

## **Purpose of this Bulletin**

When reading this bulletin, employees should consider the following questions: “Could it happen to me?” and “Will the internal procedures in operation under my control stop this type of fraud being successful?”

All officers should consider whether there is fraud taking place and how this can be stopped.

## **How do we guard against fraud and corruption?**

The annual internal audit plan has been developed to help the Council assess and take action to minimise the risks it faces.

Fraud & Corruption is one section of the audit plan and testing is undertaken on specific areas of identified risks.

However, it is the responsibility of managers to operate internal systems to ensure:

- An adequate separation of duties
- Proper authorisation procedures
- Independent monitoring and checking of data and documentation

## **What do we mean by fraud and corruption?**

**Fraud** - The intentional distortion of financial statements and accounting records and/ or misappropriation of assets involving deception.

**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.

Frauds come in all shapes and sizes. Many are successful as a result of the breakdown in internal control procedures in operation within the organisation. Another reason is that people do not believe it will happen to them.

## **Fraud Prevention Strategy's**

The Anti-Fraud and Corruption policies of our clients can be found on their respective websites.

**Contact Us** - Our intention is to produce this bulletin twice a year at least. We would be grateful for any information that you may have that could be included in these bulletins or for any feedback you may have on its content. For more information please [contact us](#).

## **Benefit Claimant fails to disclose £150,000 inheritance**

A London welfare cheat hid a £150,000 inheritance windfall while fraudulently claiming £6,500 in housing and council tax benefits. Carole Darling has become the 15th person to be successfully prosecuted for fraud by Richmond Council in 2013, after an anonymous tip-off alerted its internal audit and investigation team.

The 65-year-old's case brought the total amount the council's fraud team has identified in fraudulent benefit payments since April to £190,757 - breaking down to £145,410 in housing benefit and £45,346 in council tax benefit.

Darling will return to Richmond Magistrates' Court for sentencing after pleading guilty to one charge of failure to notify a change in circumstance.

The council's deputy leader, Cllr Geoffrey Samuel, said: "The real penalty is for these people to be named and shamed in their local newspaper so the community will never forget their cowardice and utter contempt for Richmond's taxpayers and our most financially vulnerable residents."

**This successful prosecution highlights the importance of having well advertised methods for the public to refer possible frauds to the council, which can be either by telephone or e-mail, with any successful prosecutions being reported in the local press as a deterrent to others.**

## **Abuse of Position-Driving Licence Points Scam**

A court clerk has been found guilty of helping motorists falsify their driving records and escape bans in return for cash payments. David Kelly, 47, of Liverpool, ran the scam from his office at Liverpool Magistrates' Court, a jury heard.

Preston Crown Court was told motorists would pay for driving offences to be deleted from their licences. Kelly was found guilty of conspiracy to pervert the course of justice.

Three other people were found guilty of conspiracy to pervert the course of justice and fraud after arranging to have points removed from their own driving licences.

Kelly, who worked as an administrator for Liverpool Magistrates' Court for 20 years, applied to the Driver and Vehicle Licensing Agency (DVLA) for points to be removed from the licences of more than 70 people between 2004 and 2010.

Fingerprint evidence and a handwriting expert proved that Mr Kelly wrote and submitted numerous documents to the DVLA to request that points be removed from the licences. Computer evidence showed that he then checked the progress of these requests on the computer system, which was linked with the DVLA.

**Internal control procedures within the DVLA identified a cause for concern which were subsequently investigated and resulted in the above prosecution. Local authorities need to**

**be aware to the possibility of staff in regulatory roles being approached to falsify information in return for what effectively is a bribe..**

### **Attempted Change of Bank Account Frauds**

Notifications continue to be received from suppliers notifying their clients (including local authorities) that they have no intention of changing their bank and that if they receive any communication by post, e-mail or telephone, they should contact the company immediately.

The fraudulent correspondence notifying of the change of bank account details sent have included contact names and signatures of current employees of the companies concerned which add to the authenticity of the request.

**All staff need to be aware of the possibility of fraud when they receive any request for a change in suppliers' bank account details and contact them, via the contact details already in their possession to verify the authenticity of the request before processing it.**

### **Leisure Chief Jailed for Embezzlement**

Tom Leighton, 48, earned £62,000 a year as Falkirk Council's Head of Leisure Services, and ran the annual Big In Falkirk pop festival. But he carefully siphoned off more than £27,000 from the festival and other budgets, and used his mother-in-law and a former work colleague to channel the cash back to his bank account.

Jailing Leighton for a year, Sheriff William Gallacher told him no sentence other than custody was appropriate. He had considered a 15 month sentence, but reduced it to 12 months because Leighton pled guilty.

Sheriff Gallacher told Leighton, that responsibility should have come with his job. Leighton has repaid some of the money and has made arrangements to repay the rest. The sheriff said: "I have to deal with this as a very gross breach of trust." Falkirk Sheriff Court heard that while organising Big In Falkirk, Leighton could authorise payments for services provided by third parties.

But Kirsten Cockburn, prosecuting, said his line manager, Maureen Campbell, became suspicious when a payment was made to a Mrs Gardiner in Galashiels. Mrs Campbell wondered why he should be paying anyone there, and also knew that Leighton lived in Selkirk. She contacted Mrs Gardiner to find she was Leighton's mother-in-law.

The depute fiscal said that in another instance, a payment of £6000 was made to a Mrs Brown, who had been a colleague of Leighton's when he was in a former job at Borders Council.

This prompted an internal audit at Falkirk and various other payments came to light. It emerged Leighton's former colleague had transferred the money to Leighton as he requested, but when quizzed by police claimed "she didn't know she was doing anything illegal". She said she could not give a reason other than that "she was stupid".

Police officers then questioned Leighton's mother-in-law about £4000 she received and transferred back to him. Mrs Gardiner said her daughter had asked her to transfer money due from Falkirk Council. Leighton's wife Nicola told police she was "unaware of any criminality involving her husband".

Leighton, of Selkirk, admitted embezzling £27,152 from the council between October 2006 and May 2009. He had initially been accused of stealing £75,578, but the figure was reduced by the prosecution. He also admitted attempting to embezzle £16,000 - reduced from £17,675 - between July 2007 and May 2009.

After leaving Falkirk Council, Leighton took a senior leisure job at Horsham District Council in Sussex, which he held for two years before being sacked. Leighton has since returned £13,000 to Falkirk Council and has also left his pension with the authority as repayment of the rest.

**This former senior officer abused his position of trust relying on his staff not questioning the expenditure incurred in respect of the Pop festival he had organised.**

**Internal control procedures should not be abused by senior officers and staff should, as in this case be prepared to raise any concerns they may have with regards the appropriateness of expenditure they are being asked to authorise/ process.**

**Where staff do not feel able to raise these concerns within their department, they should raise them through the Whistle blowing procedure in operation within the council, which should be regularly brought to the attention of staff.**

## **National Fraud Initiative-Case Studies**

### Case Study 1 – Immigration

Information provided in an NFI data match to expired UK visas led to the dismissal of a council employee who had no right to stay or work in the UK. The employee had worked for the council since 2005 and was employed as a mobile cleaning services assistant. They had originally started working at the council from an employment agency.

The council contacted the employee to ask them to provide evidence of their right to work in the UK. The employee then absconded from work, did not reply to any communication and failed to attend two interviews.

The council informed the Home Office that the employee had absconded. Officers were then able to intercept and arrest the employee boarding a ferry to Northern Ireland.

The employee was charged with perverting the cause of justice. They also admitted using a false identity in the past. They are currently being held in prison while the Home Office takes steps to seek to remove them from the UK.

The employee was dismissed with immediate effect and their pension frozen with a view to recovering some of the salary overpayments.

**Managers need to ensure the necessary pre-employment checks are undertaken to ensure the successful applicant has a right to work in the UK and any incorrect appointment does not result in a fine being levied on the council by the Home Office.**

**Contract procedures should be in place to ensure staff initially appointed via an agency contract comply with these requirements, prior to taking up any engagement within a local authority.**

#### Case Study 2 – Housing Tenancy Fraud

An NFI housing tenancy data match led to the conviction of a tenant for unlawfully subletting a council house in Wolverhampton to her adult children, while also renting another property in Harrow, North London.

Investigation of the match revealed that the tenant was first assessed to be homeless by Harrow Council in 1997. She was placed on the housing waiting list and housed in temporary accommodation. Unbeknown to Harrow, she also registered as homeless in Wolverhampton in 2005, and was given a tenancy in October 2005.

She did not inform Harrow and continued to be placed in temporary accommodation until she was granted a tenancy in 2006. She continued to visit Wolverhampton to mislead housing officers that she was living there.

She admitted to having two tenancies and was given a nine-month suspended sentence for obtaining services by deception. She was also suspended from her public sector job. The keys to the property in Wolverhampton have now been handed back and Harrow Council is taking civil action to evict her from their property.

**Council staff are expected to act with honesty and integrity and this tenancy fraud was breach of the trust place in the employee by the public and a breach of the employee code of conduct.**

**As a result of this deception, during the period of the illegal subletting, the local authority would have been paying for a family to be in temporary accommodation while they waited for a suitable property to become vacant.**

**As illegal sub-letting is now a criminal offence, residents should be made aware of the implications if they are found to be illegally subletting their council accommodation.**

#### Case Study 3 – City of London Blue Badges

The investigation of a match between blue badges and deceased people records identified an individual who had fraudulently obtained disabled parking permits from the corporation.

He had completed renewal application forms under his mother's name, even though she had died almost a year before.

He admitted two charges of fraud by false representation. He was given a two-year conditional discharge, and ordered to contribute £300 towards prosecution costs.

**This fraud, while not always done for financial gain results in benefits being obtained to which the fraudster is not entitled and can cause traffic concerns if used inappropriately.**

#### Case Study 4 – Civil Service Pension Scheme to Deceased Data

As a result of an NFI pensions to deceased person's data match in the 2008/09 NFI exercise, the Civil Service Pension Scheme identified a pensioner who had died in January 2007.

Upon investigation, it was found that the scheme had not been informed of the death but had been contacted in June 2007 to amend bank account details and divert the pension payment into a different bank account.

This was actioned after all the appropriate security checks had been completed. As a direct result of the match the pension was suspended and the case forwarded to the police for investigation. The total overpayment equated to £6,300

**This fraud is an example of why regular checks need to be made on a regular basis to ensure that payments are being made to the people who are entitled to them and do not continue without verification.**

### **Subletting tenants in London return keys**

More than 40 housing association tenants who had been subletting their London properties have returned their keys as part of an amnesty.

Peabody Housing Association gave its 55,000 tenants two months from October to voluntarily return the keys or face legal action. A spokesman said the keys to 45 properties had been returned and then re-let to those on the waiting list. No families were removed from the sub-let properties, the housing association added.

Legislative changes mean subletting, or tenancy fraud, can carry a two-year prison sentence and a £50,000 fine. The properties recovered were predominately in the boroughs of Lambeth, Westminster, Hammersmith and Fulham and Kensington and Chelsea.

Joe Joseph, from Peabody, said "People who breach their tenancy agreements by illegally subletting can expect a knock at the door and to face legal action."

**This exercise is an example of the action that can be taken against illegal subletting as local authorities work with their Housing Association colleagues; to reduce tenancy fraud and their Temporary Accommodation bill in respect of those families accepted as homeless**

under the Housing Act 1996 as amended by the Homeless Act 2002 by reducing the time spent in temporary accommodation.

### **Sheffield care home deputy manager admits £15,000 fraud**

A deputy care home manager is facing a possible prison sentence after she admitted defrauding 25 residents out of almost £15,000. Denise Nichols, of Kiveton Lane, Rotherham, admitted taking £14,646.84 from residents at the Wensley Street Care Home in Sheffield.

The 55-year-old pleaded guilty to one count of fraud by abuse of position between 2008 and 2013. She was bailed ahead of sentencing at Sheffield Crown Court on 12 February. The fraud was uncovered after an audit in September 2013.

Wensley Street Care Home, which is owned by South Yorkshire Housing Association, provides care and accommodation for up to 30 people with learning disabilities, according to the latest Quality Care Quality Commission report.

Kevan Taylor, chief executive of Sheffield Health and Social Care NHS Foundation Trust, which provides staff to the care home, said the fraud came to light following a review. He said "financial irregularities were identified and a thorough investigation has taken place. The Trust has worked closely with the Police and South Yorkshire Housing Association throughout and, as a result of the investigation; a member of Trust staff has been dismissed."

**Robust procedures need to be in place to safeguard the personal finances of residents to ensure the governance arrangements are appropriate with built in controls to review the expenditure incurred by the residents who finances are administered by their carers..**

### **Election expenses fraud**

A former councillor says he has no intention of seeking re-election or returning to public politics after admitting to fraud charges. Alex MacLeod was Highland Council's youngest member when he was elected in May 2012 at the age of 19.

His legal team has entered guilty pleas at Inverness Sheriff Court to charges relating to his election expenses. He has pleaded guilty to knowingly incurring more election expenses than he was allowed, and declaring false expenses to council officials. MacLeod also admitted to altering invoices for print work and submitting these to local authority officials.

**This fraud is an example of why internal control procedures are necessary within local authorities to ensure that 'claimants' are only paid/ reimbursed monies to which they are entitled. This applies to all claimants irrespective of their position and is one of the reasons the Fraud Act includes a crime of abuse of position.**

## **A4E welfare to work fraud investigation continues**

A total of 13 people have now been charged over allegations of fraud at the welfare to work company Action 4 Employment (A4E) as a result of a Police investigation which commenced in May 2011.

This company was contracted by the DWP to deliver their 'Inspire to Aspire' employment and training scheme to motivate and to assist people to find employment. Under the terms of the contract, the DWP paid out when the scheme successfully found jobs for individuals.

The new charges relate to allegations against A4E contract manager Ines Cano-Urbe, quality co-ordinator Sarah Hawkins, operations manager Serge Wyett, team leader Matthew Hannigan Train and recruiter Hayley Wilson.

They are accused of having "conspired to forge documentation in relation to services provided by A4e, with the intention of convincing Department for Work and Pensions auditors that the documentation and claims for payment were genuine", the Crown Prosecution Service said.

They face a total of 60 charges including conspiracy to defraud, multiple counts of forgery and making and possessing articles for use in fraud.

**This fraud is an example of the lengths some companies will go to provide evidence in support of the payment being requested in respect of the contract they have been commissioned to undertake.**

**Officers should always be aware of the possibility that they are being presented with forged documentation when reviewing evidence in support of payments being requested.**

## **Benefit overpayments and Right to buy applications**

A council's crackdown on welfare crooks has identified nearly £300,000 in overpayments to corrupt benefit claimants. The London Borough of Richmond Upon Thames' investigations have unearthed £271,000 in overpayments in housing benefit and previously paid council tax benefits between April and September.

The council's shared internal audit and investigations service has received 157 benefit fraud referrals and taken action against 24 housing and council tax benefit cheats. The local authority secured government funding to work with the borough's housing teams and housing associations to investigate social housing fraud, with the money invested to fund a housing intelligence officer and three in-house housing fraud investigators.

The team has recovered seven properties, has six pending recovery, and has seen eight temporary housing properties vacated. Four right to buy applications were also withdrawn with a further three pending withdrawal. With the discount offered on a right to buy purchase set at £100,000 per property, the effort has saved the council a notional £400,000.

**This fraud is an example of the number of bogus Right to Buy applications submitted by 'tenants' and the savings that can be achieved by authorities who recover properties that would otherwise go into private ownership instead of for the use of those in need.**

## **Police to probe Lancashire County Council Finances**

In November 2013 the BBC reported that the police were investigating allegations of financial irregularity at Lancashire County Council. The authority has referred the conduct of a senior officer who was the focus of a recent disciplinary investigation to police after taking legal advice. It is probing the tendering process of a £5m fleet contract and the authorisation of a £500,000 payment to a senior officer.

A Lancashire County Council (LCC) spokesman said: "In the light of external legal advice, a number of issues arising from the recent disciplinary investigation into the conduct of a senior officer have now been referred to Lancashire Constabulary.

The allegations appear to stem from the decision to create One Connect Ltd (OCL), a joint venture between the council and BT to run some services. In particular, concern has focused around the decision to award a contract to OCL to run the county council's fleet of vehicles, a contract cancelled by the incoming Labour administration.

Another issue is the payment of more than £500,000 in bonuses to the former chief executive of OCL, David McElhinney, who remains in charge of a similar venture between BT and Liverpool City Council.

Mr Halsall has always denied doing anything wrong and his supporters believe the complaints are politically motivated. Geoff Driver, the Conservative Leader at the time, believes there should be an inquiry to prove nothing untoward took place.

He had been suspended on full pay in August pending the outcome of a disciplinary investigation into the tendering of the fleet vehicle contract. The deal to run the council's fleet services was agreed in April by the former Conservative administration which was led by Geoff Driver.

It was awarded to BT but the decision was called in by county councillors and put on hold. The council's in-house provider continued to provide the services. The contract was revoked on 15 August with immediate effect by current LCC leader Labour councillor Jennifer Mein.

It was awarded to BT and One Connect Ltd, a partnership between BT and the council LCC is also conducting a separate investigation into the authorisation of the payment of more than £500,000 to David McElhinney who resigned in August. He received two separate payments that Ms Mein and the council treasurer said they were unaware of. Mr McElhinney ran One Connect Ltd, which was contracted to run various council services.

**This case is an example of why all decisions taken in respect of the awarding of contracts should be taken following the completion of the tendering process with an audit trail being in place to evidence the decisions taken, on what basis and by whom.**

**All payments made should be in accordance with the authorities' financial regulations and large payments over pre-determined amounts should require authorisation by more than one officer; with the required authorisation level increasing as the amount of the payment to be made increases.**

## **Trading Standard Scams**

The following warnings have been issued by Trading Standards into various bogus and criminal activities in recent months.

Businesses being offered counterfeit goods as they seek to reduce operational costs and increase their profits. Recent examples are power tools, and garage diagnostic software which create health and safety concerns

Bogus officials who cold call elderly residents either by telephone or on the door step whose aim is to get the residents to hand over large amounts of money. The latest incident reported related to bogus Trading Standard officers. All officials carry identity cards and should not be allowed into homes unless it is by prior appointment and at the request of the resident.

As local authorities introduce restrictions on the disposal of waste and the introduction of charging, the fraudsters have now moved into this area, targeting residents who have had building work undertaken. The caller (con-artist) claiming to be from Trading Standards attempts to extort money from them over the inappropriate dumping of contaminated waste, demanding immediate payment of the fines levied.

A resident agrees to have work undertaken by a cold caller, such as window cleaning or grass cutting for which he is paid for. A couple of months later they return late at night demanding additional payment, claiming to have undertaken similar work when the resident was not at home. This additional work was not agreed in advance and often has not been undertaken.

A resident received telephone calls from someone claiming to be the head a Trading Standards Department. The caller claimed to be working with the courts advised the resident that he had to pay almost £10,000 in relation to the court case in respect of a tradesman the resident used previously who had been detained and his assets seized. Even if a resident makes a complaint against a contractor, the victim will never be asked for a contribution towards the cost of prosecution.

Every year distraction burglaries occur across the country, where unexpected callers offer their services to check properties for damage as a result of ice or snow, or to clear gardens, driveways or gutters of debris such as leaves or snow, request payment and when they gain access into the residents home, commit the burglary, especially if more than one person undertakes the work.

## **Electronic Tagging Services Overpayment**

Overcharging allegations in July 2013 resulted in a cross- government review of contracts held by Serco and G4S which have been widely publicised. This resulted in a repayment of £68.5 M by Serco.

**Internal control procedures should be in place within all local authorities to ensure that contracts which pay by results in respect of services commission, previously provided by local authority staff are actually being undertaken as detailed in the invoices received for payment. Payments should not be authorised until the relevant support information has been provided by the contractor.**

## **Abuse of Position and Fraud**

A former employee of Kent County Council pleaded guilty and was recently convicted of four counts of fraud by abuse of position and one count of theft in the sum of £8,000.

An allegation was made in December 2012 in relation to money donated to Swale Borough Council's sports development department.

**Internal Control procedures should be in place to ensure that all grant monies paid and received are used for the reason they were given or received.**

## **Information Governance Breaches**

The following reportable cases have been published by the Information Commissioner's Office since the issue of the last Fraud and Data Protection bulletin in September.

### **Unencrypted Memory Device**

A monetary penalty notice for £80,000 was served on North East Lincolnshire Council after the loss of an unencrypted memory device containing personal data and sensitive personal data relating to 286 children on the 29th October 2013 for the loss which occurred in July 2011.

The unencrypted memory device had been issued in 2005 in order for the teacher to access necessary data to visit schools. In 2011 the Information Security policy which was introduced in March 2011 stated that all memory devices must be encrypted, however the unencrypted devices were not immediately recalled.

The unencrypted memory stick was left in the Council offices overnight still plugged into a laptop and when the teacher returned the next day it was gone.

**Where memory sticks are used by staff, it should be ensured they are encrypted and not left unsecure overnight to avoid the risk of theft. Where unencrypted memory sticks have been previously issued to staff, they should be replaced.**

Ministry of Justice

On the 15th October 2103 a monetary penalty notice for £140,000 was served on the Ministry of Justice for failing to keep personal data securely, after spreadsheets showing prisoners' details were e-mailed to members of the public in error.

On the 2nd August 2011 a member of the public reported to the data controller that he had received by email the previous day, details of inmates at Cardiff Prison.

Although he was the intended recipient, a file containing the details of 1,182 inmates had accidentally been attached to the e-mail.

The initial investigation showed there had been two previous instances of the same error on the 4th and 11th July 2011 where the prisoner details had been sent to a different individual on each occasion, which were unauthorised disclosures by the same clerk who had recently been employed.

The attached file contained personal and sensitive information which identified each inmate, their complete personal details, including their crime, location and when they were due to be released.

The clerk had received induction and specific training on the booking system and was shadowed before being allowed to work on her own.

**This incident is an example of how easy it is to send personal and sensitive information over the internet to the wrong person or to include information to which they are not entitled and should not be disclosed.**

**Procedures should be in place to ensure that checks are undertaken prior to the sending of these e-mails to ensure they are being sent to the correct person(s) and any attachments do not include information to which they are not entitled.**

Jala Transport Limited

On the 26th September 2013 a monetary penalty notice was served on Jala Transport, a small money-lending business, after the theft of an unencrypted portable hard drive containing its customer database from the data controller (owners car) while he was stationary in traffic in on the 3rd August 2012.

The owner of the company took the external hard drive home each night for business continuity purposes and to reduce the risk of theft or damage as it contained the only copy of the customer database which contained personal and sensitive information in respect of his 250 clients.

**The data controller should have taken reasonable precautions in the safeguarding of the information held on the external hard drive, which would have included, encrypting the external hard drive and placing the external hard drive out of sight in the boot of his car.**

## Fraud Bulletin January 2014



**All staff should be aware of the possibility of theft or loss of personal or sensitive information that they have in their possession and take reasonable steps to protect it at all times.**

Aberdeen City Council

A monetary penalty notice was served on Aberdeen City Council on the 27th August 2013 after inadequate home working arrangements led to 39 pages of personal data being uploaded onto the internet by a Council employee.

Between 8th and 14th November 2011 an employee working at home on her own computer inadvertently uploaded four documents which related to her work, which contained sensitive personal children's data on to a website on the internet.

At the time of the incident there was no relevant home working policy in place for staff to adhere to despite the fact that all staff were allowed to access work material from home.

A Tele-working policy did exist which addressed the Health & Safety aspects of home working demonstrated the Council's awareness that home working was necessary, but no consideration was given to what impact this might have on data security.

This incident did not come to light until 3 months later when an Aberdeen Council employee put their own name into an internet search engine and when he scrolled down the search results he noticed reference to a Care Group meeting, which when he clicked on the link made him realise that sensitive information had been posted on the internet.

The resulting investigation revealed that the personal computer used by the employee had been purchased second hand and that it contained a programme that automatically loaded files onto a website.

**This incident happened because an employee was allowed to work at home on her own computer, without adequate safeguards being put in place to safeguard the information being accessed or transferred over the internet, rather than a computer provided by the council.**

Royal Borough of Windsor & Maidenhead

In January 2013, 257 records containing personal data was posted on the council's intranet site in error. A spreadsheet containing details of individuals who had not signed a new employment contract was wrongly appended to a review document for general access on the intranet, rather than being added separately as a restricted item.

The ICO investigation revealed that data protection and information security training for those with access to personal data had not been mandatory and that the policies on handling personal data were incomplete.

**Management procedures should be in place to ensure that Data Protection and Information Security training is undertaken by all staff; records maintained of when the training was undertaken; compliance with Information Governance policies should be subject to monitoring and enforcement.**

Luton Borough Council

In December 2012 and January 2013, separate incidents occurred which involved the incorrect handling of personal data, including information on health and ethnicity by social work staff.

In the first case an email containing personal information about a family was sent across an unsecured internet connection and also sent to an agency unconnected to the family.

In the second case papers were lost in an accident when a member of staff took them home when leaving work early due to severe weather.

**These two incidents highlight how easy it is to breach the Data Protection Act when employees' duties involve the handling of personal and sensitive information collected as employees undertake the work which they are employed to do.**

**Care needs to be taken at all times when transferring personal and sensitive information to third parties and when it is being taken out of a secure environment.**

## **Bradford Kings Science Academy Inquiry**

A head teacher has been arrested and bailed in connection with suspected fraud at a free school in Bradford as part of an investigation into the city's Kings Science Academy.

It comes after the Department for Education (DfE) last year said it had found serious failings with the school's financial management. The academy, one of England's first free schools, opened in September 2011.

The DfE investigated the school after a whistle-blower made allegations about its governance, and found nearly £80,000 of public money had not been used for "its intended purpose". A DfE spokeswoman said it acted "as soon as it received allegations of wrongdoing" and referred the case to the police.

**Governance procedures should be in operation at all schools to ensure all expenditure is appropriate and used for its intended purpose. Governors should play a key role in this, especially as the Chair is required to sign confirming the annual Financial Value Standard Self-Assessment has taken place and an action plan is in place as required.**

## Phishing and scam e-mails continue

If it is too good to be true, then it probably is. Unsolicited e-mails continue to be received in various guises in an attempt to get the recipient to respond. If you do not have a bank account with the organisation concerned or do not know the person who has sent you the e-mail you should delete it, unopened.

Requests for help/ assistance are made in the hope that the reader will believe the story being told, and if they have been able to gather personal information about you from the internet, they will use this knowledge with the aim of making their story more convincing.

Cases have been reported when these e-mails have been followed up by telephone calls in the hope of generating a successful response.

Schools are reminded that in order to minimise the risk of viruses entering computer systems, staff should not open any e-mails or attachments from unknown sources, or click directly on any internet links, without being 100% sure of the site's authenticity.

**If you respond you jeopardise the security of your computer and could result in the loss of personal, sensitive and financial information.**

## Cold Callers and Placing of Advertisements

The majority of these cold callers or unsolicited telephone calls normally get no further than the reception/ office at a school; however isolated cases do get through.

Staff need to be aware of the approved purchasing procedures in operation at the school where they work and not to purchase anything where the school has not instigated the enquiry.

In the case of the placing of advertisements this should be at the instigation of the school and any publications should have a proved track record with regards meeting the intended audience.

Staff should never let themselves be pressurised into making a quick decision where the incurring of expenditure is incurred and they should discuss and proposed purchase with colleagues before placing the order.

## Purchasing Card fraud

We have been advised that an organisation has recently been the target of fraudulent transactions in respect of its' purchasing cards.

One of the cards initially had some small payment transactions which led up to a much larger fraudulent payment being drawn.

**It is recommended that card statements are regularly reconciled and appropriate security guidance is issued to staff when purchasing cards are distributed. It is also recommended,**

wherever possible, that card credit limits should be restricted in order to minimise any potential losses.

**Schools need to ensure that they have robust policies and procedures relating to the purchase of goods and services and undertake comprehensive and timely reconciliations of all bank accounts.**

## **Fraud by Impersonation**

A university has identified that fraudulent emails purporting to be from some of their Purchasing/Procurement Managers have been sent to various external suppliers.

It appears that as part of the fraudulent activity the fraudsters attempted to open up credit accounts on behalf of the university and in doing so used the university's logo and the name of one of their Procurement Officers on Purchase Orders.

Emails were sent from an 'ac.co.uk' domain which had no connection to the university. These emails were grammatically poor, used false telephone numbers and had a delivery address in East London.

**Schools need to be aware of this type of fraud if they receive invoices for goods which appear to have been ordered by the school which you have no knowledge of.**

## **Unsolicited Invoices**

Before any invoice is considered for payment, the school should satisfy itself that it relates to an approved purchase order made by the school before the invoice is checked and approved for payment.

Any invoice which appears to have originated from a foreign country should be treated with suspicion. In recent months invoices appear to have been sent from the Czech Republic and the United States of America.

## **Debt Collection fraud**

A number of organisations have received correspondence from Garner Bruce Legal Services in connection with debts claimed to be owed for the supply of goods and services by Powwow Water Company Limited. An example of the wording etc of the correspondence is detailed below:

*"Powwow Account No. 200132288*

*Customer Reference: 44372*

*Total Amount Outstanding: £1915.1623*

*Dear Sir,*

## Fraud Bulletin January 2014



*Garner Bruce Legal Services have been instructed as agents in the recovery of the debt owed by your company for the supply of goods and services by Powwow Water Company Limited on the following account.*

*Under the Late Payment of Commercial Debts (Interest) Act 1998 we are entitled to charge interest calculated at 8% above the base per annum and continuing at a daily rate until the outstanding balance is paid in full plus penalty costs of £40.00 per invoice. We have levied a charge of 25% on the outstanding balance of each account which is included in the account balance detailed above.*

*Given that the most recent invoice is over three years old this is considerably below the amount which we are entitled to charge.*

*This debt is due and payable now.*

*Please remit within 7 days of this email to our account at Santander Bank, Sort Code 09-01-27, account no. 08311186. Should you require us to produce a summary of the account this will be done at a charge of £40.00.*

*There is a standard charge for reproduction of invoices of £100.00. This charge includes 5 invoices with any additional invoices being charged at £20.00 each.*

*Failure to remit within 7 days will result in a court action being raised immediately to recover the full amount of the debt, all expenses, charges, interest and legal costs without further recourse to you.*

*The amount sought will therefore be considerably more than the amount stated above.”*

With regard to the above, a statement has been received from Deloitte advising that Garner Bruce Legal Services are not appointed agents of the Joint Administrators of Powwow Water Company Limited. The Joint Administrators actually appointed Wild About Water (UK) Ltd to collect any debts.

**Schools should not be pressurised to pay debts which they have not incurred because of spiralling charges and the threat of legal action if the debt is not settled promptly.**