NHSmail

Enabling collaboration across health and social care

Local Administrator (LA) bulletin – 6 February 2020

Please note this information is correct at the time of publishing

Management of shared mailboxes

A shared mailbox (also known as a generic mailbox) can be accessed by a group of users from the same organisation. Mailboxes become inactive and eligible for deletion when they have not sent an email for over six months.

Inactive shared mailboxes will be deleted from March 2020.

Further information is available on the NHSmail support site and also in the Data Retention and Information Management Policy.

What action do I need to take?

Please advise your users that eligible inactive shared mailboxes will be deleted from March 2020 and they need to take action now, and in the future, to ensure their shared mailbox remains active if they still wish to use it.

Note: We recommend that shared mailbox owners send an email at least once every four to five months, to avoid inactivity and deletion after six months.

Adding multiple Primary Local Administrators

Multiple Primary Local Administrators (PLAs) can be added to your organisation for contingency purposes, for example annual leave, sickness etc.

This enables your organisation to continue to receive key communications and ensure you act upon these messages in a timely manner.

If your organisation does not have a PLA, contact feedback@nhs.net with the appropriate approval attached to the request from either your chief executive officer, IT director or HR director.

If you leave your current organisation, please ensure that your PLA rights are delegated to an appropriate person.

For further information on the PLA role, see the article Roles and Permissions.

Spoofed email now set to 'reject'

We have now applied amendments to DMARC DNS settings so that incoming spoof email is set to 'reject' rather than 'quarantine'.

Following the implementation of spoofing in August 2019, there continues to be a downward trend of spoofed emails.

Currently, recipients of spoof emails receive a notification from the NHSmail team, warning of the spoof emails. This notification will soon stop and we will communicate via the Announcements page on the support site when this change is applied.

Actions to protect your NHSmail account

Due to the scale of the NHSmail platform and the various types of emails processed, and along with the enhanced security features recently added, a low volume of blocked legitimate email may be encountered.

To reduce the impact of non-delivered high importance email, users should be encouraged to check their Junk E-mail folder and should ensure delivery receipts are used as outlined in the Acceptable Use Policy (Section 4.3.4).

Although the NHSmail platform provides a high level of reliability, the delivery of email cannot be 100% guaranteed.

Note: Where an application account is used to send email to an nhs.net email address, periodic monitoring / testing should be conducted to ensure successful email delivery is occurring for the targeted recipients.

Free simulated phishing awareness exercise – now available

NHS Digital's Data Security Centre is offering a free-to-use simulated phishing email exercise for health and care organisations to assist in the education, and highlight users' awareness, of phishing attacks.

The exercise includes a training / awareness animation for users and once deployed a report is issued providing a list of targeted users and recommendations on the results.

What action do I need to take?

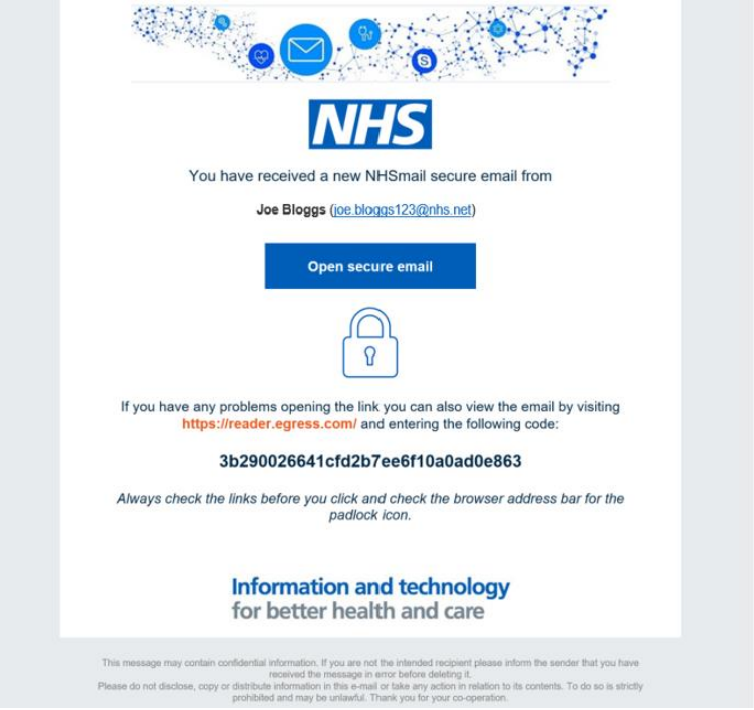
To sign up please visit the NHS Digital simulated phishing training tool for further information.

Egress encryption service – coming soon

The NHSmail service includes an encryption feature that allows users to exchange information securely with users of non-accredited or non-secure email services, for example Gmail, Hotmail, nhs.uk (*.secure.nhs.uk however is considered secure).

Note: Emails that are sent with the word [secure] in square brackets within the email subject line are sent encrypted.

As part of a technology refresh, we are changing the provider of the encryption service to Egress. NHSmail users will not be affected by this change and can continue to send emails securely to non-secure email domains by using [secure]. However, recipients of the encrypted email will now receive an NHSmail branded email as follows:



When an encrypted email is first received from NHSmail via Egress, the recipient will be prompted to create an Egress account – they will only need to do this once and then they will be able to securely view and send any future emails.

Previously sent emails used by the old encryption technology will still be accessible. We will be updating the NHSmail support site, from March 2020, with information for NHSmail users and external recipients regarding Egress and encrypted emails.

What action do I need to take?

Please let your NHSmail users know now that this change will be happening in March 2020 and remind them that:

- if they are sending sensitive information outside of NHSmail, then they should refer to the sharing sensitive information by email guide on the support site
- they can exchange sensitive information securely with other NHSmail users (@nhs.net to @nhs.net), without needing to use the encryption feature.

Note: If there is doubt or uncertainty, you should use the NHSmail encryption feature, meaning that NHSmail will encrypt the email only if the destination domain is not secure. If sending an email to multiple organisations with some secure and some insecure domains, those that are secure will receive an unencrypted email and those that are not secure will receive an encrypted email.

Hiding application accounts in the NHS Directory (People Finder) – coming soon

After listening to feedback from Local Administrators, new Portal functionality is being introduced to allow Local Administrators to hide application accounts from appearing in the NHS Directory. By introducing this, hidden application accounts will not be listed or searchable via the NHS Directory.

Introducing Same Sign On – coming soon

We are developing functionality that will enable users to sign-in to their local Active Directory (AD) using their NHSmail password.

The benefits will be an improved user experience, increased cyber security resilience and reduced administrative burden for password management.

Same Sign On will be available on an 'opt-in' basis and further details will be provided in our next Local Administrator bulletin.

Contacts for further help

NHSmail helpdesk:	0333 200 1133 / helpdesk@nhs.net
Service status:	https://support.nhs.net/service-status/
NHSmail support site:	https://support.nhs.net/

Privacy Statement
Terms and Conditions

NHSmail is provided by NHS Digital in partnership with Accenture

accenture NHS Digital

Working together in partnership