NHS Greater Glasgow and Clyde

Core brief

Daily update
(13 July 2023, 11.00am)

Topics in this Core Brief:

- iMatter 2023 – every voice matters
- The Health and Care (Scotland) (Staffing) Act 2019 Guidance Chapter Webinars
- Cyber Crime: Recognising the signs

iMatter 2023 – every voice matters

Thank you to everyone who has taken the time to complete the iMatter survey in 2023. The questionnaire stage in all Cohorts is now complete, and we received almost 27,000 responses which is fantastic.

The most important bit of iMatter is the discussion you now have in your team based on that feedback. This is your chance to discuss and agree as a team how you want to work together to make things better.

You have eight weeks from receiving your report to meet to discuss your feedback, agree actions and put these into the iMatter system. You can see the timelines here (and below). To help you with those discussions, we have provided refreshed action planning information and guides available on HR Connect. Please contact the iMatter team with any questions.

Our full iMatter Board report will be available during week commencing 17 July, when we'll take the opportunity to review, identifying positive themes and areas for improvement to align with our Workforce Strategy actions.

NHSGGC response rate currently 54% (awaiting final paper copy input)		
Cohort One	**Cohort Two**	**Cohort Three**
Action Planning deadlines*:		
Fully electronic 01/08/23 **Paper & electronic: 14/08/23**	**Fully electronic 08/08/23** **Paper & electronic: 21/08/23**	**Fully electronic 22/08/23** **Paper & electronic: 04/09/23**

Please note that the action planning dates will be reflective of the response methods used within the Directorate/HSCP, therefore please check HR Connect for more information.

The Health and Care (Scotland) (Staffing) Act 2019 Guidance Chapter Webinars

The Corporate Healthcare Staffing Team are supporting NHSGGC with the preparation of the enactment of the Health and Care (Staffing) (Scotland) Act 2019, and facilitating support for staff to keep up to date with the steps we need to take to implement the Act.

Four webinars have been created and facilitated by Health Improvement Scotland and Scottish Government colleagues to provide an opportunity for you to get informed and prepared for Enactment in April 2024.

All four can be accessed via the following links.

Guidance Chapter Webinar and Topic	Links to Webinar Recordings	Additional Resources
Guidance Chapter Webinar 1 This webinar will cover the guiding principles, the duty to ensure appropriate staffing, agency reporting, commissioning in healthcare and reporting.	01. HCSA Webinar 1 - Guiding Principles and ensuring appropriate Staffing.url	20230601 Legislation Webinar 1 Presentation v4.0.pdf
Guidance Chapter Webinar 2 This webinar will cover risk escalation, real-time staffing assessment, clinical leadership and advice, training, staff consultation and reporting	01. HCSA Webinar 2 - Real-time staffing, risk, clinical leadership and advice.url	20230615 Legislation Webinar 2 Presentation FINAL v3.0.pdf
Guidance Chapter Webinar 3 This webinar will cover the Common Staffing Method and the role of Healthcare Improvement Scotland's	01. HCSA Webinar 3 - The CSM and the role of HIS.url	20230622 Legislation Webinar 3 Presentation v1.0.pdf

monitoring and compliance duties.		
Guidance Chapter Webinar 4 This webinar will cover the role of the Care Inspectorate, care service providers and commissioning and reporting for care services.	01. HCSA Webinar 4 - care services .url	20230629 Legislation Webinar 4 CI Resource Links v1.0.pdf 20230629 Legislation Webinar 4 Presentation v2.0.pdf

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. Here we look at one of the most widely used means used by scammers – Phishing.

What is Phishing?

Phishing is a form of social engineering where a scammer impersonates a well-known figure or organisation, most commonly via email, to defraud the target into forwarding sensitive information. Some common goals of a phishing attack are:

- get access into your network
- inject malware
- gain access to confidential information
- transfer money or anything of value.

What can I do?

It's easy to assume the messages arriving in your inbox or calls you receive are legitimate, but be wary - phishing emails often look safe and genuine. To avoid being fooled, slow down and examine hyperlinks and senders' email addresses for clues such as spelling mistakes, especially before clicking on any reply in the body of the message.

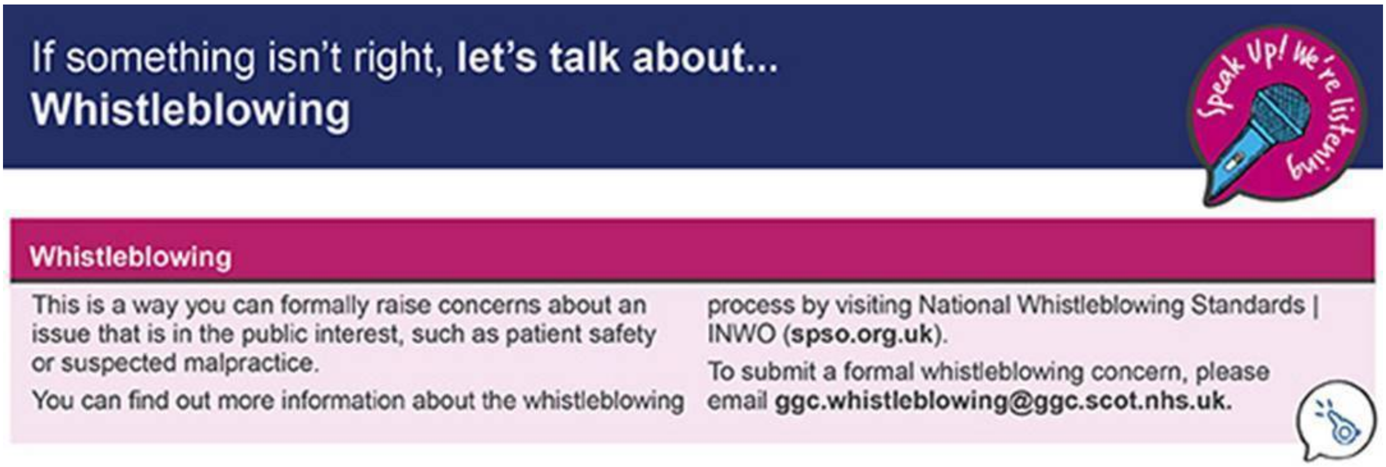
Top Things to look out for:

- Emails with bad grammar and spelling mistakes
- Emails with an unfamiliar greeting or salutation
- Inconsistencies in email addresses, links & domain names
- Suspicious attachments
- Emails or calls requesting **login credentials**, **payment information** or **sensitive data**.

Reporting suspicious content
It's important to remember never to click on any links or open any emails which look even remotely suspicious.

If you suspect you have received anything to your work email address containing malicious content you can report it to: spam@ggc.scot.nhs.uk.

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



If something isn't right, **let's talk about...**
Whistleblowing

Speak Up! We're listening

Whistleblowing

This is a way you can formally raise concerns about an issue that is in the public interest, such as patient safety or suspected malpractice.

You can find out more information about the whistleblowing process by visiting National Whistleblowing Standards | INWO (**spso.org.uk**).

To submit a formal whistleblowing concern, please email **ggc.whistleblowing@ggc.scot.nhs.uk.**

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