NHS Greater Glasgow and Clyde

Core brief

Wednesday, 12 December 2018

Introduction

This issue brings you details of the new email usage policy.

New email usage policy

The last three years have seen many changes to email, its usage, legislation that affects use, underpinning technology and boundaries for secure exchange.

NHSGGC has a new Email Usage Policy that applies to all our staff using GGC or NHS Mail. The policy can be found on StaffNet Information Governance and Information Technology Security Framework. All GGC users should read and comply with the policy.

New key points to note

- The email exchange between GGC mail and NHS.net email is considered secure and can be used to exchange sensitive information (Red and Amber).

- Email exchange between GGC and any other domain is not secure and outgoing email with red or amber sensitive data should be encrypted using the GGC email encryption service. Details about email encryption can be found in StaffNet Be Cyber Safe Guidance .
- It is the senders responsibility to ensure that mail is appropriately secured.

- The vast majority of email-related privacy breaches have been the result of sending information to the wrong person. No amount of encryption will help reduce this. It can simply be the result of choosing the incorrect name from an address list. So users should confirm a recipients address if you are planning to send Amber or Red data.

- All users should ensure their details in the Global Address List (GAL) are correct.

- All users should keep their corporate persona separate from their personal persona by not using your corporate email address for your personal life and vice versa. (Regardless of attractiveness of Uber offer during Christmas 2018.)

Do not open emails or click on links or attachments in an email from untrusted sources. Please refer to Phishing Awareness Presentation in Be Cyber Safe page.