NHSmail Intune Service

Terms of Reference

Published November 2022

Contents

1. Overview

This document has been created to ensure that organisations joining the NHSmail Intune Platform are aware of the onboarding steps and shared responsibilities of the service.

Please read the following terms and prerequisites carefully as you will be required to confirm that you have read and agree to all terms as outlined in this document when completing the Onboarding Request Form.

By submitting an onboarding request (via completion and submission of the Onboarding Request Form) you are confirming that your organisation is fully aware of and can meet the requirements laid out in this document.

2. Enrolment Prerequisites

The below pre-requisites are requirements on the onboarding organisation (unless stated) and need to be met prior to onboarding users and devices onto the NHSmail Intune service. Failure to meet any of the stated enrolment pre-requisites will delay or even prohibit successful onboarding onto the Intune service.

2.1 Completing the Onboarding Request Form

- Organisations will be invited to complete the Onboarding Request Form once they have completed either the NHSmail Intune Information Gathering Survey or the Intune Registration Form.
- Organisations will not be able to complete the Onboarding Request Form until they have received an invitation from the Intune Live Service Team to do so.
- The Onboarding Request Form (accessed via Helpdesk Self-Service on the NHS Portal) will need to be completed and include all requested information in order for an onboarding request to be submitted and processed.
- The Local Admin who completes the Onboarding Request Form will be assumed to be the Onboarding Manager and will be regarded as the key point of contact at the organisation.

2.2 Technical Prerequisites

- Organisations will need to un-enrol all required devices from existing device management platforms and then reset all devices to factory settings to enable the enrolment of devices into NHSmail Intune.
- It is the responsibility of the local organisation to remove all data prior to the factory reset and for the subsequent storage of that data. Please note that this may include personal data a user may wish to keep.
- Devices mix for the NHSmail Intune Platform (as of November 2022) is confirmed as iOS/iPadOS, Android, Windows 10, and HoloLens 2. Both single user devices and shared devices will be supported.
- Google Zero Touch deployment is not currently supported.

- Organisations will need to gather the hardware hashes of all Windows10 and HoloLens2 devices and then upload these into Intune Autopilot.
- Organisations should follow the naming conventions provided in the Operations Guide for Local Administrators and Onboarding Managers before onboarding Windows10 and/or HoloLens2 devices into Intune Autopilot.
- For Windows 10 and HoloLens2 devices, a group tag attribute must be assigned before the device is imported into Intune. Any device which doesn't have a group tag assigned, can be deleted by the central IT teams.
- The Windows Autopilot Device Import Page in Intune is shared by all organisations on the platform and LAs will be able to see hardware IDs which do not belong to their organisation. LAs should not make any changes/updates to any device which does not belong to them (doesn't have their ODS assigned to the Group Tag Attribute).
- LAs should inform the Intune Live Service Team by raising an incident if they have bulk imported devices without a group tag.
- There is a device limitation of 15 devices per Local Administrator.

2.2.1 ABM for iOS/iPadOS

- Organisations wanting to enrol Apple devices (iOS iPhones and iPadOS iPads) will require those devices to exist in an Apple Business Manager (ABM) instance already.
- Organisations will be required to associate their vendor management portals with Intune (e.g., connect ABM with NHSmail Intune); note: the Intune Live Service team will support the connecting of ABM to NHSmail Intune, this is an available Service Request once your organisation has been onboarded. Service Requests for NHSmail Intune will be outlined in more detail below.
- When connecting your organisation's ABM into NHSmail Intune, the Apple ID used to connect into Intune should have **either** the Administrator role or the Device Enrolment Manager (DEM) role assigned to it in ABM. Please do not have both roles assigned to the Apple ID being used to connect into Intune as this may cause a conflict.
- Locations will need to be set up within ABM and domain verification setup, including the acceptance of terms and conditions should have been completed.
- Organisation ownership and management of Apple Business Manager (ABM) for iPads and iPhones is to be maintained at all times, including Apple IDs.

2.2.2 Minimum Platform Requirements

- Relevant and required device and Operating System licensing (e.g., Windows 10).
- Cloud-only device enrolment will involve leaving the existing organisation On-Premises domain and joining NHSmail's Azure AD.
- For Windows devices, Windows 10 Pro/Enterprise version 1809 or higher with relevant OS license will be supported.
- For Windows 10, a central baseline of policies will be set, apply to all organisations and will be locked down.
- For HoloLens2, running the Windows 10 April 2018 update is required.
- For HoloLens2, an internet connection of at least of 1.5 mbps bandwidth is recommended.
    - Organisations will need to confirm that minimum platform requirements have been across all device types. Further details can be found in the Operations Guide for Local Administrators and Onboarding Managers.

2.3 Policies

- LAs will be provided with native Role-Based-Access-Controls (RBAC) to the NHSmail Intune tenant to manage their individual device estates. This will provide LA autonomy when enrolling and managing devices.
- For all platforms, there are advised “pencil-in” policies to be applied to devices, but these can be changed from within the NHSmail Intune tenant by LAs, at their own risk.
- Any changes organisations make to their environment after Intune has been provisioned are the responsibility of the organisation.
- LAs will be required to support End Users with regards to data storage back-up to avoid any data loss during enrolment and the resetting of devices.
- Only corporate mobile device management (MDM) is available at this time. App Protection policies for BYO devices are currently not supported or available.
- Via the Intune RBAC model, the organisation will be able to deploy applications to their device estate via Intune. Organisations must ensure their applications are licensed, compatible for the target platform and compatible with Intune delivery.
- Any application remediation for applications not operating as expected on the target platforms and operating systems, is to be owned by organisations.

2.4 Organisation

- Organisations must consider the clinical implications of using the Intune Service, and undertake a clinical risk assessment in line with the clinical safety standard DCB0160.
- No formal Intune training will be available to LAs, although guidance documentation will be available to all onboarded organisations to support LAs to upskill and end users to begin using Intune-enrolled devices (see Section 5.3 for more details).
- It is expected and the responsibility of organisations that LAs are upskilled in Intune device management sufficiently to be able to enrol devices and provide Level 1 and Level 2 support to their end users.
- Where appropriate, organisations should ensure there are suitable back-up device arrangements in place; it should be noted though that LAs will retain the right via their RBAC permissions to unenroll devices from NHSmail Intune.

2.5 End Users

- End users can be in either clinical or non-clinical roles and can work any hours.
- All end users and LAs must have an nhs.net account.
- There is a device limitation of 5 devices per end user.

3. Licensing Requirements

The below requirements need to be fulfilled for organisations’ EMS E3 and AADP2 licenses to be available for use. Failure to fulfil licensing requirements will cause a delay to onboarding.

- EMS E3 and AADP2 licenses are required and should be procured before engagement.

- Procured EMS and AADP2 licenses should be allocated to the NHSmail Shared tenant. This is required to ensure that your licenses are visible in the NHSmail Portal and available for LAs to manage. For further details and guidance on how to complete this process, please see Section 4.1 of the Operations Guide for Local Administrators and Onboarding Managers.
- EMS E3 and AADP2 licenses are required for all End Users and LAs who will be using the Intune service on Single User Devices.
- For Shared Devices, EMS E3 and AADP2 licenses are required for the Win10 Autopilot Shared Device Mode but are not required for the following Shared Device Modes:
  - iPadOS Non-User Affinity / Guest Mode
  - iOS Managed Apple ID
  - Android Shared Device Mode (Dedicated)
- Organisations should provide details of licenses procured if requested.
- Where required, relevant Operating System licensing should be in place (e.g., Windows 10 Pro or Enterprise).
- If your licenses can't be assigned, it may be because they have not been moved into the NHS Tenant. If you are unsure if you have moved your procured licenses into the NHS Tenant, please read this article and follow the steps outlined if necessary: https://support.nhs.net/knowledge-base/onboarding-guide-for-local-administrators/
- If your organisation has not moved your procured licenses into the NHS Shared Tenant, please complete and submit the License Onboarding Form accessible via Helpdesk Self-Service.
- The License Onboarding Form can be completed and submitted at any time, as organisations may have procured new licenses when already onboarded onto the NHSmail Intune Service.

4. Set Policies and RBAC Settings

Best endeavours have been made to preserve LA device management autonomy; however some policies are set centrally and locked-down for LAs. The below policies and RBAC settings have been set centrally and will not be changeable to LAs from onboarded organisations. LAs from onboarded organisations do not have permissions to configure these settings and will be blocked from doing so.

A standard baseline for all policies will be configured or “pencilled-in” for all technology platforms. Such “pencilled-in” policies will be delivered via the NHSmail Intune Role Based Access Control (RBAC) model to be provided to LAs as part of the onboarding process. Intune RBAC permissions will enable LAs to configure Intune policies, baselines, and applications for their device estate only.

Requests from LAs to update Windows 10 baselines (centrally managed) can be made. These should be requested by completing a Service Request Form via Helpdesk Self-Service. Requests will be considered by the NHSmail Technical Design Authority (TDA) – see Support Model Diagram C in Section 5.4 of this document. There is no requirement for NHSmail to approve requests for changes to these set policies and RBAC Settings, however the outcome of the request will be communicated to the LA who raised the ticket.

4.1 Centrally Managed Permissions

Organisations should consider whether the below security settings may conflict with any local settings or policies that have been set locally. It is recommended that you adjust any conflicting local policies and/or settings accordingly to minimise enrolment delays.

- MDM Authority
- Apple MDM Push Certificate
- Manage Google Play account
- Microsoft Store for Business
- Android Enterprise – corporate owned fully managed enrolment
- Android Enterprise – Enrolment Profiles
- Device Clean-up rules
- Conditional Access
- Intune Company Portal – branding and customisation
- Custom notifications
- Windows 10 Security Baseline
- Android Enterprise – Corporate Owned Dedicated Device

4.2 LA Delegated Permissions

LAs from onboarded organisations do have permissions to configure the following policies and RBAC settings:

- Autopilot Profile
- Apple Automated Device enrolment
- Device Categories
- Device management
- App management
- Device compliance policies
- Device configuration profiles
- App configuration profiles
- iOS app provisioning profiles
- Apple VPP tokens
- Policy sets
- Terms of Use
- Update policies for iOS/iPad
- Enrolment restrictions

More detailed information on the Intune environment is included in the Operations Guide for Local Administrators and Onboarding Managers.

5. Live Service Support, Service Responsibilities and Supporting Documentation

The below terms detail the service support available to any organisation onboarded to the NHSmail Intune Service, the service responsibilities of onboarded organisations and guidance materials available to support onboarded organisations to roll-out NHSmail Intune successfully across their organisation.

5.1 Service Support

- All onboarding requests (license onboarding and organisation onboarding), service requests and Level 3 incidents will need to be raised as tickets via Helpdesk Self-Service (HSS) on the NHS Portal.
- Helpdesk Self-Service should be used in the first instance for all incidents requiring the support of the Intune NHSmail Live Service team and should be limited to Level 3 incidents or service requests.
- All completed and submitted Incidents and Service Requests will be sent to the Intune Live Service Team for review and the LA who submitted the form/s will be updated on the progress and outcome of any request via the standard incident process.

5.1.1 Service Requests

- The following Service Requests tickets can be submitted for review by the Intune Live Service Team:
  - Windows 10/11 BitLocker recovery key
  - Request an Android enrolment profile (Shared Device)
  - Request to offboard an organisation from the NHSmail Intune Service
  - Request to onboard your organisation's Apple Business Manager (ABM) for Apple Devices
  - Request to add a certificate connector
  - Request to add a multi-organisation
  - Query related to security posture
  - Request for Cloud + SSO Track and Hybrid Join Track
  - Other
- If the service request ticket falls outside of the areas stated above, LAs are required to select 'Other' and fill in the description box with their service request. The Intune Live Service Team will update the requestor with the resolution and close ticket.

5.1.2 Incidents

- The following Incidents can be submitted for review by the Intune Live Service Team (LST):
  - Organisation onboarding
  - Device enrolment
  - Intune Role Based Access Control (RBAC) Permissions
  - Device configuration and policies (LA Delegated)
  - Intune Group Management Tool
  - Resetting Devices
  - Applications
  - Conditional Access
  - Centrally managed configuration (security posture)
  - Other
- If the incident falls outside of the areas stated above, LAs are required to select 'Other' and fill in the description box with their incident request. The LST will update the requestor with the resolution and close ticket.
- It is highly recommended that LAs use Helpdesk Self-Service in the first instance to ensure that the raised ticket is directed to the correct team/s and can be reviewed and actioned promptly.

- The national NHSmail Helpdesk (Helpdesk@nhs.net) should only be contacted regarding incidents, service requests or onboarding requests if:
    - LAs are unable to complete or understand the form
    - Form/s are not working
    - Out of Hours Support is required
    - There is an urgent escalation
  - NHSmail Helpdesk can be contacted in any of the above scenarios via phone on 03332001133 or by emailing helpdesk@nhs.net, 24 hours a day, 365 days a year.
  - If the Helpdesk is contacted in relation to an incident request, they provide links to relevant information on the NHSmail Support Site or will direct the LA to the Incident Form accessible via Helpdesk Self-Service.
  - If the Helpdesk is contacted in relation to a service request, they will log the query and direct the LA to the Service Request Form accessible via Helpdesk Self-Service.
  - If the LA contacting the Helpdesk is unable to complete either the Incident Form or the Service Request Form, the Helpdesk will be able to complete either Form on behalf of the LA and will submit the incident or review to the Intune Live Service Team.
  - If the Helpdesk is contacted in relation to an Onboarding request, they will log the query and direct the LA to the Onboarding Request Form accessible via the Helpdesk Self-Service.
  - The Helpdesk will be unable to complete the Onboarding Request Form on behalf on an LA. The Helpdesk can assist an LA to complete the Onboarding Request Form but the Onboarding Request Form must be completed and submitted by an LA.
  - Any tenant-wide technical updates (changes affecting every organisation on the NHSmail Intune platform), change/s in terms or general notices to all organisations onboarded onto the NHSmail Intune Service, will be communicated to the LAs at onboarded organisations and it is expected that LAs will communicate the update as appropriate within their organisation to ensure continuity of service.
  - As a last resort, LAs can wipe, reset, or remove devices from Intune. Wiping devices and removing them from Intune is the responsibility of organisations.
  - Organisations have the option to offboard from the Intune service. This process will take at least a day to complete and offboarding times may vary depending on how many devices have been enrolled in the tenant. LAs will need to raise a service request via Helpdesk Self-Service if they want to offboard from the Intune service. The process for offboarding will require secondary sign-off from someone within your organisation.

5.2 Service Responsibilities of the Onboarded Organisation

- Before raising an incident, LAs should ensure that they have referred to the Operations Guide for Local Administrators and Onboarding Managers in order to try to troubleshoot the issue themselves first.
- Organisations should ensure that all LAs who have RBAC controls or are supporting end users using Intune-enrolled devices have access to Helpdesk Self-Service site. This can be found via this link: Helpdesk Self-Service. LAs will need to use their nhs.net credentials to log in and be able to submit tickets.
- Organisations must ensure resources with suitable experience are available to provide Level 1 support (service desk and deskside support) and Level 2 triage and fix support (via delegated RBAC permissions) to end users.
- LAs are responsible for the enrolment and unenrolment of devices

- LAs are responsible for the management of all of their devices
- Post onboarding and creation of their organisation’s bespoke environment in NHSmail Intune platform using scope tags, LAs are responsible for management of that environment.
- LAs are responsible for managing local device configuration policies and profiles (apart from Windows 10 baselines).
- Any changes made (by LAs via delegated RBAC permissions) to an organisation’s Intune estate post organisation onboarding are the responsibility of the organisation.
- LAs are responsible for using scope tags (their ODS code) when creating items and objects in Intune (see Operations Guide for Local Administrators), any objects or items created without a scope tag may be deleted by the Intune Live Service team without notice.

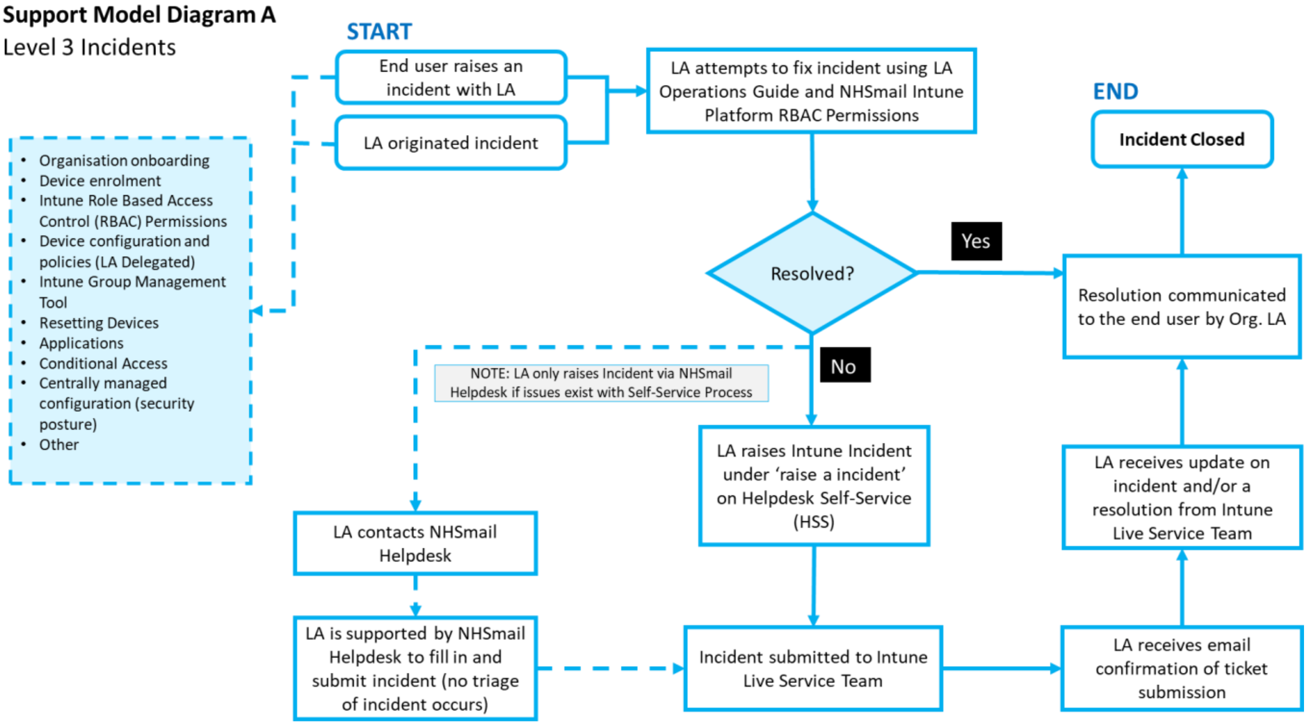
5.3 Supporting Documentation & Communications

- Organisations are responsible for all communications to their user base.
- All end user and LA communications and guidance materials provided to organisations onboarded to the NHSmail Intune Service will be held in a central repository on the NHSmail Support Site. A link to this repository will be provided to you once you have received your confirmation of onboarding email.
- If any LA / end user communications and / or guidance materials are edited by an organisation to suit the specificities of an individual organisation’s context, this is done at that organisation’s own risk.
- Quick Start End User Guides and FAQs will be provided to support end users at onboarded organisations to start using Intune-enrolled devices and perform some simple technical troubleshooting.
- LAs and Organisation Intune Onboarding Managers will be provided with the Operations Guide for Local Administrators and Onboarding Managers to support upskilling.
- LA and end user Communications templates will be provided to support organisations to inform LAs and end users about the NHSmail Intune Service.

5.4 NHSmail Intune Platform Support Model Diagrams

Support Model Diagram A

Level 3 Incidents



START

End user raises an incident with LA

LA originated incident

- Organisation onboarding
- Device enrolment
- Intune Role Based Access Control (RBAC) Permissions
- Device configuration and policies (LA Delegated)
- Intune Group Management Tool
- Resetting Devices
- Applications
- Conditional Access
- Centrally managed configuration (security posture)
- Other

LA attempts to fix incident using LA Operations Guide and NHSmail Intune Platform RBAC Permissions

Resolved?

Yes

No

NOTE: LA only raises Incident via NHSmail Helpdesk if issues exist with Self-Service Process

LA contacts NHSmail Helpdesk

LA is supported by NHSmail Helpdesk to fill in and submit incident (no triage of incident occurs)

LA raises Intune Incident under 'raise a incident' on Helpdesk Self-Service (HSS)

Incident submitted to Intune Live Service Team

LA receives email confirmation of ticket submission

LA receives update on incident and/or a resolution from Intune Live Service Team

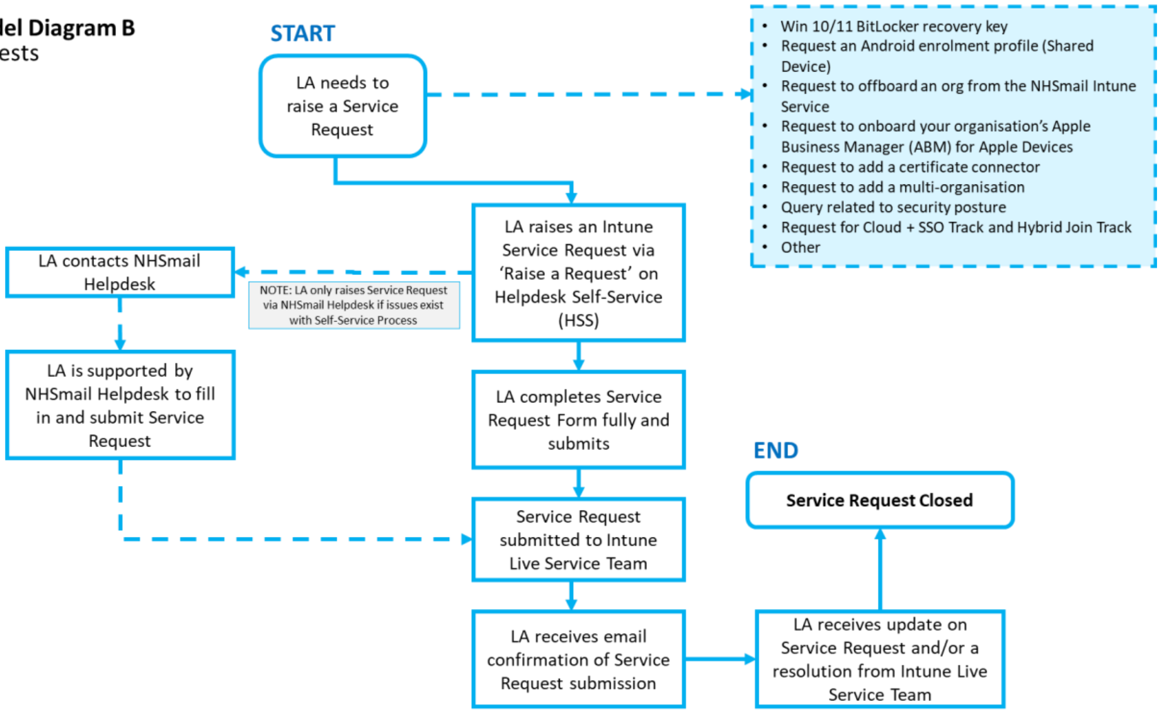
Resolution communicated to the end user by Org. LA

END

Incident Closed

Support Model Diagram B

Service Requests



START

LA needs to raise a Service Request

- Win 10/11 BitLocker recovery key
- Request an Android enrolment profile (Shared Device)
- Request to offboard an org from the NHSmail Intune Service
- Request to onboard your organisation's Apple Business Manager (ABM) for Apple Devices
- Request to add a certificate connector
- Request to add a multi-organisation
- Query related to security posture
- Request for Cloud + SSO Track and Hybrid Join Track
- Other

LA raises an Intune Service Request via 'Raise a Request' on Helpdesk Self-Service (HSS)

NOTE: LA only raises Service Request via NHSmail Helpdesk if issues exist with Self-Service Process

LA contacts NHSmail Helpdesk

LA is supported by NHSmail Helpdesk to fill in and submit Service Request

LA completes Service Request Form fully and submits

Service Request submitted to Intune Live Service Team

LA receives email confirmation of Service Request submission

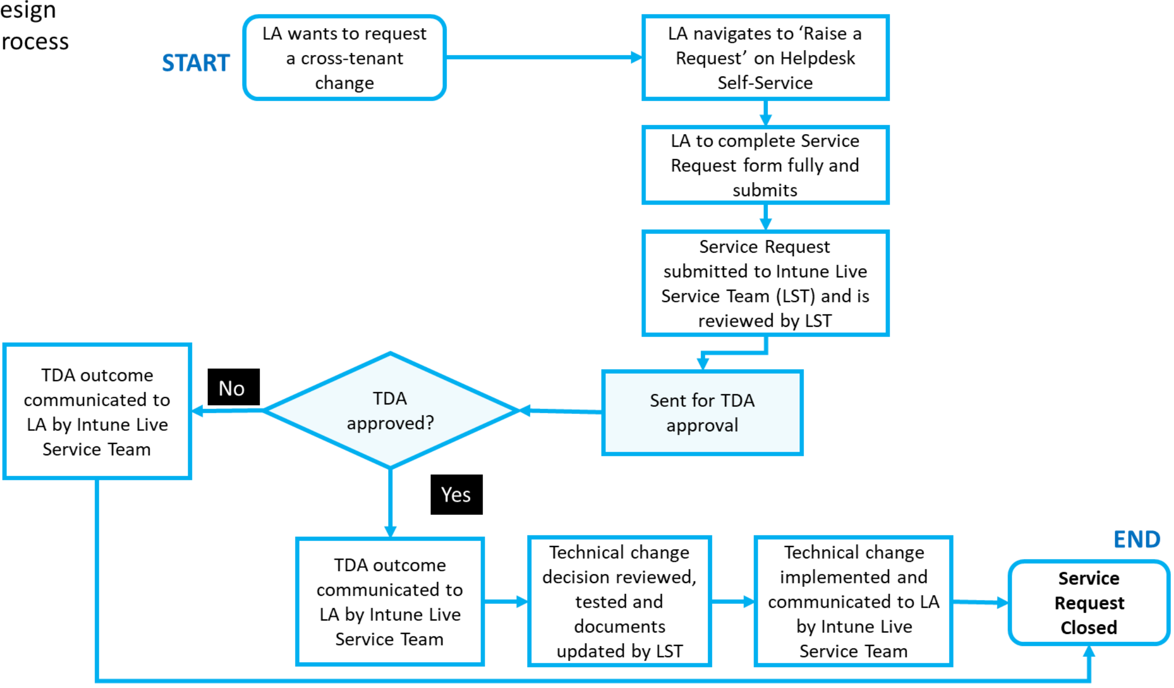
LA receives update on Service Request and/or a resolution from Intune Live Service Team

END

Service Request Closed

Support Model Diagram C

Technical Design Authority Process


START
LA wants to request a cross-tenant change
LA navigates to 'Raise a Request' on Helpdesk Self-Service
LA to complete Service Request form fully and submits
Service Request submitted to Intune Live Service Team (LST) and is reviewed by LST
Sent for TDA approval
TDA approved?
No
TDA outcome communicated to LA by Intune Live Service Team
Yes
TDA outcome communicated to LA by Intune Live Service Team
Technical change decision reviewed, tested and documents updated by LST
Technical change implemented and communicated to LA by Intune Live Service Team
END
Service Request Closed

5.5 NHSmail Intune Platform RACI Chart

R **Responsible**: The individual(s) that complete the task.

A **Accountable**: The individual(s) that is ultimately answerable for the activity or decision.

C **Consulted**: The individual(s) to be consulted prior to a final decision or action.

I **Informed**: The individual(s) that need to be informed after a decision or action is taken.

Please note: All instances where the Intune Live Services Team need to be consulted (C) or informed (I) will happen automatically via the submission of Helpdesk Self-Service forms. Organisations are not required to do anything.

	ACTIVITY / SERVICE ITEM	ONBOARDED ORGANISATION / LAs				INTUNE LIVE SERVICES TEAM			
ONBOARDING ORG.	Read and agree to the Terms of Reference	**R**	**A**	C	I	R	A	C	**I**
	Provide requested information to assist with org. onboarding (technical and business readiness information)	**R**	**A**	C	I	R	A	**C**	**I**
	Complete all technical and business readiness activities to ensure org. is ready to onboard devices onto NHSmail Intune	**R**	**A**	C	I	R	A	C	I
GUIDANCE DOCUMENTATION	Own and manage key guidance documentation provided on NHSmail Support Site	R	A	C	I	**R**	**A**	C	I
	Send / distribute links to key guidance documentation to LAs once organisation has been onboarded	R	A	C	**I**	**R**	**A**	C	I
	Update key guidance documentation with any technical changes and/or service changes	R	A	C	**I**	**R**	**A**	C	I
SUPPORT	Provide Level 1 support to end users (e.g., Service Desk)	**R**	**A**	C	I	R	A	C	I
	Provide Level 2 support to end users	**R**	**A**	C	I	R	A	C	I
	Provide Level 3 support to organisation's LAs (via submitted incidents)	R	A	**C**	**I**	**R**	**A**	C	I
	Review and action Service Requests	R	A	**C**	**I**	**R**	**A**	C	I
	Upskilling LAs in Intune and NHSmail Intune Platform	**R**	**A**	C	I	R	A	C	I
INTUNE MANAGEMENT	Enrolment and unenrolment of devices	**R**	**A**	C	I	R	A	C	**I**
	Management of enrolled devices and organisation's device estate on NHSmail Intune	**R**	**A**	C	I	R	A	C	I
	Manage delegated device configuration policies and profiles (apart from Windows 10 baselines)	R	A	**C**	**I**	**R**	**A**	C	I
	Manage centrally-controlled Windows 10 Baselines	R	A	C	I	**R**	**A**	C	I

6. Additional Considerations

Additional considerations for organisations enrolling onto the NHSmail Intune Platform include the following:

Intune Awareness and Knowledge: There is an assumption that if an organisation enrols onto NHSmail Intune, there exists within that organisation a good level of understanding of the Intune solution and the functionality of MDM and RBAC features.

Organisation's Service Support Responsibilities: All onboarded organisations are responsible for Level 1 and Level 2 incidents which arise from their user base and there is an assumption that all onboarded organisations will be able to resolve these.

Data Visibility: Organisations who join the NHSmail Intune tenant are joining a single tenant containing multiple organisations. Management of an organisation's devices and changes to an organisation's data are limited to an organisation through custom permissions, however some areas cannot be controlled by such custom permissions and limited data pertaining to other organisations may be visible. In particular, in some monitoring and reporting views data pertaining to other organisations are visible and can in some cases be exported, such as device names and UPNs of assigned users.

Organisations **must treat any such data as confidential**. In addition, organisations can make changes in some areas (Android applications, Autopilot devices) which can affect other organisations, so care should be exercised when accessing and managing these areas.

Organisations are responsible for protecting their sensitive data and ensuring that they follow their local data security policies – particularly regarding naming standards and free text fields.

Further details pertaining to specific areas of Intune where data may be visible can be found in the Operations Guide for Local Administrators and Onboarding Managers.