary of terms

Fraud – The intentional distortion of financial statement and accounting records and/or misappropriation of assets involving deception.
Bribery – The offering, giving, receiving, or soliciting of something of value for the purpose of influencing the actions taken by the audited body, its members or officers.
Corruption – The offering, giving, soliciting or acceptance of an inducement or reward that may influence the actions taken by the audited body, its members or officers.
Ransomware – This is a form of malware that attacks your computer, locking you out and demanding payment in the form of a “fine” or “ransom” to have it unlocked.
Phishing – An attempt to obtain sensitive information such as usernames, passwords, and credit card details (and indirectly, money), often for malicious reasons, by illegally impersonating a trustworthy entity via an email.
Vishing – the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers.
Port-Out Fraud – The act of porting a victim’s telephone number to a new SIM card under the fraudster’s control and then using the number to access the victim’s bank accounts.