NHS Greater Glasgow and Clyde

Core brief

Daily update
(6 May 2025, 1.50pm)

Topics in this Core Brief:

- FairWarning – Appropriate access to clinical records
- Ligature and self-harm
- May 2025 – Digital Skills and Literacy: eHealth drop-in sessions and floor walking

FairWarning – Appropriate access to clinical records

The Board has a moral and legal responsibility to protect the confidentiality of the data it holds and patients expect the information we retain about them will be kept secure and confidential. Your job role may give you access to patients' clinical information and it is essential that you are aware of your responsibility to access only the information that is required to allow you to carry out your legitimate duties.

To protect against inappropriate access to records, NHSGGC continues to use an audit system called FairWarning which was put in place to provide assurance that clinical information is kept safe. The system provides the Information Governance Team with daily audit reports from clinical systems which allows them to monitor and investigate any potential inappropriate access to records, including staff accessing their own records and those of family members. If, after investigation, a record is found to be accessed inappropriately, then a formal discussion between the member of staff and manager will take place and depending on the severity of the breach, there could be a number of consequences including refresher training and/or formal disciplinary action. Some good practice tips are:

1. Never share system passwords with other colleagues or managers
2. Keep your LearnPro Safe Information Handling Training up to date learnPro NHS - Login (learnprouk.com)
3. Be familiar with the FairWarning guidelines, visit: Information Governance Guidance & FAQ's.

Staff are reminded that if they wish to access their own health information, they should not view their own clinical records but should submit a subject access request. The Subject Access Policy provides the relevant information and forms needed and can be found at: Information Governance Policies & Privacy Notices.

If you have any questions on FairWarning or data protection in general, including training, please visit our Information Governance Knowledge Hub: Information Governance Knowledge Hub or contact the Information Governance Team at: ggc.data.protection@nhs.scot.

Ligature and self-harm

The Health and Safety Executive has previously prosecuted NHSGGC and continues to take enforcement action across the NHS and other health and social care providers in relation to the management of ligature and self-harm risk.

Make Safety Personal

In order to provide a safe environment for our patients and comply with our legal responsibilities, departments across NHSGGC should have an up-to-date assessment for the risk of suicide and self-harm.

Control measures within a risk assessment should detail appropriate actions to be taken to remove or manage identified high risk ligature points and other self-harm risks within your department. Control measures may also include:

- Self-Harm Control Checklist (Environmental)
- Staff training , e.g. LearnPro module GGC 292 – Ligature Awareness

Clinical assessments and controls will also be utilised to manage self-harm risk as part of an individual's care plan.

This year's SHaW Task Calendar includes the undertaking of Self-Harm Self Audits. These self audits allow managers and services to check their compliance with managing this risk and are also an integral NHSGGC governance tool.

For more information and guidance please refer to the Self-Harm Sharepoint.

Or contact your local Health and Safety Team: Master Team Alignment Slides 07.02.2025.pptx

May 2025 – Digital Skills and Literacy: eHealth drop-in sessions and floor walking

Issues with digital systems, accounts or equipment?

Get help face-to-face on your site, via floor walks or drop-in sessions!

Floor walks and drop-ins allow you to speak to eHealth trainers/facilitators and technical analysts face-to-face. Drop-ins also provide a Microsoft Teams option.

There are issues that can be resolved quickly so that you do not need to log on eHelp.

These can help you if have any general IT issues related to:

- GGC Network accounts
- M365 including Teams, SharePoint and Outlook
- TrakCare
- Clinical Portal
- HEPMA
- OneSign (Single Sign-On)
- Secure Personal Printing (SPP)
- Winscribe
- Emis Web

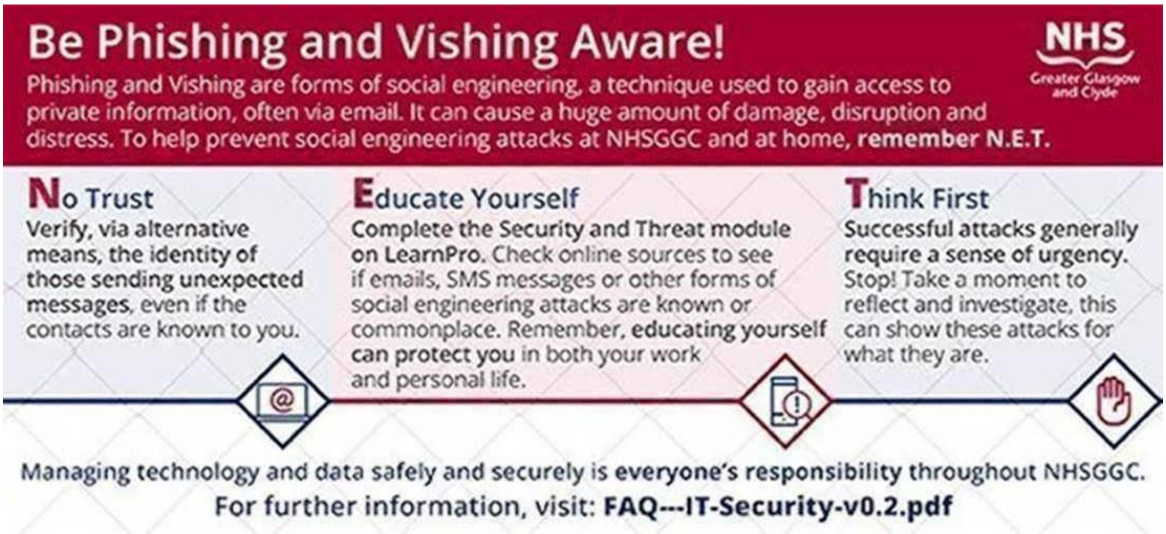
eHealth drop-in sessions (April/May 2025)

Date	Time	Location
27 May	10:00-12:00	Glasgow Royal Infirmary Queen Elizabeth Building Atrium
28 May	10:00-12:00	Queen Elizabeth University Hospital INS near reception area
29 May	10:00-12:00	Royal Alexandra Hospital – Main foyer

eHealth floor walking support (May 2025)

Date	Time	Location
7 May	13:00-15:00	Royal Hospital for Children
8 May	10:00-12:00	Royal Alexandra Hospital Maternity
13 May	13:00-15:00	Glasgow Royal Infirmary
14 May	13:00-15:00	Queen Elizabeth University Hospital Admin Building
15 May	10:00-12:00	Leverndale Hospital
20 May	13:00-15:00	Glasgow Royal Infirmary
21 May	13:00-15:00	Queen Elizabeth University Hospital
22 May	10:00-12:00	Inverclyde Royal Hospital - Larkfield

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



Be Phishing and Vishing Aware!

NHS Greater Glasgow and Clyde

Phishing and Vishing are forms of social engineering, a technique used to gain access to private information, often via email. It can cause a huge amount of damage, disruption and distress. To help prevent social engineering attacks at NHSGGC and at home, **remember N.E.T.**

No Trust

Verify, via alternative means, the identity of those sending unexpected messages, even if the contacts are known to you.

Educate Yourself

Complete the Security and Threat module on LearnPro. Check online sources to see if emails, SMS messages or other forms of social engineering attacks are known or commonplace. Remember, **educating yourself can protect you** in both your work and personal life.

Think First

Successful attacks generally require a sense of urgency. Stop! Take a moment to reflect and investigate, this can show these attacks for what they are.

Managing technology and data safely and securely is **everyone's responsibility** throughout NHSGGC.

For further information, visit: **FAQ---IT-Security-v0.2.pdf**

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