NHS Greater Glasgow and Clyde

Core brief

Daily update
(18 September 2023, 12.45pm)

Topics in this Core Brief:

- Your pension - New Pension Contribution Rates
- Cyber Crime: Recognising the signs
- Removal of peak time rail fares

Your pension - New Pension Contribution Rates

We have received notification of new NHS pension contribution rates from 1 October 2023 - Scottish NHS Circular 2023/11

The main change is that the percentage contribution which members pay will be based on actual pensionable pay, rather than whole time equivalent salary. Around 40 per cent of members work part-time, and so most of those members will see a reduction in their contribution rates. However, other members will see an increase in their contribution rate. Member pension contributions are paid before tax, and so therefore reduce taxable pay.

The table below explains the new contribution rates for each salary range from 1 October 2023.

Pensionable earnings in 2022/23	Applicable contribution percentage rate from 1 October 2023
Up to £13,330	5.7%
£13,331 to £23,819	6.1%
£23,820 to £28,186	6.7%
£28,187 to £35,364	8.2%
£35,365 to £35,521	9.8%
£35,522 to £37,086	10.0%
£37,087 to £45,079	10.5%
£45,080 to £48,784	10.8%
£48,785 to £68,222	11.3%
£68,223 and above	13.7%

An SPPA consultation on the proposed changes ran from 23 May to 15 August 2023. Click here to read the outcome from the consultation.

Cyber Crime: Recognising the signs

Cyber-crime and the Threat Actors who deploy it, continue to use ever more elaborate ways of stealing both your personal and your organisations information. It's easy to assume the messages arriving via Microsoft Teams are legitimate, however, this is becoming a more frequent form of attack in the wider Public Sector.

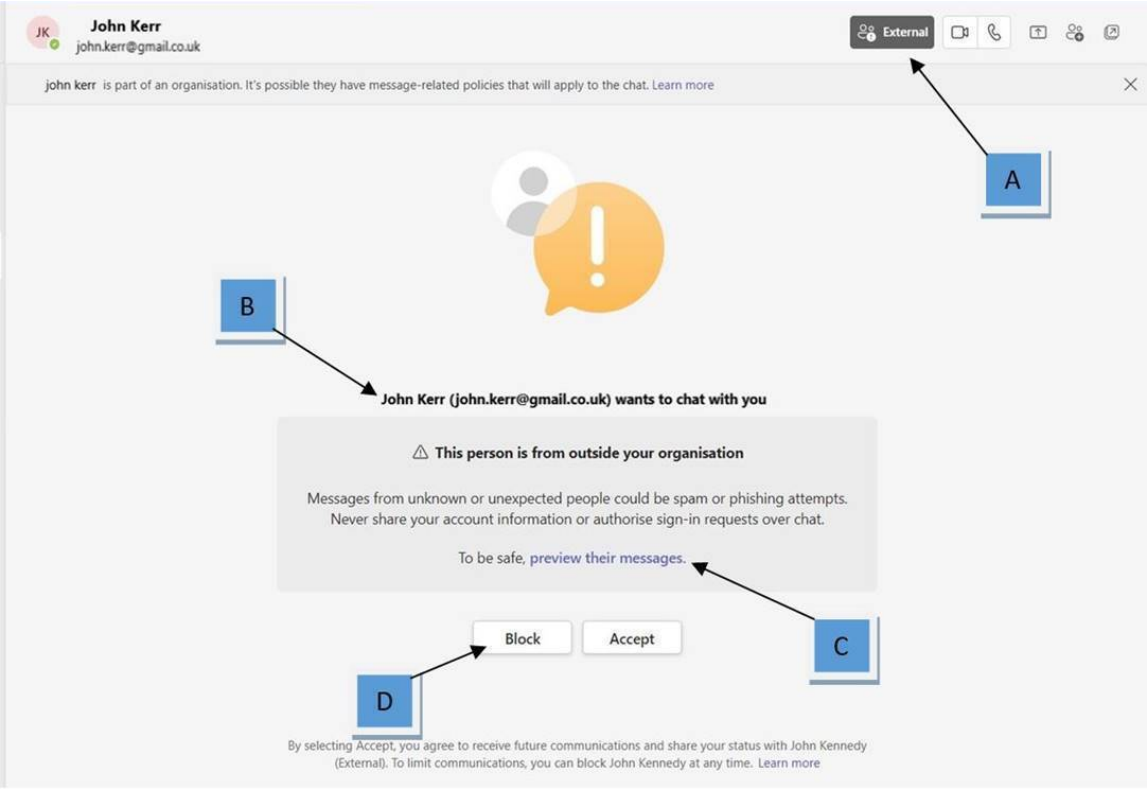
What is Microsoft Teams Phishing?

This is similar to other forms of Phishing undertaken by threat actors but specifically targets organisations and individuals through the use of the Microsoft Teams platform.

What to look out for

Beware of **external invite requests** on MS Teams, threat actors may be impersonating genuine staff or trusted external contacts. The attacker would request to chat with you on teams and once accepted may encourage you to open a malicious attachment, click a suspicious link, or provide sensitive information.

Below is an image of what an external invite will look like on teams:



1. Look for the **External** Markers, this indicates the request is coming from outside the organisation. It may well be named as a genuine member of staff but it will show as external as indicated at points **A** and **B** of the diagram.

2. Click on **preview messages** as shown in point **C** of the diagram to view content safely **without** accepting the invite.

3. Do not accept external invites on Teams without prior verification. Click **block** as shown in point **D** if you believe the communication not to be genuine.

Reporting suspicious content
It's important to remember never to click on any links or accept any external MS Teams requests which look even remotely suspicious.

If you suspect you have received any suspicious teams request you can report it to: **itsecurity@ggc.scot.nhs.uk**.

Removal of peak time rail fares

The Scottish Government is funding a trial to allow ScotRail to remove peak time fares from 2 October 2023 – 31 March 2024. This will mean far cheaper travel options for those who need to travel at peak times. More information is available from ScotRail. Information on active & sustainable travel options is available from the Travel Plan Office.

Remember, for all your latest news stories, visit our new Staffnet Hub:
GGC-Staffnet Hub - Home (sharepoint.com)

Staff are reminded to make sure their personal contact details are up to date on eESS.

It is important to share Core Brief with colleagues who do not have access to a computer.
A full archive of printable PDFs are available on website