FEBRUARY 2025

AUDIT YORKSHIRE

COUNTER FRAUD NEWSLETTER

Welcome to our Counter Fraud Newsletter. We hope you find the contents helpful. As always, if you need any fraud advice please reach out to your Local Counter Fraud Specialist.

How to Play Your Part

As we move through 2025, we want to thank NHS staff for their continued support in helping to tackle fraud across all our organisations. Your commitment to reporting concerns and suggesting improvements plays a vital role in safeguarding resources and ensuring they are directed where they are needed most—towards patient care and vital services.

Fraud not only costs the NHS millions every year, but it also undermines trust and impacts the services we all rely on. By reaching out to our Counter Fraud Service you help us detect and prevent fraud, whilst strengthening processes to protect the NHS against future fraud risks. Every report matters, no matter how small it may seem.

Fraud prevention is a collective responsibility. Staying alert and speaking up about potential issues contributes to a culture of transparency and integrity across the NHS. If you have the slightest suspicion of an occurrence of fraud or have ideas for improving procedures, we encourage you to contact your Local Counter Fraud Specialist.

You can also sign up to learn more about different types of NHS fraud by accessing our Fraud Prevention Masterclasses, or receive this newsletter direct to your inbox by emailing yhs-tr.counterfraudyork@nhs.net.

Thank you for playing your part in keeping the NHS safe and secure. Together, we can build a system that is resilient and focused on what matters most—delivering excellent care to patients.

Winter Fuel Payment Scam

Whilst Spring is on the horizon, we're still making our way through the winter months. Fraudsters are continuing to send out texts and emails claiming to be from the UK government, claiming that you need to apply for a winter fuel payment, heating subsidy or cold weather payment. Some of these messages say that the payment relates to recent snowy weather.

The messages contain a link to a fake version of the GOV.UK website which asks for the person's personal and financial details. These phishing sites tend to mimic GOV.UK branding which can make them harder to spot.

The government does pay a winter fuel payment to some people who were born before the 23rd of September 1958. You can check if you are eligible for this payment on the official GOV.UK website: https://www.gov.uk/winter-fuel-payment/how-to-claim

PayPal Invoice Scam

Which? are warning of a PayPal invoice scam which is doing the rounds. Fraudsters are taking advantage the ability to raise invoices / payment requests using PayPal.

The fraudster creates a payment request using the official PayPal platform. They add a phone number and write on the invoice that the recipient can call if they do not recognise the request. The invoice is sent to the target from an official PayPal email address, making the request look more authentic.

People who receive these requests may panic, and call the number on the invoice to try and understand why they've been sent a bill they were not expecting. Their call goes directly to the fraudster, who then asks for personal and financial information.

Some previous examples of this scam have included fraudsters posing as HMRC. They sent out PayPal payment requests for "overdue taxes" and threatened that if the recipient did not respond within 48 hours, a warrant would be issued for their arrest.

If you receive an unexpected request for money via PayPal, do not click any links or call any numbers that are contained within the email.

Instead, log into your PayPal account, go to "Payment Requests" and cancel the fraudulent request. You can also get in touch with their customer services team using the official PayPal website, and can forward the dodgy email to phishing@paypal.com.

TikTok Job Offer Scam

There have been reports in the news recently about people receiving text messages from scammers who are posing as TikTok recruiters. The texts are advertising jobs where for £300 - £800 a day, all you have to do is watch and 'like' videos which are on the TikTok platform.

People who have been victim of this scam state that they have had to undertake training then have had to pay an upfront fee in cryptocurrency before they could do any 'work'. These payments started out to be small, and the 'employees' did see it returned plus a commission. This made them feel confident enough to start paying larger fees. Once a significant sum had been paid, the scammers disappeared, along with the money.

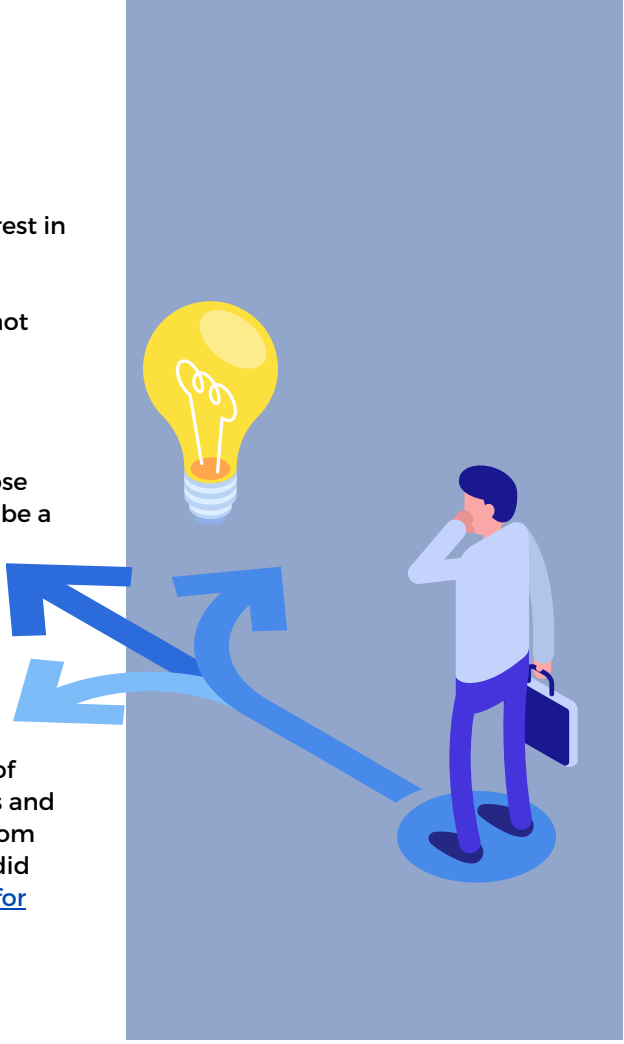
To avoid this scam:

- Be wary of any unsolicited offers of work, especially ones which pay highly for easy tasks.
- Research companies offering work and verify with them independently.
- If you have to pay to earn – especially in cryptocurrency – it's probably a scam.

You can read more about this scam on the Guardian website: Rise in Scam Job Offers (www.theguardian.com)

A Conflicts of Interest Update and Reminder

NHS England have recently revised their Managing Conflicts of Interest in the NHS guidance which is applicable to all staff in Integrated Care Boards (ICBs) and NHS Trusts. Other organisations, such as social enterprises, are encouraged to use this or similar guidance but are not compelled to do so.



What is a conflict of interest?

If a staff member or decision maker in the NHS has a personal or close interest which could clash with their professional duties, there may be a conflict of interest.

The NHS spends around £190 billion of taxpayer's money and so it is important to make sure that decisions about spending are made honestly and fairly.

Let's say for example that a member of staff has a business outside of their NHS work. This business supplies locks and fittings. As part of their NHS role, they are responsible for sourcing the best value locks and fittings. It could be tempting for the staff member to get supplies from their own company and pocketing the profit. It was tempting, and did happen. Read more about it here - Locksmith Andrew Taylor jailed for £600,000 NHS fraud - BBC News

What you must do:

- Any interests must be declared as soon as they arise.
- Ask yourself whether any interests you have could affect the way in which taxpayers' money is spent. If the answer is yes, or you're not sure, declare.

We encourage you to read the full NHS England guidance here - Managing conflicts of interest in the NHS

Gifts and Hospitality

In the NHS, being open and transparent is essential—especially when it comes to gifts and hospitality. While receiving a small thank-you gift may seem harmless, accepting certain gifts or hospitality could create a conflict of interest or give the wrong impression.

What Are the Rules?
Each NHS organisation has its own policies, so it's essential to check your employer's guidance. You might find details in a dedicated Gifts and Hospitality Policy, or your organisation may cover this topic in a Conflicts of Interest Policy, or Standards of Business Conduct Policy. If you're not sure which policy your organisation uses, please do reach out to your Local Counter Fraud Specialist who will be happy to assist.

Why Does This Matter?
Following the correct procedures helps maintain public trust in the NHS. If you're unsure, always refer to your employer's policies or check with your local counter fraud team. When in doubt, it's safer to say no!

Get a Refresher
For a quick reminder of what Gifts and Hospitality might look like and what you need to do, please watch our 2 minute video which you can access using the button below.

The video doesn't have any sound, so you don't need to worry if you don't have access to headphones or speakers.

Click the button to watch our 2 minute video refresher on Gifts and Hospitality.

WATCH NOW

REPORTING FRAUD CONCERNS

Fraud vs the NHS

If you think that fraud may be being carried out against the NHS, please **notify your Local Counter Fraud Specialist**. You'll find our contact details on the next page.

You can also report your concerns to the **NHS Counter Fraud Authority** using their online reporting tool or phone number. You'll find these details on the next page.

If you choose to make an anonymous report, please give as much information as possible as we won't be able to get back in touch with you to clarify anything.

Suspicious Emails

Do not click on any links or attachments.

If you have received a suspicious email to your **@nhs.net** email account, you can forward it (as an attachment) to **spamreports@nhs.net**

If you are not sure how to forward an email as an attachment, contact the LCFS team and we will help you.

If you have been sent a suspicious email to another type of email account (not @nhs.net) you can forward it to **report@phishing.gov.uk**

Suspicious texts

Do not click on any links in the suspicious text message.

You can forward suspect text messages to 7726.

Fraud against a member of the public

These concerns can be reported to **Action Fraud (0300 123 20 40),**

If the person has lost money, it may also be appropriate to report the matter to **the police.**

If you suspect that the person's bank account has been compromised, it is important that they **speak to their bank** as a matter of urgency.

I've read the options but I'm still not sure what to do

The Local Counter Fraud team will be happy to advise.

Our contact details are on the next page.