# NHSmail Impersonation Accounts Guide

October 2018
Version 1

# Contents

# Target audience

NHSmail organisations who wish to set up an impersonation account.

# Introduction

Microsoft Exchange Impersonation enables an individual, administrator or application to impersonate a given user account. On the NHSmail Service, impersonation rights will only be granted to a person account that has been converted to an application type account.

# Granting access to a mailbox

Local Administrators have the facility to set up access to other user's mailboxes in one of three ways:

- By adding delegates and specifying permissions for each delegate.
- By modifying folder permissions directly.
- By using impersonation.

# When should you use delegate access, folder permissions or an impersonation account?

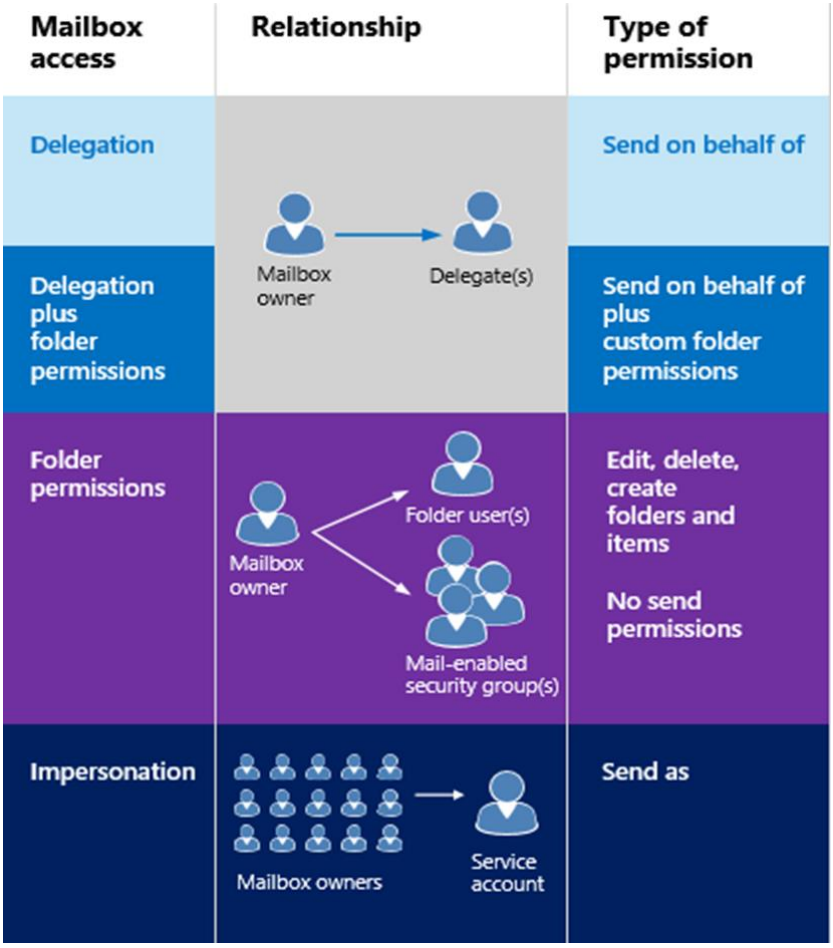
The following guidelines will help you decide when you should use delegate access, folder permissions or an impersonation account:

- Use **delegate access** when you want to give one user permission to perform work on behalf of another user. Typically, this is a one-to-one or one-to-a-few permission. For example, a single administrative assistant managing the calendar for an administrator, or a single room scheduler managing the calendars for a group of meeting rooms.
- Use **folder permissions** when you want to provide a user access to a folder but do not want the user to have "send on behalf of" permissions.
- Use **impersonation** when you have a service application that needs to access multiple mailboxes and "act as" the mailbox owner. Emails sent will appear to be sent from the account being impersonated but will originate from elsewhere.

Delegation and folder permissions are best when you're only granting access to a few users and for ease this can be done within the Portal tools without any specific request to the NHSmail team.

Impersonation is the best choice when you're dealing with multiple mailboxes because you can easily grant one service account access to the required mailboxes.

**Figure 1:** Differences between each type of access.




Impersonation is ideal for applications that connect to Exchange and perform operations, such as:

- archiving email
- setting Out of Office automatically for users on holiday
- any other task that requires the application to act as the owner of a mailbox.

When an application uses impersonation to send a message, the email appears to be sent from the mailbox owner. There is no way for the recipient to know the mail was sent by the service account and not the owner.

# Security considerations for impersonation

Impersonation enables a specific account to impersonate a given user account. This enables the account to perform operations by using the permissions that are associated with the impersonated user account, instead of the permissions that are associated with the impersonation account. For this reason, you should be aware of the following security considerations:

- The Impersonation role is granted to an application account dedicated to a particular application or group of applications, not to a user account. To convert a person mailbox into an application account please contact feedback@nhs.net You can request as many application accounts as you need.
- Only application accounts that have been granted the Impersonation role by the NHSmail helpdesk team can use impersonation.
- You must have director approval for the use of impersonation accounts, stating the scope of use for approval.
- You must inform the person/s whose accounts are being impersonated to ensure they are aware of activity (sending of emails appearing to be from them).
- The requesting organisation's Chief Information Officer (CIO) needs to review the security and clinical implications for their organisation in regard to the use of impersonation.

# Management of impersonation accounts

Inactive impersonation accounts will be managed in accordance with the Data Retention and Information Management Policy.

Removal of impersonation accounts is the responsibility of the Local Administrator and must be requested via the NHSmail helpdesk whenever there is a change in status.

Whilst inactive accounts will be removed, in line with the Data Retention & Information Management Policy, Local Administrators shouldn't rely on this and should be proactive in the removal of impersonation rights when they are no longer required.

# How to request an impersonation account

Impersonation accounts should be requested via the NHSmail helpdesk by completing the template below.

All requests must:

- Relate to an application account (a person mailbox needs to be converted via a request to feedback@nhs.net)
- State the application account name that needs impersonation rights
    - This account must be an application account (already set to application in the Portal)
    - The name of this cannot be a person account e.g. john.smith@nhs.net but could be myapplication.alerts@nhs.net
- The list of email accounts it needs to impersonate
    - Confirmation that the person(s) whose account(s) is being impersonated has been informed
- The reason why an impersonation account is required e.g. what it is going to be used for
- Impersonation rights can ONLY be granted for users within the same organisation as the application account
- The helpdesk will need CIO sign off / approval from the organisation requesting the impersonation account before they proceed

# Impersonation account request template

| Information requested | Answer |
|---|---|
| Email account that needs impersonation rights | **[insert application account name] @nhs.net** * |
| Is the account already set as an application account? | **Yes/No** |
| Is the name of the account a person account i.e. john.smith@nhs.net<br><br>It must not be. | **Yes/No** |
| Has the person(s) whose account(s) is being impersonated been informed | **Yes/No** |
| Please list the NHSmail email accounts in your organisation it needs to impersonate | |
| Please state the reason for the request i.e. what is going to be used for | |
| Is the user from the same organisation as the application account? | **Yes/No** |
| * **In exceptional circumstances, applications allowing an organisation to request that one account has permissions over every account in the organisation will be considered. In this case, the following confirmation is required:**<br><br>a) Have members of the Board signed off - which must include one or other of the Chief Technology Officer (CTO) or Chief Executive Officer (CEO) at least<br>b) Does your organisation process Patient Identifiable Data (PID) through NHSmail? If so have you conducted a clinical safety review? | **a) Yes / No**<br>CTO/CEO email:<br><br>**b) Yes** - clinical safety review has been completed<br>**No** – clinical safety review has not been completed |
| Name, email address and role of requestor | **Name:**<br><br>**Email:**<br><br>**Role: [CIO level or Board member]** |

# How to remove impersonation rights on an account

Removal of impersonation rights on an account should be requested via the NHSmail helpdesk by completing the template below.

All requests should:

- State the email account that needs impersonation rights removed
  - Confirmation that the person whose impersonation account is being removed has been informed.
- The list of email accounts the application account was impersonating (if not removing impersonation from all accounts)
- The reason why the permissions need to be removed
- The helpdesk will need CIO sign off / approval from the organisation requesting the impersonation rights to be removed before they proceed

# Request to remove impersonation rights template

| **Information requested** | **Answer** |
|---|---|
| Email account that needs impersonation rights removed | **[insert application account name] @nhs.net *** |
| Has the person whose impersonation rights being removed been informed? | **Yes/No** |
| Is the request for a full removal of the impersonation rights?<br><br>If removing from a subset of users please list the user accounts, the rights should be removed from. Otherwise state ALL | **Yes/No**<br><br>**Subset:** |
| Please state the reason for the removal request i.e. why is it no longer required. | |
| Name, email address and role of approver | **Name:**<br>**Email:**<br>**Role: [CIO level or Board member]** |